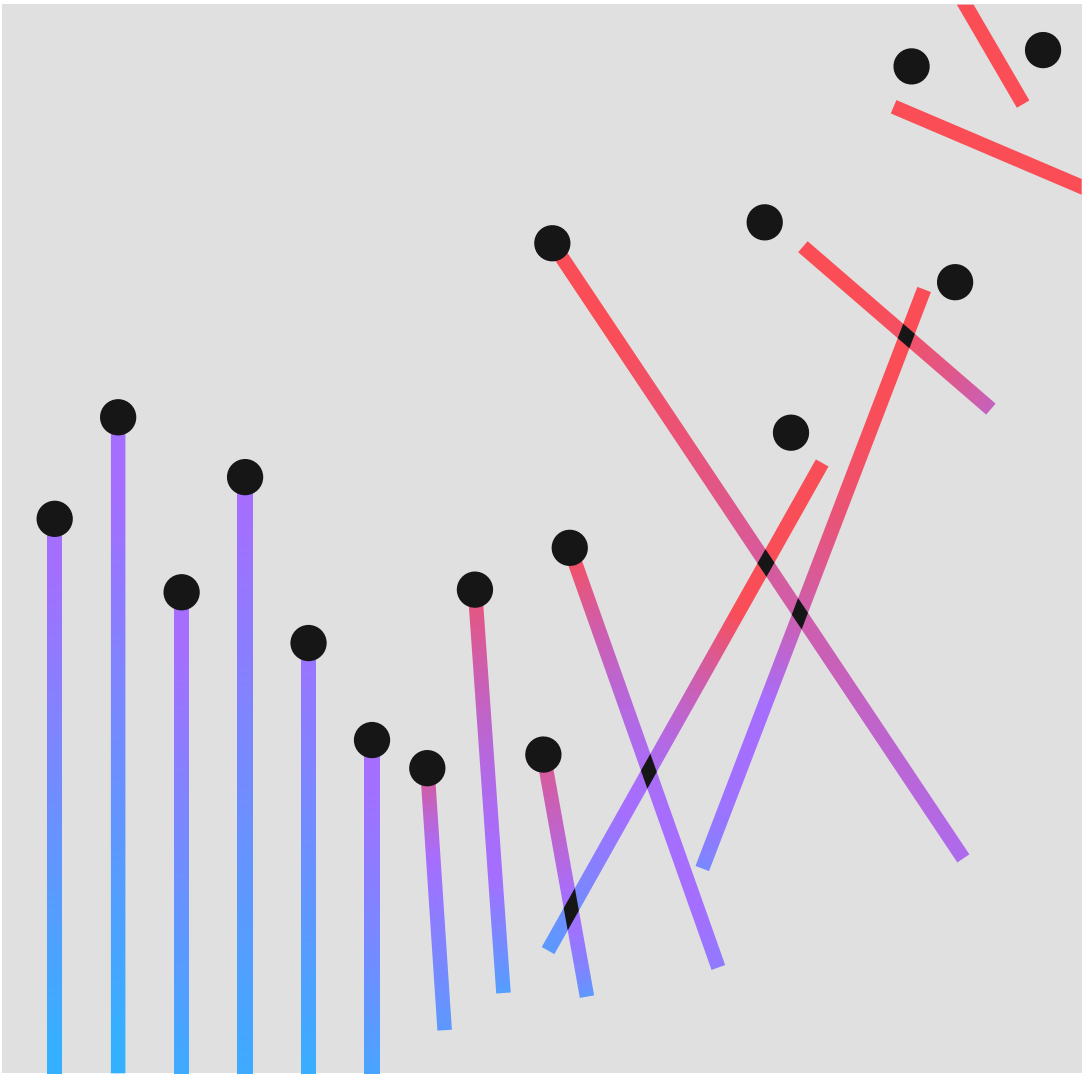
IBM **Security**

Cost of a Data Breach 2022: Resumen ejecutivo



IBM

Contenido

Resumen ejecutivo

El informe Cost of a Data Breach ofrece a los líderes de TI, gestión de riesgos y seguridad información útil sobre factores que pueden aumentar o frenar el incremento del coste de una vulneración de datos.

Ahora, en su decimoséptimo año, este estudio —llevado a cabo de forma independiente por el Instituto Ponemon y patrocinado, analizado y publicado por IBM® Security— investigó a 550 organizaciones afectadas por vulneraciones de datos entre marzo de 2021 y marzo de 2022. Las infracciones se produjeron en 17 países o regiones y en 17 sectores diferentes.

