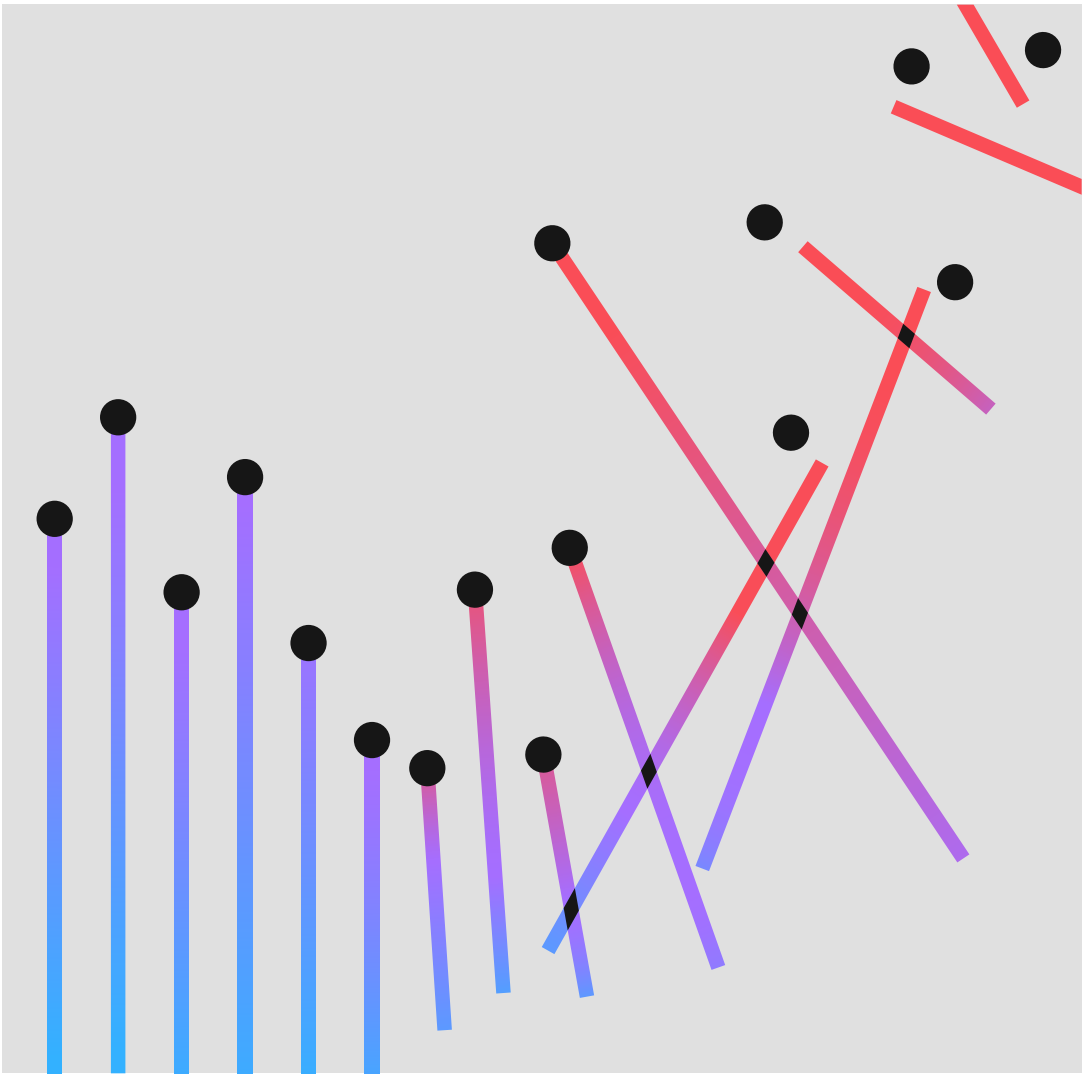
IBM **Security**

Informe del Coste de la vulneración de datos 2022



IBM

Contenido

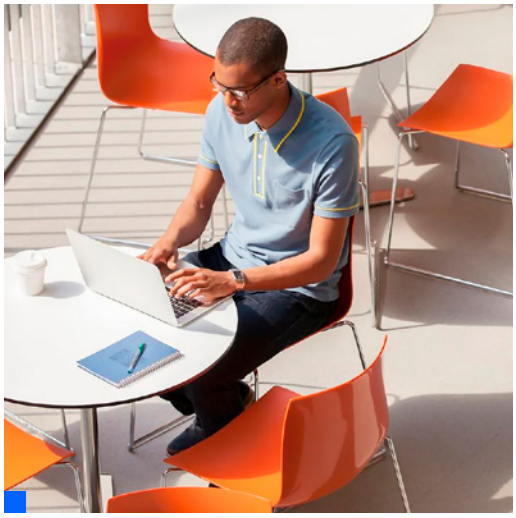
Resumen ejecutivo

El informe “Coste de la Vulneración de Datos” ofrece a los líderes de TI, gestión de riesgos y seguridad, una mirada a los factores que pueden aumentar o ayudar a mitigar el coste creciente de las vulneraciones de datos.

Esta investigación, en su decimoséptimo año, realizada de forma independiente por Ponemon Institute y patrocinada, analizada y publicada por IBM® Security, estudió a 550 organizaciones que se vieron afectadas por vulneraciones de datos, producidas entre marzo de 2021 y marzo de 2022. Las vulneraciones tuvieron lugar en 17 países y regiones y en 17 industrias diferentes.

Realizamos más de 3600 entrevistas con personas de organizaciones que se vieron afectadas por vulneraciones de datos. Durante las entrevistas, quisimos conocer el coste que supone a las organizaciones responder de forma inmediata y prolongada a las vulneraciones de datos.

Como con los informes de años anteriores, los datos de este año ofrecen un panorama de cómo docenas de factores impactan en los costes que aumentan cada vez más después de que se produce una vulneración de datos. Además, el informe examina las causas de fondo, las consecuencias en el corto y largo plazo de las vulneraciones de datos y los factores atenuantes, así como también las tecnologías que permiten que las empresas limiten las pérdidas.



Algo significativo es que por primera vez, la investigación muestra la siguiente información:

83%

