Informe “Cost of a Data Breach” de 2025

La brecha en la supervisión de la IA

Resumen ejecutivo

think report

IBM

Resumen ejecutivo

Bienvenido al informe “Cost of a Data Breach” anual de IBM. Con esta edición, celebramos 20 años de investigación sobre vulneraciones de datos. Este año nos centramos en el cambio tecnológico más importante de la última generación: la adopción de la IA.

En el informe de 2025, empezamos a documentar y cuantificar los riesgos asociados a la IA. Lo que hemos descubierto es preocupante: muchas organizaciones están dejando de lado la seguridad y el gobierno en favor de una adopción acelerada de la IA. Estos sistemas no controlados son más vulnerables y, cuando se ven afectados, resultan más costosos.
Esto no nos sorprende.

Desde 2005, este informe ha estado realizando un seguimiento del panorama tecnológico en constante expansión y de las amenazas que lo acompañan. Nuestros socios del Ponemon Institute no solo han documentado la aparición de nuevas amenazas y superficies de ataque, sino que también las han cuantificado en términos financieros para que los responsables de seguridad y de la empresa puedan comprenderlas y actuar en consecuencia. En total, sus investigadores han estudiado más de 6485 vulneraciones y han entrevistado a más de 34 652 responsables de tecnología, seguridad y empresa implicados en la respuesta de su organización ante la vulneración.

Obviamente, las amenazas a la seguridad han cambiado con los años. Hace dos décadas, casi la mitad de las vulneraciones de datos (45 %) se debían a la pérdida o el robo de un dispositivo informático, como un ordenador portátil o una memoria USB, mientras que solo el 10 % se atribuía a “sistemas electrónicos pirateados”. En la actualidad, la mayoría de las vulneraciones se deben a una serie de actividades maliciosas, que van desde el phishing hasta las amenazas internas.

Hace diez años, las vulneraciones debidas a una mala configuración de la nube ni siquiera estaban catalogadas como amenaza. En la actualidad, la nube y los datos que contiene son un objetivo prioritario. No fue hasta los bloqueos por la pandemia de la COVID-19 en 2020 cuando el ransomware empezó a dispararse. Un año después, esos ataques supusieron una media de 4,62 millones de dólares en costes por vulneraciones, cifra que alcanzó los 5,08 millones de dólares en el informe de este año.

Sin embargo, una constante ha sido la labor de Ponemon.
La investigación de este año, realizada de forma independiente por el Ponemon Institute y patrocinada, analizada y publicada por IBM, estudió 600 organizaciones afectadas por vulneraciones de datos entre marzo de 2024 y febrero de 2025. En total, se analizaron organizaciones de 17 sectores en 16 países y regiones, y vulneraciones que oscilaban entre 2960 y 113 620 registros comprometidos. Con el fin de obtener conocimientos de primera mano, los investigadores de Ponemon entrevistaron a 3470 ejecutivos de equipos directivos y de seguridad que habían experimentado de primera mano las vulneraciones de datos en sus organizaciones. Entre ellos había CEO, responsables de operaciones, control de gestión, finanzas, TI, jefes de unidad de negocio, directores generales y profesionales de gestión de riesgos y ciberseguridad.

El resultado es un informe de referencia que los líderes empresariales, tecnológicos y de seguridad pueden utilizar para reforzar sus defensas, informar sobre la asignación de recursos e impulsar la innovación, en particular en lo referente a la seguridad y la gestión de sus iniciativas de IA.

El titular de este año es que los costes mundiales de las vulneraciones de datos han disminuido por primera vez en cinco años, y se han situado en 4,44 millones de dólares, gracias a una contención más rápida de las vulneraciones impulsada por defensas con IA. Sin embargo, a medida que las defensas se vuelven más inteligentes y rápidas, los atacantes también se hacen más inteligentes y rápidos: en el 16 % de las vulneraciones de datos, según los informes, los atacantes utilizaron IA, que a menudo se emplea en ataques de phishing y deepfake. Aunque esta carrera armamentística de la IA ha beneficiado a las organizaciones al reducir los costes de las vulneraciones a nivel mundial, Estados Unidos no sigue la tendencia. En este país, los costes de las vulneraciones han superado los diez millones de dólares debido al endurecimiento de las sanciones normativas y al aumento de los costes de detección.