Entrevistamos a más de 3600 individuos de organizaciones afectadas por vulneraciones de datos. Les hicimos una serie de preguntas para determinar cuál fue el coste para estas empresas en diferentes actividades relacionadas directamente con la respuesta inmediata y prolongada a dichos ataques.

Como en años anteriores, los datos de este año ofrecen una perspectiva de los múltiples factores que repercuten en los costes, que siguen aumentando tras una vulneración. Además, el informe analiza las causas raíz, las consecuencias a corto y largo plazo de la vulneración de datos, y los factores y tecnologías que ayudaron a las empresas a limitar sus pérdidas.

Principales hallazgos

Los principales hallazgos aquí descritos se basan en el análisis de datos de investigación de IBM Security compilados por el Instituto Ponemon.[1]

4,35 millones de dólares

Coste medio total de una vulneración de datos

El coste medio de una vulneración de datos fue de 4,35 millones de dólares en 2022, un récord histórico. Esta cifra representa un aumento del 2,6 % con respecto al año pasado, cuando el coste medio fue de 4,24 millones de dólares. El coste medio ha aumentado un 12,7 % con respecto a los 3,86 millones de dólares del informe de 2020.

83 %

Porcentaje de organizaciones que han sufrido más de una vulneración

El 83 % de las organizaciones estudiadas han sufrido más de una vulneración de datos y tan solo el 17 % dijo que fue la primera. El 60 % de las organizaciones estudiadas afirmó que aumentaron el precio de sus servicios o productos como consecuencia de dichas vulneraciones.

4,82 millones de dólares

Coste medio de una vulneración de datos de infraestructura crítica

El coste medio de una vulneración de datos para las empresas de infraestructura crítica estudiadas fue de 4,82 millones de dólares, un millón más que el coste medio para las organizaciones de otros sectores. Entre las empresas de infraestructura crítica se incluyeron las de servicios financieros, industriales, tecnología, energía, transporte, comunicación, sanidad, educación y sector público. El 28 % experimentó un ataque destructivo o de ransomware, mientras que el 17 % experimentó una vulneración al verse comprometido uno de sus socios.

3,05 millones de dólares

Ahorro medio asociado a la IA y la automatización de la seguridad a pleno rendimiento

Las vulneraciones en organizaciones con IA y automatización de la seguridad totalmente implementadas cuestan 3,05 millones de dólares menos que los ataques al resto de las empresas. Esta diferencia del 65,2 % de media —entre los 3,15 millones de las empresas con IA y automatización frente a los 6,20 millones de las que no implementaron estas tecnologías— representó el mayor ahorro del estudio. Las compañías que cuentan con IA y automatización de la seguridad a pleno rendimiento también tardaron de media 74 días menos en identificar y contener el ataque, conocido como el ciclo de vida del ataque, que aquellas sin IA ni automatización de la seguridad (249 días frente a 323). El uso de la IA y la automatización de la seguridad aumentó casi una quinta parte en dos años, de un 59 % en 2020 a un 70 % en 2022.

1. Los costes de este informe están calculados en dólares estadounidenses (USD).

4,54 millones de dólares

Coste medio de un ataque de ransomware, sin incluir el coste del rescate

El 11 % de los ataques del estudio fueron de ransomware, lo que supuso un aumento con respecto a 2021, cuando solo el 7,8 % de los ataques fueron de este tipo. Esto implica una tasa de crecimiento del 41 %. El coste medio de los ataques de ransomware disminuyó ligeramente, de 4,62 millones de dólares en 2021 a 4,54 en 2022. Este coste fue ligeramente superior que la media total de una vulneración de datos, que es de 4,35 millones de dólares.

19 %

Frecuencia de ataques causados por credenciales robadas o en riesgo

El uso de credenciales robadas o en riesgo sigue siendo la causa más común de vulneración de datos. Las credenciales robadas o en riesgo fueron el vector de ataque principal en el 19 % de los casos en el estudio de 2022 y también en el de 2021, en el que constituyeron la causa del 20 % de los ataques. Los ataques causados por credenciales robadas o en riesgo costaron de media 4,50 millones de dólares. Estos ataques tuvieron el ciclo de vida más largo: 243 días hasta identificar el ataque y otros 84 para contenerlo. El phishing fue la segunda causa de infracciones más común, con un 16 %, y también la más costosa, con un coste medio de 4,91 millones de dólares.

