

Estudio de IBM muestra aumento en el costo de brechas de datos y un impacto financiero que dura años

- Las brechas plantean un riesgo creciente para las pequeñas y medianas empresas, con un costo que equivale hasta el 5% de sus ingresos anuales



CAMBRIDGE, MA. Julio 23, 2019. - IBM (NYSE: [IBM](#)) Security anunció hoy los resultados de su estudio anual que examina el impacto financiero de las brechas de datos en las organizaciones. Según el informe, el costo de una brecha de datos ha aumentado el 12% durante los últimos cinco años^[1] y ahora muestra un costo promedio de \$3.92 millones de dólares. Estos gastos crecientes resultan del impacto financiero de varios años, el aumento en las regulaciones de la industria y el complejo proceso de resolución de ataques criminales.

Las consecuencias financieras de una brecha de datos pueden ser particularmente graves para pequeñas y medianas empresas. En el estudio, las organizaciones con menos de 500 empleados sufrieron pérdidas de más de \$2.5 millones de dólares en promedio, una cifra potencialmente paralizante para pequeñas empresas, que suelen ganar \$50 millones de dólares o menos en ingresos anuales.

Por primera vez este año, el informe también examinó el impacto financiero prolongado que tiene una brecha de datos, y reveló que los efectos de tal incidente se sienten por años. Si bien en promedio un 67% de los costos de brecha de datos se hicieron efectivos dentro del primer año después de la brecha, el 22% se recuperó en el segundo año, y otro 11% siguió acumulándose dos años después de la brecha. Los costos a largo plazo fueron más altos en el segundo y el tercer año para organizaciones en entornos con regulaciones estrictas, tales como salud, servicios financieros, energía y farmacéutica.

“El delito cibernético representa grandes sumas para los delincuentes cibernéticos, y desafortunadamente eso equivale a pérdidas significativas para las organizaciones,” comenta Francisco García, Director de IBM Security en México. “Con empresas que enfrentaron la pérdida o el robo de más de 11,700 millones de registros en los últimos tres años solamente, las compañías deben estar al tanto del impacto financiero total que una brecha de datos puede tener en sus resultados, y concentrarse en formas de reducir esos costos”.

Con el auspicio de IBM Security, el estudio anual realizado por Instituto Ponemon y titulado *Costo de una Brecha*

de Datos se basa en entrevistas detalladas con más de 500 empresas de todo el mundo que sufrieron una brecha durante el último año.^[2] El análisis tiene en cuenta cientos de factores de costos que incluyen: actividades legales, regulatorias y técnicas, así como las pérdidas en términos de valor de marca, clientes y productividad de los empleados. Algunas conclusiones destacadas del estudio de este año:

- **Brechas maliciosas: las más comunes y más caras:** Más del 50% de las brechas de datos en el estudio fueron el resultado de ataques cibernéticos maliciosos, y costaron a las compañías \$1 millón de dólares más en promedio que las que se originaron por causas accidentales.
- **Las “Mega brechas” conducen a mega pérdidas:** Si bien son menos comunes, las brechas de más de 1 millón de registros costaron a las organizaciones una cifra proyectada de \$42 millones de dólares en pérdidas, mientras que las brechas que implican la pérdida de más de 50 millones de registros tendrán un costo proyectado para las organizaciones de \$388 millones de dólares.^[3]
- **La práctica lleva a la perfección:** Las compañías con un equipo de respuesta a incidentes que además comprueba ampliamente dicho plan experimentaron \$1.23 millones de dólares menos en costos de brechas de datos en promedio que las que no tenían ninguna medida implementada.
- **Las brechas estadounidenses cuestan el doble:** El costo promedio de una brecha en los Estados Unidos es \$8.19 millones de dólares, más del doble que el promedio mundial.
- **Las brechas en salud son las más costosas:** Por noveno año consecutivo, las organizaciones del sector salud tuvieron el mayor costo: casi \$6.5 millones de dólares en promedio (más del 60% superior a otras industrias comprendidas en el estudio).

Las brechas maliciosas plantean una amenaza creciente; las brechas accidentales siguen siendo comunes

Según el estudio, las brechas de datos que se originaron de un ataque cibernético malicioso eran no solo la razón más común de una violación sino también la más costosa.

Según el estudio, las brechas de datos maliciosas cuestan a las compañías \$4.45 millones de dólares en promedio, más de \$1 millón de dólares más que las que se originan por causas accidentales, como un defecto en el sistema o error humano. Estas brechas son una amenaza creciente, ya que el porcentaje de ataques maliciosos o delictivos en el informe aumentó del 42% al 51% durante los últimos seis años del estudio (un aumento del 21%).

Dicho esto, las violaciones inadvertidas, por error humano y problemas de sistemas seguían siendo la causa de casi la mitad (49%) de las brechas de datos del informe, con un costo para las compañías de

\$3.50 y \$3.24 millones de dólares respectivamente. Estas infracciones por error humano y de máquinas representan una oportunidad para mejora, que puede abordarse a través de la capacitación y concientización en seguridad para el personal, inversiones en tecnología y servicios de prueba para identificar brechas accidentales en etapas tempranas. Un área particular de preocupación es la configuración errónea de servidores de nube, que contribuyó a la exposición de 990 millones de registros en 2018, y representó el 43%

de todos los registros perdidos durante el año, según el Índice de Inteligencia de Amenazas IBM X-Force[4].

