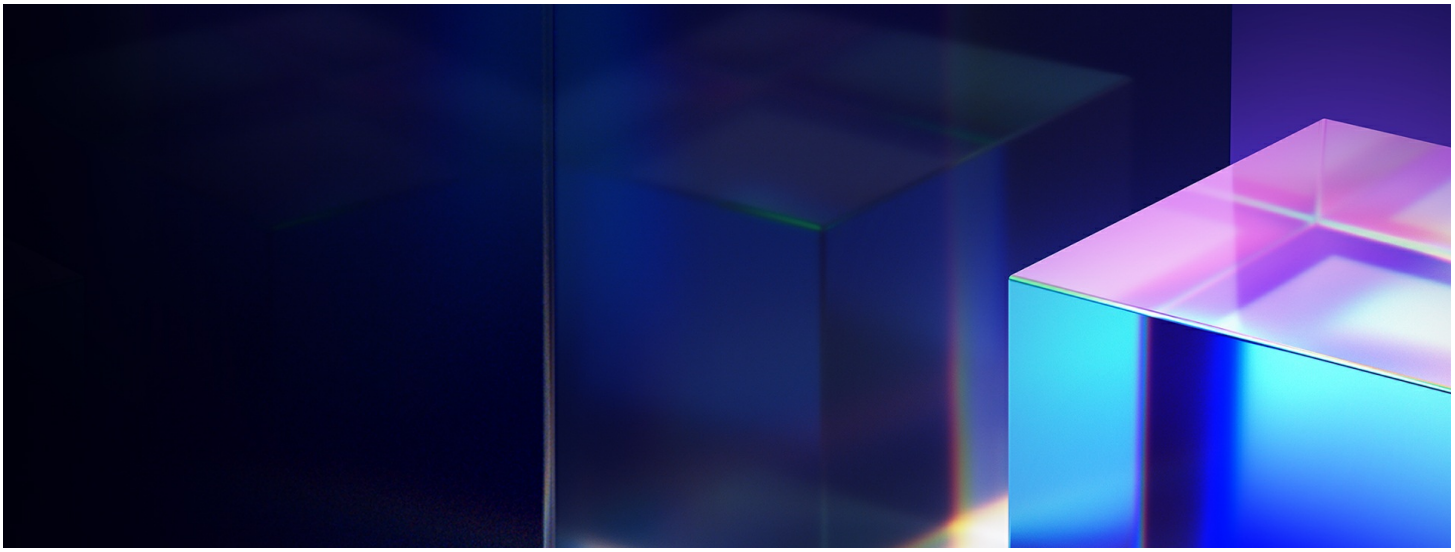
Anuncios

El 13% de las organizaciones ha sufrido brechas en modelos o aplicaciones de IA, y el 97% no contaba con controles de acceso adecuados, según el último informe de IBM

El coste medio de una brecha de datos en EE. UU. alcanza los 10,22 millones de dólares, mientras que la media global se reduce a 4,44 millones. Solo el 49% de las organizaciones afectadas planea invertir en seguridad.



Madrid, 4 de septiembre de 2025. -- IBM ha publicado su nuevo informe anual Cost of Data Breach Report, que desvela un desequilibrio preocupante: la adopción de la IA está avanzando a gran velocidad, pero no va acompañada del refuerzo necesario en materia de seguridad y gobernanza. Por primera vez, el informe examina específicamente la protección de los sistemas de IA, y los resultados muestran que esta tecnología se ha convertido ya en un objetivo fácil y de gran valor para los ciberdelincuentes.

> *“El informe revela una brecha clara entre la velocidad con la que se está adoptando la IA y las medidas de supervisión que la acompañan, una laguna que los atacantes ya están aprovechando”*

- El 13% de las organizaciones encuestadas ha sufrido una brecha en modelos o aplicaciones de IA, y un 8% adicional no está seguro de si se han visto comprometidos de esa manera.
- El 97% de las organizaciones afectadas no contaba con controles de acceso específicos para IA.
- Como resultado, el 60% de estos incidentes comprometieron datos y el 31% provocaron interrupciones operativas.

“El informe revela una brecha clara entre la velocidad con la que se está adoptando la IA y las medidas de supervisión que la acompañan, una laguna que los atacantes ya están aprovechando”, explica Ana Gobernado, directora general de IBM Consulting en España, Portugal, Grecia e Israel. “La falta de controles básicos de acceso deja datos sensibles expuestos y modelos vulnerables a la manipulación. Si la IA va a integrarse de forma estructural en los procesos de negocio, su seguridad debe ser también estructural. Lo que está en juego no es solo el dinero: es la confianza, la transparencia y el control”.

A pesar de esta situación, el informe también señala una ventaja clave: las organizaciones que emplean IA y automatización de forma intensiva en sus operaciones de ciberseguridad reducen el coste medio de una brecha en 1,9 millones de dólares y acortan su ciclo de vida en 80 días de media.

El informe ha sido elaborado por el Instituto Ponemon, con el patrocinio y análisis de IBM, a partir del estudio de 600 brechas de datos registradas entre marzo de 2024 y febrero de 2025 en organizaciones de todo el mundo.