También descubrimos que la adopción de la IA supera a la supervisión. El 97 % de las violaciones de seguridad relacionadas con la IA implicaban sistemas de IA que carecían de controles de acceso adecuados. Además, la mayoría de las organizaciones afectadas por vulneraciones informaron de que no contaban con políticas de gobierno para gestionar la IA o evitar su uso no autorizado. Tanto el uso encubierto de la IA en la sombra como la falta de gobierno están incrementando el coste de las vulneraciones.

Novedades en el informe de 2025

Como siempre, el informe “Cost of a Data Breach” refleja las nuevas tecnologías, las tácticas emergentes y los acontecimientos recientes. Por primera vez, la investigación de este año explora:

- El estado de la seguridad y el gobierno de la IA
- La prevalencia y el perfil de riesgo de la IA en la sombra
- El tipo de datos objeto de incidentes de seguridad relacionados con la IA
- La duración de las interrupciones por vulneraciones en las organizaciones
- El ahorro de costes por el uso de herramientas de seguridad cuántica
- Los costes de las vulneraciones asociados a los ataques impulsados por IA
- El importe de los costes de las vulneraciones repercutidos a los clientes

Principales conclusiones

Las principales conclusiones se basan en el análisis realizado por IBM de los datos de la investigación recopilados de forma independiente por Ponemon Institute.

4 440 000 USD

Coste medio mundial de una vulneración de datos

El coste medio mundial de las vulneraciones se redujo a 4,44 millones de dólares, frente a los 4,88 millones de dólares de 2024, lo que supone un descenso del 9 % y sitúa el coste de nuevo en los niveles de 2023. La rápida identificación y contención de las vulneraciones, en gran parte por parte de los propios equipos de seguridad y servicios de seguridad de las organizaciones, con la ayuda de la IA y la automatización, impulsaron este descenso. La media mundial habría sido más baja si no fuera por Estados Unidos, donde el coste medio aumentó un 9 % hasta alcanzar los 10,22 millones de dólares, la cifra más alta registrada hasta la fecha en cualquier región. El aumento de las multas reglamentarias y de los costes de detección y escalada contribuyó a este incremento.

13 %

Porcentaje de incidentes de seguridad relacionados con la IA

De momento, los incidentes de seguridad relacionados con la IA de una organización siguen siendo limitados. De media, el 13 % de las organizaciones informaron de vulneraciones relacionadas con sus modelos o aplicaciones de IA. Sin embargo, entre las que lo hicieron, casi todas (el 97 %) carecían de controles de acceso adecuados a la IA. Los incidentes de seguridad más comunes se produjeron en la cadena de suministro de la IA, a través de aplicaciones, API o complementos comprometidos. Estos incidentes tuvieron un efecto dominó: llevaron a un compromiso generalizado de los datos (60 %) y a la interrupción de las operaciones (31 %). Estos resultados sugieren que la IA se está convirtiendo en un objetivo muy valioso.

4 920 000 USD

Coste medio de los ataque de usuario interno negligente

Por segundo año consecutivo, los ataques de usuario interno negligente provocaron el coste medio más elevado entre los vectores de amenaza iniciales: 4,92 millones de dólares. Le siguieron de cerca los ataques a proveedores externos y a la cadena de suministro, con 4,91 millones de dólares. Otros vectores de ataque costosos fueron la explotación de vulnerabilidades y el phishing. Sin embargo, el tipo de vector de ataque más frecuente contra las organizaciones fue el phishing, con un 16 %, y supuso una media de 4,8 millones de dólares.

200 000 USD

Coste añadido de una vulneración que involucre IA en la sombra

De las organizaciones estudiadas este año, el 20 % afirmó haber sufrido una vulneración debido a incidentes de seguridad relacionados con la IA en la sombra. Estas vulneraciones incrementaron en 200 321 USD el precio medio de la vulneración. Estos incidentes también pusieron en peligro datos de identificación personal (65 %) y de propiedad intelectual (40 %). Estos datos se almacenaban a menudo en múltiples entornos, lo que revela que un solo sistema de IA no supervisado puede dar lugar a una exposición generalizada. El rápido auge de la IA en la sombra ha desplazado a la escasez de conocimientos de seguridad como uno de los tres factores más costosos de las vulneraciones analizadas en este informe.