de las organizaciones estudiadas han tenido más de una vulneración de datos.

60%

de las vulneraciones de las organizaciones llevaron a aumentos en los precios que se trasladaron a los clientes.

79%

de las organizaciones de infraestructura crucial no implementaron una arquitectura de zero trust.

19%

de las vulneraciones se produjeron debido a que un socio comercial se vio comprometido.

45%

de las vulneraciones fueron en el cloud.

Novedades en el informe de 2022

En la edición de este año, apuntamos a construir sobre la base de la investigación pasada, manteniéndonos actualizados en cuanto a la tecnología y los eventos cambiantes. También intentamos generar una visión general más relevante de los riesgos y las estrategias para proteger los datos y responder a una vulneración, desde la inteligencia artificial (IA) hasta zero trust. La edición de 2022 de este informe, que abarca algunas de las tecnologías en las cuales se han concentrado la mayoría de las empresas durante el último año, tiene un nuevo análisis relacionado con el valor de lo siguiente:

- Detección y respuesta ampliada (XDR).
- El uso de técnicas de clasificación de riesgos.
- Impactos de las tecnologías individuales que contribuyen a una infraestructura de seguridad de zero trust, como gestión de identidad y acceso (IAM), y autenticación multifactorial (MFA).

Asimismo, el informe analiza de forma más amplia algunos de los principales factores que contribuyen a los mayores costes de las vulneraciones de datos. Por primera vez, el informe observa los efectos de los compromisos en la cadena de suministro y la falta de competencias en seguridad.