59 %

Porcentaje de organizaciones que no emplean zero trust

Tan solo el 41 % de las organizaciones del estudio indicaron que cuentan con una arquitectura de seguridad zero trust. El otro 59 % de las empresas, que no tienen una arquitectura zero trust, paga de media un millón de dólares más por dichos ataques que las otras organizaciones. Entre las organizaciones de infraestructura crítica, el porcentaje es incluso superior: el 79 % no ha implementado una arquitectura zero trust. Estas empresas tuvieron que asumir un coste medio de 5,40 millones de dólares por dichos ataques, más de un millón más que la media mundial.

1 millón de dólares

Diferencia media en el coste cuando el trabajo remoto fue un factor en la causa de los ataques frente a cuando no lo fue

Cuando el trabajo remoto supuso un factor en la causa del ataque, el coste fue de media un millón de dólares superior que cuando no lo supuso: 4,99 millones frente a 4,02 millones. Los ataques relacionados con el trabajo remoto cuestan una media de 600 000 dólares más que la media mundial.

45 %

Porcentaje de ataques que ocurrieron en el cloud

El 45 % de los ataques del estudio ocurrieron en el cloud. Los ataques que ocurrieron en un ambiente de cloud híbrido costaron una media de 3,80 millones de dólares, frente a los 4,24 millones de los ataques en clouds privados y los 5,02 millones en clouds públicos. La diferencia en el coste fue del 27,6 % entre los ataques de cloud híbrido y los de cloud público. Las organizaciones con un modelo de cloud híbrido también tuvieron ciclos de vida del ataque más cortos que aquellas que solo adoptaron un modelo de cloud público o privado.

2,66 millones de dólares

Ahorro medio asociado a un equipo y aun plan de respuesta a incidentes puesto a prueba con regularidad

Casi tres cuartas partes de las organizaciones del estudio dijeron que tenían un plan de respuesta a incidentes, mientras que el 63 % de dichas organizaciones afirmaron que lo comprobaban regularmente. Contar con un equipo de respuesta a incidentes y un plan de respuesta testado con regularidad condujo a un ahorro significativo. A las empresas con un equipo de respuesta a incidentes que puso a prueba su plan, los ataques les costaron una media de 2,66 millones de dólares menos que a aquellas sin dicho equipo y que no pusieron a prueba su plan de respuesta. La diferencia de 3,26 millones de dólares frente a 5,92 millones representa un ahorro del 58 %.

29 días

Ahorro en el tiempo de respuesta para aquellos con tecnología de detección y respuesta extendidas (XDR)

Las tecnologías XDR fueron implementadas por el 44 % de las organizaciones. Las organizaciones con dicha tecnología observaron ventajas considerables en el tiempo de respuesta. Dichas empresas redujeron el ciclo de vida de los ataques en un mes de media aproximadamente frente a aquellas que no implementaron XDR. En concreto, las organizaciones que usaron XDR tardaron 275 días en identificar y contener un ataque, frente a los 304 días de aquellas sin dicha tecnología. Esto supone una diferencia en el tiempo de respuesta del 10 %.

12 años

Años consecutivos en los que el sector sanitario experimentó el coste medio más elevado por vulneración

El coste de las vulneraciones en el sector sanitario alcanzó un nuevo récord histórico. La media de una vulneración en dicho sector aumentó en casi un millón de dólares y alcanzó los 10,10 millones. Los ataques en el sector sanitario han sido los más costosos durante 12 años consecutivos y han aumentado un 41,6 % desde el informe de 2020. Las organizaciones financieras están en segundo lugar —con una media de 5,97 millones de dólares—, seguidas por las farmacéuticas con 5,01 millones, las tecnológicas con 4,97 millones y las energéticas con 4,72 millones.

9,44 millones de dólares

Coste medio de una infracción en Estados Unidos, más elevado que en ningún otro país

Los cinco países y regiones con la media de costes más alta por vulneraciones de datos fueron Estados Unidos con 9,44 millones de dólares, Oriente Medio con 7,46 millones, Canadá con 5,64 millones, el Reino Unido con 5,05 millones y Alemania con 4,85 millones. Estados Unidos ha estado a la cabeza de la lista durante 12 años consecutivos. Por otra parte, el país con el crecimiento más rápido durante el año pasado fue Brasil, con un aumento del 27,8 %, de 1,08 a 1,38 millones de dólares.

Recomendaciones para minimizar el impacto económico de una vulneración de datos

En esta sección, IBM Security resume los pasos que las organizaciones pueden seguir para reducir el coste económico y reputacional de una vulneración de datos. Las recomendaciones aquí resumidas incluyen medidas de seguridad eficaces que las organizaciones del estudio pusieron en marcha.