1 900 000 USD

Ahorro de costes gracias al uso generalizado de la IA en materia de seguridad

Los equipos de seguridad que utilizan ampliamente la IA y la automatización acortaron en 80 días el tiempo que tardaban en sufrir una vulneración y redujeron sus costes medios por vulneración en 1,9 millones de dólares en comparación con las organizaciones que no utilizaban estas soluciones. Casi un tercio de las organizaciones afirmaron que utilizaban ampliamente estas herramientas en todas las etapas del ciclo de vida de la seguridad: prevención, detección, investigación y respuesta. Sin embargo, esta cifra es ligeramente superior a la del año anterior, lo que sugiere que la adopción de la IA puede haberse estancado. También muestra que la mayoría todavía no utiliza la IA y la automatización, por lo que no percibe los beneficios económicos.

63 %

Porcentaje de organizaciones que se negaron a pagar el rescate a los hackers que utilizaron ransomware

En 2025, el 63 % de las víctimas de ransomware se negó a pagar un rescate, frente al 59 % en 2024. Sin embargo, el coste medio de un incidente de extorsión o ransomware sigue siendo elevado, especialmente cuando lo comete un atacante (5,08 millones de dólares). Al mismo tiempo, menos víctimas de ransomware informaron de que habían involucrado a las fuerzas de seguridad: el 40 % de las organizaciones este año frente al 53 % del año pasado.

49 %

Porcentaje de organizaciones que invierten en seguridad tras sufrir una vulneración

El número de organizaciones que planean invertir en seguridad después de una violación ha disminuido significativamente, situándose en el 49 % este año, en comparación con el 63 % del año pasado. Menos de la mitad de las que tienen previsto invertir en seguridad planean centrarse en soluciones o servicios de seguridad impulsados por IA, como la detección y respuesta a amenazas, la planificación y las pruebas de respuesta a incidentes (IR) y las herramientas de protección o seguridad de datos.

63 %

Porcentaje de organizaciones que carecen de políticas de gobierno de la IA

La mayoría de las organizaciones afectadas (el 63 %) no tienen una política de gobierno de la IA o todavía la están desarrollando. Incluso cuando tienen una política, menos de la mitad cuenta con un proceso de aprobación para implementar la IA, y el 62 % carece de controles de acceso adecuados en los sistemas de IA. Entre las organizaciones que cuentan con políticas de gobierno, solo una minoría (el 34 %) realiza auditorías periódicas de la IA no autorizada. Esto demuestra que la IA sigue sin control, ya que su adopción supera tanto a la seguridad como al gobierno.

1 de cada 6

Número de vulneraciones relacionadas con ataques impulsados por IA

Los atacantes pueden utilizar la IA generativa para perfeccionar y ampliar sus campañas de phishing y otros ataques de ingeniería social. IBM descubrió anteriormente que la IA generativa reducía a cinco minutos el tiempo necesario para elaborar un correo electrónico de phishing convincente, que antes era de dieciséis horas. El informe de este año muestra el impacto: de media, en el 16 % de las vulneraciones de datos los agresores utilizaron IA, sobre todo para el phishing generado por IA (37 %) y los ataques de suplantación de identidad (35 %).

Recomendaciones

Para ayudar a prevenir, mitigar y reducir los costes de una vulneración de datos, así como para garantizar la seguridad y el gobierno de los modelos, las aplicaciones y el uso de la IA, los expertos de IBM sugieren estos cinco enfoques exitosos.

Refuerce las identidades, tanto humanas como mecánicas

Muchas organizaciones tienen controles de acceso laxos, cuentas con demasiados permisos y poca visibilidad sobre quién tiene acceso a los sistemas críticos. En muchos casos, la gestión de identidades y accesos (IAM) se lleva a cabo mediante distintos departamentos y herramientas. Todos estos factores crean puntos débiles que los atacantes explotan activamente, por lo que es esencial limitarlos. Mientras tanto, los modelos y la infraestructura de IA crecen rápidamente, lo que ofrece a los atacantes una nueva superficie de ataque muy valiosa.