El informe examina las áreas de vulnerabilidad de la seguridad, desde el cloud hasta la infraestructura crucial. Y profundizamos, más que los años anteriores, en los impactos del ransomware y los ataques destructivos. También se estudia el fenómeno del teletrabajo, que sigue siendo una realidad para muchas organizaciones después de superar el pico de la pandemia de la COVID.

A medida que las empresas experimenten más vulneraciones y los costes sigan aumentando, este informe puede servir como herramienta para ayudar a sus equipos a gestionar mejor el riesgo y limitar las posibles pérdidas.
El informe se divide en las siguientes cinco secciones principales:

- El resumen ejecutivo con los principales hallazgos y las novedades de la edición de 2022.
- El análisis exhaustivo de todos los hallazgos, incluidos los costes de las vulneraciones por región geográfica y sector.
- Las recomendaciones de seguridad de expertos de IBM Security, con base en los resultados de este informe.
- Los datos demográficos de las organizaciones y las definiciones del sector.
- La metodología del estudio, incluyendo cómo se calcularon los costes.

A IBM Security y Ponemon Institute les complace presentar los resultados del informe “Coste de la Vulneración de Datos 2022.”

Principales hallazgos

Los hallazgos clave que se describen aquí se basan en el análisis que hizo IBM Security de los datos de la investigación que recopiló Ponemon Institute.[1]

4,35 millones de dólares

Coste total promedio de una vulneración de datos

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

83%

Porcentaje de organizaciones que han tenido más de una vulneración

El 83% de las organizaciones estudiadas han experimentado más de una vulneración de datos y solo el 17% indicó que se trató de su primera vulneración de datos. El 60% de las organizaciones estudiadas dijeron que habían incrementado el precio de sus productos/servicios debido a la vulneración de datos.

4,82 millones de dólares

Coste promedio de una vulneración de datos de una infraestructura crítica

El coste promedio para las organizaciones estudiadas de una vulneración de datos de infraestructura crucial fue de entre 4,82 millones de dólares y 1 millón de dólares más que el coste promedio para las organizaciones que forman parte de otras industrias. Entre las organizaciones de infraestructura incluidas, están las que prestan servicios en las industrias financiera, industrial, de tecnología, transporte, comunicación, atención médica, formación y sector público. Un 28% experimentó un ataque destructivo o de ransomware, mientras que un 17% sufrió una vulneración porque un socio comercial se vio comprometido.

3,05 millones de dólares

Ahorro promedio de costes, asociado con la IA y la automatización de seguridad totalmente implementadas

Las vulneraciones en las organizaciones con IA y automatización de seguridad totalmente implementadas cuestan 3,05 millones de dólares menos que las vulneraciones en organizaciones sin IA ni automatización de seguridad implementadas. Esta diferencia del 65,2% en el coste promedio de las vulneraciones (entre 3,15 millones de dólares para las que tienen un despliegue total, versus 6,20 millones de dólares para las que no tienen despliegue), representa el mayor ahorro de costes recogido en el estudio. Las empresas con IA y automatización de seguridad totalmente implementadas, también tuvieron, en promedio, un plazo de 74 días menos hasta identificar y contener la vulneración, conocido como el ciclo de vida de la vulneración, que aquellas sin IA y automatización de seguridad: 249 días en comparación con 323 días. El uso de IA y automatización de seguridad tuvo un incremento en dos años, pasando del 59% en 2020 al 70% en 2022.

1. Los importes de los costes en este informe se miden en dólares estadounidenses (USD).

4,54 millones de dólares

Coste promedio de un ataque de ransomware, sin incluir el coste del cibersecuestro en sí.

El 11% de las vulneraciones contempladas en el estudio fueron ataques de ransomware. Lo que con respecto al 2021, año en el que un 7,8% de las vulneraciones fueron de ransomware, representa un crecimiento del 41%. El coste promedio de un ataque de ransomware disminuyó levemente, pasando de 4,62 millones de dólares en 2021, a 4,54 millones de dólares en 2022. Este coste fue levemente superior que el coste total promedio global de una vulneración de datos, 4,35 millones de dólares.