Brechas en la era de la IA

- **Políticas de gobernanza de la IA.** El 63% de las organizaciones que sufrieron una brecha no contaban con una política de gobernanza de IA o estaban en proceso de desarrollarla. Solo el 34% de las que sí la tienen realizan auditorías periódicas para detectar usos no autorizados de IA.
- **El coste oculto de la IA en la sombra.** Una de cada cinco organizaciones sufrió una brecha causada por IA no autorizada (shadow AI), y solo el 37% tiene políticas activas para detectar y gestionar la IA. Las organizaciones con un uso intensivo de IA en la sombra tuvieron costes un 15% más altos (670.000 dólares de media) y vieron comprometida más información personal (65%) y propiedad intelectual (40%) que la media global (53% y 33%, respectivamente).
- **Ciberataques más sofisticados.** En el 16% de las brechas analizados, los delincuentes emplearon herramientas de IA, principalmente para campañas de phishing o suplantación mediante deepfakes.

El coste financiero de una brecha de datos

- **Menor duración de las brechas.** El ciclo de vida de una brecha (tiempo medio para detectar y contener una infracción, incluidos los servicios de restauración) se redujo a 241 días, 17 menos que el año anterior. Las organizaciones que detectaron la brecha por sí mismas ahorraron de media 900.000 dólares en comparación con aquellas en las que fue el atacante quien la reveló.
- **Sanidad, el sector más costoso.** Con un coste medio de 7,42 millones de dólares, la sanidad sigue siendo el sector más afectado, a pesar de haber reducido en 2,35 millones su media respecto a 2024. El tiempo medio de contención y recuperación en este sector es de 279 días, casi 40 más que la media global.
- **Menos disposición a pagar rescates.** El 63% de las organizaciones se negó a pagar el rescate exigido, frente al 59% del año anterior. Aun así, los incidentes de ransomware siguen teniendo un coste medio muy elevado (5,08 millones de dólares), especialmente cuando son los atacantes quienes los revelan.
- **Menos inversión post-brecha.** Solo el 49% de las organizaciones planea reforzar su seguridad tras una brecha, frente al 63% del año pasado. De ellas, menos de la mitad prevé invertir en soluciones específicas de ciberseguridad con IA.

Más allá del ataque: el impacto operativo

Según el informe de 2025, prácticamente todas las organizaciones analizadas sufrieron disrupciones operativas tras una brecha de seguridad, lo que ha impactado significativamente en los plazos de recuperación. Entre las organizaciones que lograron recuperarse, la mayoría tardó más de 100 días de media en hacerlo.

Sin embargo, las consecuencias de una brecha no terminan con la contención del incidente. Aunque hayan descendido respecto al año anterior, casi la mitad de las organizaciones afirmaron que planeaban subir el precio de sus productos o servicios a raíz de la brecha, y casi un tercio declaró que esas subidas serían del 15% o más.

Sobre el Cost of Data Breach Report

El Cost of a Data Breach Report ha analizado cerca de 6.500 incidentes en los últimos 20 años. Desde su primera edición en 2005, la naturaleza de las brechas ha evolucionado de forma drástica: antes, el riesgo era principalmente físico; hoy, el entorno es predominantemente digital y cada vez más dirigido, con ciberataques motivados por una amplia variedad de actividades maliciosas.

Con la rápida adopción de la IA en el entorno empresarial, por primera vez el estudio incluye un análisis exhaustivo del estado de la seguridad y la gobernanza de esta tecnología. En concreto, el informe examina el tipo de datos más expuestos en incidentes de seguridad relacionados con IA, los costes de las brechas impulsadas por IA, o la prevalencia y el perfil de riesgo de la IA en la sombra (uso no regulado o no autorizado de herramientas de inteligencia artificial).

Hallazgos destacados de informes anteriores:

- **2005:** Casi la mitad (45%) de las brechas de datos se debieron a la pérdida o robo de dispositivos físicos, como ordenadores portátiles o memorias USB. Solo el 10% se originó en sistemas electrónicos hackeados.
- **2015:** Las brechas causadas por una configuración incorrecta en la nube ni siquiera se categorizaban como amenaza. Hoy, constituyen uno de los principales vectores de ataque.
- **2020:** El ransomware comenzó a proliferar. En 2021, el coste medio asociado a estas brechas alcanzó los 4,62 millones de dólares. En 2025, esa cifra ha aumentado hasta los 5,08 millones cuando el incidente es divulgado por el atacante.
- **2025:** Por primera vez, la seguridad de la inteligencia artificial se incluye como área de estudio, y ya se perfila como un objetivo prioritario y de alto valor para los atacantes.

Recursos adicionales

- Descarga el informe completo aquí.

Acerca de IBM

IBM es un proveedor líder de nube híbrida global, inteligencia artificial y experiencia en consultoría. Ayudamos a clientes en más de 175 países a capitalizar el conocimiento de sus datos, optimizar los procesos de negocios, reducir costos y obtener una ventaja competitiva en sus industrias. Más de 4.000 entidades gubernamentales y corporativas en infraestructuras críticas como servicios financieros, telecomunicaciones y atención médica confían en la plataforma de nube híbrida IBM y Red Hat OpenShift para abordar sus transformaciones digitales de manera rápida, eficiente y segura. Las innovaciones revolucionarias de IBM en IA, computación cuántica, soluciones de nube específicas de la industria y consultoría ofrecen opciones abiertas y flexibles para nuestros clientes. Todo esto está respaldado por el compromiso de larga data de IBM con la confianza, la transparencia, la responsabilidad, la inclusión y el servicio. Visita ibm.com para obtener más información.

For further information: Camila Cuetos, Dpto. Comunicación, camila.cuetos2@ibm.com