Fortalecer la seguridad de las identidades con la ayuda de la IA y la automatización puede mejorar la IAM sin sobrecargar a los equipos de seguridad, que suelen estar crónicamente escasos de personal. A medida que los agentes de IA empiezan a desempeñar un papel más importante en las operaciones de las organizaciones, es necesario aplicar el mismo rigor a la protección de las identidades de los agentes que a la de las identidades humanas. Al igual que los usuarios humanos, los agentes de IA dependen cada vez más de las credenciales para acceder a los sistemas y realizar tareas. Por lo tanto, es esencial implementar controles operativos sólidos o servicios que puedan ayudarle a hacerlo, y mantener la visibilidad de toda la actividad de identidad no humana (NHI). Las organizaciones deben ser capaces de distinguir entre las NHI que utilizan credenciales gestionadas y las que utilizan credenciales no gestionadas.

Una vez que se gestionan las credenciales, es crucial protegerlas y aplicar una gestión y gobierno adecuados a lo largo de todo su ciclo de vida. Esto incluye el aprovisionamiento, la rotación, la auditoría, la protección y el desmantelamiento de las credenciales, así como la monitorización del comportamiento de las NHI para garantizar que operan dentro de los parámetros esperados. Así, las organizaciones pueden reducir el riesgo de uso indebido de credenciales y mantener un entorno seguro y conforme a la normativa.

Hoy en día, muchos atacantes prefieren iniciar sesión en lugar de piratear. Para combatir este problema, resulta crítico impedir que los atacantes obtengan esas credenciales en primer lugar. Una de las formas más eficaces de lograrlo es garantizar que todos los usuarios humanos utilicen métodos de autenticación modernos y resistentes al phishing, como las claves de acceso. Estas tecnologías están diseñadas para eliminar las vulnerabilidades de las contraseñas tradicionales y de los códigos de un solo uso, por lo que resulta mucho más difícil para los atacantes interceptar o utilizar indebidamente las credenciales de inicio de sesión.

Mejore las prácticas de seguridad de datos de IA

Las organizaciones han superado la fase de experimentación con la IA generativa y los agentes de IA, y han pasado a innovar en el mundo real al integrar la tecnología en el tejido de sus empresas. Sin embargo, la velocidad de adopción está superando a la seguridad. Según el informe de este año, el 62 % de las organizaciones carece de controles de acceso adecuados en los sistemas de IA. Y, como los datos son el combustible de la IA, constituyen un objetivo prioritario para los atacantes.

La protección de los datos de la IA no solo es esencial para garantizar la privacidad y el cumplimiento de la normativa, sino también para proteger su integridad, mantener la confianza de la organización y evitar ponerla en peligro. Este enfoque implica ir más allá de los controles superficiales y aplicar sólidos fundamentos de seguridad de datos, como la detección de datos y su clasificación, así como protecciones de datos, como el control de acceso, el cifrado y la gestión de claves. También puede incluir el uso de servicios de seguridad de datos y de IA. Estas medidas no son exclusivas de la seguridad de la IA, pero el auge de esta como vector de amenazas y como ayudante de seguridad significa que son más importantes que nunca.

Conecte la seguridad y el gobierno de la IA

La seguridad y el gobierno de la IA son disciplinas complementarias. Cuando las organizaciones las mantienen en silos, aumentan el riesgo, la complejidad y el coste. Lamentablemente, la adopción de la IA está superando a la de la seguridad y el gobierno: el 41 % de las organizaciones incluidas en el informe de este año afirmaron que no disponen de dichas políticas y el 22 % todavía las está desarrollando.

Las organizaciones deben asegurarse de que los directores de seguridad de la información (CISO), los directores de ingresos (CRO) y los directores de cumplimiento (CCO) (y sus equipos) colaboren de manera regular. Invertir en software y procesos integrados de seguridad y gobierno que agrupen a estas partes interesadas interfuncionales puede ayudar a las organizaciones a descubrir y gobernar automáticamente la IA en la sombra. Estas inversiones también pueden ayudarles a:

- Obtener visibilidad de todas las implementaciones de IA.
- Identificar y mitigar las vulnerabilidades.
- Proteger las instrucciones y los datos generados de usos no intencionados.
- Utilizar herramientas de observabilidad para mejorar el cumplimiento y detectar anomalías.