La respuesta a las brechas sigue siendo el mayor factor de ahorro de costos

Durante los últimos 14 años, el Instituto Ponemon viene examinando los factores que aumentan o reducen el costo de una brecha y ha descubierto que la velocidad y eficiencia con la que una compañía responde a una brecha tiene un impacto significativo en el costo general.

El reporte de este año reveló que el ciclo de vida promedio de una brecha era 279 días, mientras que hay compañías que tardan 206 días en identificar una brecha después de que se produce, y unos 73 días adicionales para contener la brecha. Sin embargo, las compañías en el estudio que pudieron detectar y contener una brecha en menos de 200 días gastaron \$1.2 millones menos en el costo total de una brecha.

Un enfoque en la respuesta a incidentes puede contribuir a reducir el tiempo que les lleva a las empresas responder, y el estudio dejó ver que estas medidas tenían una correlación directa con los costos generales. Tener un equipo de respuesta a incidentes constituido y planes amplios de prueba de respuesta a incidentes fueron de los mayores factores de ahorro de costos examinados en el estudio. Las compañías que contaban con ambas medidas implementadas tuvieron \$1.23 millones de dólares de costos totales menos para una brecha de datos promedio que las que no tenían ninguna de esas medidas (\$3.51 millones de dólares versus \$4.74 millones de dólares).

Factores adicionales que impactan en el costo de una brecha para las compañías incluidas en el estudio:

- Cantidad de registros comprometidos: las violaciones de datos les cuestan a las compañías aproximadamente **150 dólares por registro** perdido o robado.
- Las compañías que habían implementado completamente **tecnologías de automatización de seguridad** experimentaron aproximadamente la mitad del costo de una brecha (\$2.65 millones promedio) en comparación con las que no tenían estas tecnologías implementadas (\$5.16 millones de dólares promedio).
- **El uso extenso del encriptado** también fue un factor de ahorro de costos importante, que redujo el costo total de una brecha en \$360 mil dólares.
- **Las brechas originadas en un tercero** – como un socio o proveedor – cuestan a las compañías \$370 mil dólares más que el promedio, lo cual recalca la necesidad de que las compañías inspeccionen cuidadosamente la seguridad de las compañías con las que hacen negocio, alineen las normas de seguridad y monitoreen activamente el acceso de terceros.

Tendencias regionales y de la industria

El estudio también examinó el costo de violaciones de datos en distintas industrias y regiones, y reveló que las infracciones de información en Estados Unidos son mucho más costosas, ya que cuestan \$8.19 millones de dólares, lo cual equivale a más del doble del promedio para compañías mundiales en el estudio. Los costos de

brechas de datos en los Estados Unidos aumentaron un 130% durante los últimos 14 años del estudio, en comparación con los \$3.54 millones de dólares revelados por el estudio de 2006.

Además, las organizaciones en Oriente Medio informaron el más alto número promedio de registros violados, con casi 40 mil registros por incidente (en comparación con el promedio global de unos 25 mil).

Por noveno año consecutivo, las organizaciones de salud participantes en el estudio tuvieron los mayores costos asociados a las violaciones de datos. El costo promedio de una brecha de datos en la industria de salud fue de casi \$6.5 millones de dólares, más del 60% superior al promedio para todas las industrias.

Descargue el informe completo y regístrese para el webinar

De clic para ver el [Estudio sobre el Costo de una Brecha de Datos 2019](#).

Para registrarse al webinar de IBM Security y el Instituto Ponemon Institute el 30 de julio (11:00 horas del Este), de [clic en esta liga](#).

Acerca de IBM Security

IBM Security ofrece una de las carteras más avanzadas e integradas de productos y servicios de seguridad empresarial. La cartera, respaldada por la investigación de renombre mundial IBM X-Force®, permite a las organizaciones administrar los riesgos de forma efectiva y defenderse contra amenazas emergentes. IBM opera una de las organizaciones de investigación, desarrollo y distribución de seguridad más amplias del mundo, supervisa 70 mil millones de eventos de seguridad por día en más de 130 países y ha obtenido más de 8,000 patentes de seguridad en todo el mundo. Para obtener más información, visite www.ibm.com/security, y siga IBM Security en Twitter o visite el blog [IBM Security Intelligence](#).

[1] Comparación del costo promedio de una brecha de datos del reporte de 2014 al reporte de 2019.

[2] Las limitaciones del reporte y las metodologías empleadas pueden consultarse en el reporte completo.

[3] Los cálculos de costos de mega-brechas se basan en un análisis de 14 compañías, que aplican un enfoque analítico Montecarlo para simular los resultados de mayor importancia estadística.

[4] IBM X-Force Threat Intelligence Index 2019