19%

Frecuencia de las vulneraciones causadas por credenciales robadas o comprometidas.

El uso de credenciales robadas o comprometidas sigue siendo la causa más común de la vulneración de datos. Las credenciales robadas o comprometidas fueron el principal vector de ataque en el 19% de las vulneraciones contempladas en el estudio de 2022. También fueron el principal vector de ataque en el estudio de 2021, año en el que causaron un 20% de las vulneraciones. Las vulneraciones causadas por credenciales robadas o comprometidas tuvieron un coste promedio de 4,50 millones de dólares. Estas vulneraciones tuvieron el ciclo de vida más prolongado: identificar la vulneración tomó 243 días y se necesitaron otros 84 días para contenerla. El phishing fue la segunda causa más común de una vulneración, con un 16% y también la más costosa, con un promedio de 4,91 millones de dólares en costes.

59%

Porcentaje de organizaciones que no implementan zero trust.

Solo un 41% de las organizaciones del estudio indicaron que implementaron una arquitectura de seguridad de zero trust. El 59% de las organizaciones que no implementaron zero trust incurren en un promedio de 1 millón de dólares más en costes de vulneración, en comparación con las que sí lo hicieron. Entre las organizaciones de infraestructura crucial, un porcentaje todavía mayor, el 79%, no había implementado zero trust. Estas organizaciones experimentaron un promedio de 5,40 millones de dólares en costes de vulneración, por encima de 1 millón de dólares más que el promedio global.

1 millón de dólares

Diferencia promedio en el coste, en los casos en el que teletrabajo fue un factor causante de la vulneración, en comparación con los casos en los que no lo fue.

En los casos en los que el teletrabajo fue uno de los factores causantes de la vulneración, los costes alcanzaron un promedio de casi 1 millón de dólares más que en las vulneraciones en las que el teletrabajo no fue un factor: 4,99 millones de dólares versus 4,02 millones de dólares. Las vulneraciones relacionadas con el teletrabajo cuestan de promedio aproximadamente 600.000 dólares más, comparadas con el promedio global.

45%

Porcentaje de vulneraciones producidas en el cloud.

El 45% de las vulneraciones del estudio se produjeron en el cloud. No obstante, las vulneraciones que se produjeron en un entorno de cloud híbrido cuestan un promedio de 3,80 millones de dólares, en comparación con 4,24 millones de dólares en las clouds privados y 5,02 millones de dólares para las vulneraciones en clouds públicos. La diferencia en el coste entre las vulneraciones del cloud híbrido y las vulneraciones del cloud público fue del 27,6%. Las organizaciones con un modelo de cloud híbrido también tuvieron ciclos de vida más cortos para las vulneraciones que las organizaciones que solamente adoptaron un modelo de cloud público o privado.

2,66 millones de dólares

Ahorro promedio en costes asociados, con un equipo de respuesta a incidencias (RI) y un plan de RI probado regularmente

Casi tres cuartas partes de las organizaciones del estudio indicaron que tenían un plan de RI, mientras que solo el 63% de esas organizaciones dijeron que ponían a prueba regularmente el plan. Tener un equipo de RI y un plan de RI que se pruebe de forma regular, llevó a lograr un ahorro significativo en los costes. Las empresas con un equipo de respuesta a incidencias que pruebe su plan de RI observan un promedio de 2,66 millones de dólares menos en costes que las organizaciones sin un equipo de RI o que teniéndolo, no prueban el plan de RI. La diferencia entre 3,26 millones de dólares y 5,92 millones de dólares representa un ahorro de costes del 58%.