Adopte un modelo de seguridad zero trust para prevenir accesos no autorizados a datos confidenciales.
Los resultados del estudio demostraron que, a pesar de que solo el 41 % de las organizaciones había implementado un modelo de seguridad zero trust, esta implementación supuso un ahorro potencial de 1,5 millones de dólares. Cuando las organizaciones incorporan entornos multicloud híbridos y de trabajo remoto, una estrategia zero trust puede ayudarles a proteger los datos y recursos al limitar su accesibilidad y requerir contexto.

Las herramientas de seguridad que pueden compartir datos entre diversos sistemas y centralizar las operaciones de seguridad de datos facilitan a los equipos de seguridad la detección de incidentes en entornos multicloud híbridos complejos. Puede obtener un mayor conocimiento, mitigar riesgos y acelerar la respuesta con una plataforma de seguridad abierta que optimice su estrategia zero trust. Al mismo tiempo, puede usar sus inversiones actuales sin cambiar la ubicación de sus datos, para así potenciar la eficiencia y capacidad de colaboración de su equipo.

Proteja datos confidenciales en entornos de cloud mediante políticas y cifrado.
Con el número y valor cada vez mayores de los datos alojados en entornos de cloud, las organizaciones deberían tomar medidas para proteger sus bases de datos en el cloud. Las buenas prácticas de seguridad de cloud se asociaron con un ahorro de 720 000 dólares en costes por vulnerabilidad. Use el esquema de clasificación de datos y programas de retención para aumentar la visibilidad de la información confidencial vulnerable a ataques y reducir su volumen. Proteja la información confidencial mediante cifrado de datos y cifrado totalmente homomórfico. Usar un marco interno para las auditorías, evaluar los riesgos en la empresa y monitorizar la conformidad con los requisitos de gobierno puede incrementar su capacidad para detectar una vulneración de datos y escalar los esfuerzos para contenerlo.

Invierta en orquestación, automatización y respuesta de seguridad (SOAR) y XDR para mejorar el tiempo de detección y respuesta.
Junto con la IA y automatización de la seguridad, la tecnología XDR contribuye a una reducción significativa del coste medio de la vulneración de datos y sus ciclos de vida. Según el estudio, las organizaciones que implementaron XDR acortaron el ciclo de vida de los ataques en 29 días de media frente a las que no usaron esta tecnología. Gracias a esto ahorraron 400 000 dólares. SOAR y el software de información de seguridad y gestión de eventos (SIEM), la detección gestionada y los servicios de respuesta y XDR pueden ayudar a su organización a acelerar la respuesta a incidentes mediante la automatización, la estandarización de procesos y la integración con sus herramientas de seguridad actuales.

Emplee herramientas que ayuden a proteger y monitorizar los endpoints y los empleados remotos.
En el estudio, cuando el trabajo remoto fue un factor en la causa de vulneraciones, estas costaron casi un millón de dólares más que cuando no lo fue. Los productos y servicios de gestión unificada de endpoints (UEM), detección y respuesta de endpoints (EDR) y gestión de identidad y acceso (IAM) pueden proporcionar una mayor visibilidad de las actividades sospechosas a los equipos de seguridad. Esta supervisión engloba dispositivos BYOD (traiga su propio dispositivo) y los portátiles, ordenadores, tabletas, dispositivos móviles e IoT de la empresa, incluidos los endpoints a los que la organización no tiene acceso físico. UEM, EDR e IAM aceleran el tiempo de investigación y respuesta para aislar y contener el daño en los ataques en los que el trabajo remoto fue un factor.

Cree y evalúe la guía de respuesta a incidentes para aumentar la ciberresiliencia.
Dos de los modos más efectivos para reducir el coste de la vulneración de datos son crear un equipo de respuesta a incidentes (IR) y evaluar en profundidad su plan de acción. Las organizaciones con equipos de IR que comprueban su plan periódicamente ahorraron 2,66 millones de dólares en costes asociados a ataques frente a las que no tienen dicho equipo o no comprueban su plan de acción. Las organizaciones pueden responder rápidamente para contener los efectos de un ataque estableciendo una estrategia de ciberincidentes detallada. Pruebas rutinarias que planean ejercicios de simulación o provocan un ataque en un entorno simulado, como un cyber range.

Los ejercicios de simulación de adversario, también conocidos como ejercicios de equipo rojo, pueden mejorar la efectividad de los equipos de IR al descubrir vías de acceso y técnicas de ataque que podrían pasar por alto e identificar fallas en su capacidad de detección y respuesta. Una solución de gestión de superficie de ataque puede mejorar la posición de seguridad de las empresas al localizar los puntos vulnerables desconocidos con simulaciones de una experiencia de ataque real.

Las recomendaciones para las prácticas de seguridad tienen fines formativos y no garantizan resultados específicos.