Utilizar herramientas de seguridad y automatización de IA para avanzar más rápido.

La IA ya está ayudando a los atacantesa actuar con mayor rapidez, por ejemplo, al facilitar la creación de deepfakes con unas pocas instrucciones o reducir el tiempo necesario para producir un mensaje de phishing realista de horas a minutos. A medida que los agresores recurren a la IA para producir y distribuir ataques más adaptables, los equipos de seguridad también deberían adoptar tecnologías de IA. Los equipos de seguridad pueden utilizar la IA para reducir o prevenir los ataques y su impacto en el negocio, al utilizar medidas proactivas que mejoren la precisión de la detección (búsqueda de amenazas) y reduzcan el tiempo de respuesta.

Las herramientas de seguridad y los servicios de seguridad gestionados, incluidos los basados en IA y automatización, pueden descongestionar los equipos de seguridad, que ya están sobrecargados. Estas herramientas pueden reducir significativamente el volumen de alertas, identificar los datos de riesgo, detectar antes las brechas de seguridad y las amenazas, detectar las vulneraciones en curso y permitir respuestas más rápidas y precisas a los ataques.

Mejore la resiliencia

A largo plazo, las vulneraciones de datos son inevitables. Ocurren incluso con fuertes medidas preventivas. Aunque es importante intentar bloquear las amenazas, este no puede ser el único objetivo de una organización. También deben centrarse en planificar la minimización de los daños una vez que se ha producido un ataque y una violación de datos.

Crear resiliencia significa ser capaz de detectar problemas rápidamente, contenerlos antes de que causen un impacto significativo y recuperar las operaciones de manera rápida y con la mayor continuidad posible. Un plan de resiliencia debe incluir la comprobación periódica de los planes de IR y la restauración de las copias de seguridad, la definición clara de funciones y responsabilidades durante la respuesta a una crisis (incluso para los responsables no técnicos) y la limitación del acceso de alto nivel para reducir el alcance de un posible problema. La formación presencial o virtual puede resultar esencial para ayudar a los equipos de seguridad a comprender sus funciones y actuar en caso de crisis. Para mejorar su capacidad de hacer frente a los ataques, las organizaciones también pueden participar en ejercicios de simulación de crisis cibernéticas.

Acerca de

IBM

IBM es un proveedor líder mundial de servicios en la nube, IA y empresariales, que ayuda a clientes de más de 175 países a aprovechar el conocimiento de sus datos, agilizar sus procesos empresariales, reducir costes y obtener una ventaja competitiva en sus sectores. Todo ello respaldado por el legendario compromiso de IBM con la confianza, la transparencia, la responsabilidad, la inclusión y la atención al cliente. Para obtener más información, visite ibm.com/es-es.

Para obtener más información sobre cómo mejorar su posición de seguridad: visite ibm.com/es-es/security.

Súmese a la conversación en la IBM Security Community.

Ponemon Institute

Fundado en 2002, el Ponemon Institute se dedica a la investigación y la formación independientes para promover prácticas responsables de gestión de la información y la privacidad en empresas y gobierno. Nuestra misión consiste en llevar a cabo estudios empíricos de alta calidad sobre cuestiones críticas relacionadas con la gestión y la seguridad de la información confidencial sobre personas y organizaciones.

El Ponemon Institute mantiene estrictas normas de confidencialidad de datos, privacidad e investigación ética, y no recopila ningún dato de información de identificación personal (PII) de personas o información identificable de la empresa en la investigación empresarial. Además, las estrictas normas de calidad garantizan que no se hagan preguntas extrañas, irrelevantes o inadecuadas a los participantes. Si tiene alguna pregunta o comentario sobre este informe de investigación, incluidas las solicitudes de permiso para citarlo o reproducirlo, póngase en contacto con nosotros por correo electrónico, postal o teléfono:

Ponemon Institute LLC
Departamento de investigación
1-800-887-3118
research@ponemon.org