29 días

El ahorro en el tiempo de respuesta para los que cuentan con tecnologías de detección y respuesta ampliada (XDR)

Un 44% de las organizaciones implementaron las tecnologías de XDR. Estas organizaciones con tecnologías de XDR disfrutan de beneficios considerables en los tiempos de respuesta. Aquellas organizaciones que desplegaron XDR, acortaron el ciclo de vida de la vulneración en aproximadamente un mes, de promedio, en comparación con las organizaciones que no implementaron XDR. Más concretamente, las organizaciones invirtieron 275 días en identificar y contener una vulneración con XDR implementado en comparación con los 304 días sin XDR implementado. Esta cifra representa una diferencia del 10% en los tiempos de respuesta.

12 años

Los años consecutivos durante los que la industria de la atención médica ha tenido el coste promedio más alto de una vulneración

Los costes de las vulneraciones en el entorno de la atención médica han alcanzado un nuevo récord. La vulneración promedio en el sector de la atención médica aumentó casi en 1 millón de dólares, hasta alcanzar los 10,10 millones de dólares. Los costes de las vulneraciones en la industria de la atención médica han sido los más costosos durante 12 años seguidos, con un aumento del 41,6% desde el informe de 2020. Las organizaciones financieras tuvieron el segundo nivel de costes más altos, promediando 5,97 millones de dólares, seguidas de las farmacéuticas con 5,01 millones de dólares, tecnología con 4,97 millones de dólares y energía con 4,72 millones de dólares.

9,44 millones de dólares

Coste promedio de una vulneración en los Estados Unidos, el mayor en cualquier país

Los cinco países y regiones principales con el coste promedio más alto para una vulneración de datos fueron: Estados Unidos con 9,44 millones de dólares, Oriente Medio con 7,46 millones de dólares, Canadá con 5,64 millones de dólares, Reino Unido con 5,05 millones de dólares y Alemania con 4,85 millones de dólares. Estados Unidos ha liderado esta lista durante 12 años consecutivos. Por otro lado, el país con la tasa de crecimiento más rápida durante el último año fue Brasil, con un aumento del 27,8%, pasando de 1,08 millones de dólares a 1,38 millones de dólares.

Todos los hallazgos

En esta sección, proporcionamos los hallazgos detallados de este informe en 16 temas.
Los temas se presentan en el siguiente orden:

- Lo más destacado a nivel global
- Ciclo de vida de la vulneración de datos
- Vectores iniciales del ataque
- Principales factores de los costes
- IA y automatización de la seguridad
- Tecnologías de XDR
- Respuesta a incidencias
- Clasificación de riesgos
- Zero trust
- Ransomware y ataques destructivos
- Ataques a la cadena de suministro
- Infraestructura crucial
- Vulneraciones en el cloud y modelo de cloud
- Teletrabajo
- Falta de competencias
- Megavulneraciones