Sobre el Instituto Ponemon e IBM Security

Instituto Ponemon

El Instituto Ponemon se dedica a la investigación y formación independientes para mejorar la información responsable y las prácticas de gestión de privacidad en empresas y gobiernos. Nuestra misión es llevar a cabo estudios empíricos de alta calidad sobre temas clave que afectan a la gestión y seguridad de la información confidencial de individuos y organizaciones.

El Instituto Ponemon mantiene una estricta confidencialidad de datos, privacidad y estándares de investigación éticos. Además, no recopila ninguna información que permita la identificación de las personas o empresas participantes en sus estudios. Sus estrictos estándares de calidad también garantizan que los sujetos no sean objeto de preguntas no pertinentes, irrelevantes o inapropiadas.

IBM Security

IBM Security ofrece una de las carteras de productos y servicios de seguridad empresarial más avanzadas e integradas. Dicha cartera, respaldada por el estudio de IBM® Security X-Force reconocido mundialmente, proporciona soluciones de seguridad que ayudan a las organizaciones a integrar la seguridad en su tejido empresarial a fin de prosperar ante la incertidumbre.

IBM dirige una de las organizaciones de investigación, desarrollo y soluciones de seguridad más amplias y rigurosas. IBM, que monitoriza más de 4,7 billones de eventos al mes en más de 130 países, cuenta con más de 10 000 patentes de seguridad. Para saber más, visite ibm.com/es-es/security. Únase a la conversación en la Comunidad de IBM Security.

Si tiene preguntas o comentarios sobre esta investigación, incluido el permiso para citar o reproducir partes del informe, póngase en contacto con nosotros por carta, teléfono o correo electrónico.

Ponemon Institute LLC
A la atención de: Research Department
2308 US 31 North
Traverse City
Michigan 49686 (EE. UU.)

1 800 887 3118
research@ponemon.org

Dé el siguiente paso

Soluciones de seguridad zero trust
Ajuste la seguridad en torno a cada usuario, dispositivo y conexión.
Más información

Gestión de identidad y acceso
Conecte cada usuario, API y dispositivo a cada aplicación de forma segura.
Más información

Seguridad de datos
Descubra, clasifique y proteja los datos empresariales confidenciales.
Más información

Orquestación de seguridad, automatización y respuesta
Acelere la respuesta a incidentes con la orquestación y la automatización.
Más información

Información de seguridad y gestión de eventos
Mejore su visibilidad para detectar amenazas, investigarlas y responder a ellas.
Más información

Seguridad del cloud
Integre la seguridad en su trayecto hacia el multicloud híbrido.
Más información

Seguridad de endpoint
Proteja los dispositivos, usuarios y organizaciones frente a ataques sofisticados.
Más información

Servicios de ciberseguridad
Reduzca el riesgo con servicios de consultoría, cloud y seguridad gestionada.
Más información

Respuesta a incidentes e inteligencia de amenazas
Gestione y responda de forma proactiva a las amenazas de seguridad.
Más información

Programe una consulta individual con un experto de IBM Security X-Force.
Prográmela ahora

IBM España, S.A.
Santa Hortensia, 26-28
28002 Madrid

Producido en los
Estados Unidos de América
Julio de 2022

Este documento está actualizado en la fecha inicial de publicación e IBM puede modificarlo en cualquier momento. No todas las ofertas están disponibles en todos los países en los que opera IBM.

Los datos de rendimiento y ejemplos de clientes mencionados se presentan únicamente con fines ilustrativos. Los datos reales de rendimiento pueden variar en función de las configuraciones y condiciones de funcionamiento específicas. LA INFORMACIÓN DE ESTE DOCUMENTO SE OFRECE «TAL CUAL ESTÁ» SIN NINGUNA GARANTÍA, NI EXPLÍCITA NI IMPLÍCITA, INCLUIDAS, ENTRE OTRAS, LAS GARANTÍAS DE COMERCIABILIDAD, ADECUACIÓN A UN FIN CONCRETO Y CUALQUIER GARANTÍA O CONDICIÓN DE INEXISTENCIA DE INFRACCIÓN. Los productos de IBM están garantizados según los términos y condiciones de los acuerdos bajo los que se proporcionan.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

El cliente es responsable de garantizar el cumplimiento de las leyes y reglamentos aplicables. IBM no presta asesoramiento legal ni declara o garantiza que sus servicios o productos aseguren que el cliente cumpla con cualquier ley o reglamento. Las declaraciones relativas a la dirección e intención futuras de IBM están sujetas a cambios sin previo aviso y solo representan metas y objetivos.