4,35 millones de dólares

Coste total promedio global de una vulneración de datos

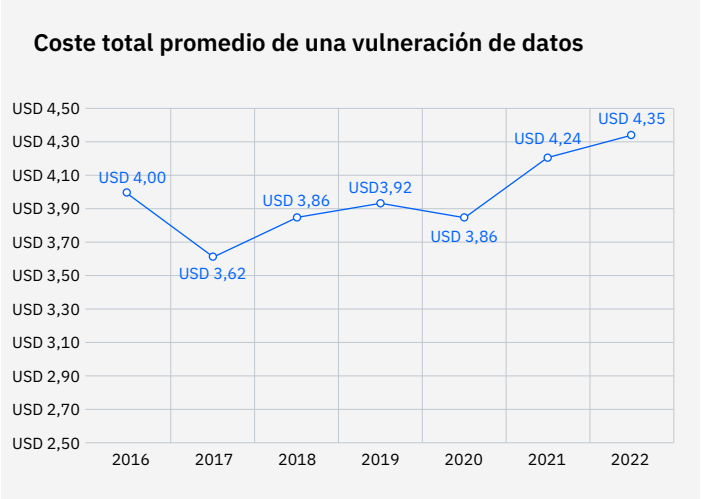


Figura 1: Medido en millones de dólares

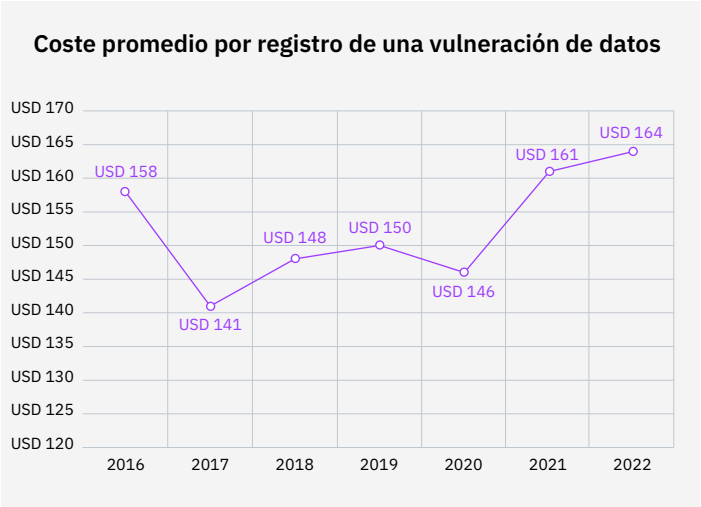


Figura 2: Medido en USD

Lo más destacado a nivel global

El informe Coste de la vulneración de datos es global incluye datos de 17 países y regiones y 17 industrias. En esta sección, observamos varias métricas clave a nivel del promedio global, así como costes comparativos entre países y entre industrias.

Figura 1: El coste promedio de una vulneración de datos alcanzó un récord máximo en 2022.
El coste total promedio global de una vulneración de datos aumentó en 110.000 dólares hasta los 4,35 millones de dólares en 2022, el valor más alto que se ha alcanzado históricamente en este informe. El aumento de los 4,24 millones de dólares del informe de 2021 a los 4,35 millones de dólares en el informe de 2022, representa un incremento del 2,6%. En los últimos dos años, el coste total promedio ha aumentado un 12,7% con respecto a los 3,86 millones de dólares del informe de 2020.

Figura 2: El coste por registro de una vulneración de datos alcanzó el valor máximo en los últimos siete años.
El coste global por registro de una vulneración de datos en 2022 fue de 164 dólares, un aumento del 1,9% con respecto a los 161 dólares en 2021. El aumento con respecto a los 146 dólares en 2020 supone un incremento del 12,3%. Este estudio examina las vulneraciones que tienen una magnitud de entre 2200 y 102.000 registros. No se contempla con esta investigación el uso del coste por registro para calcular el coste de una vulneración o varias cuando se sobrepasan 102.000 registros. Para obtener más información, consulte la sección “Metodología de investigación”.

Coste promedio de una vulneración de datos por país o región

Figura 3: Medido en millones de dólares

Figura 3: Estados Unidos fue el país con mayores costes promedio en una vulneración de datos por duodécimo año consecutivo. Los cinco países o regiones principales con el coste promedio más alto de una vulneración de datos fueron:

1. Estados Unidos: 9,44 millones de dólares
2. Oriente Medio: 7,46 millones de dólares
3. Canadá: 5,64 millones de dólares
4. Reino Unido: 5,05 millones de dólares
5. Alemania: 4,85 millones de dólares

Estados Unidos tuvo el coste promedio mayor de una vulneración de datos con 9,44 millones de dólares, lo que representa un aumento del 4,3% o de 390.000 dólares, con respecto a los 9,05 millones de dólares en 2021. De forma similar al año anterior, la región de Medio Oriente volvió a tener el segundo coste total promedio más alto de una vulneración de datos, pasando de 6,93 millones de dólares en 2021 a 7,46 millones de dólares en 2022. Este coste promedio tuvo un aumento de 530.000 dólares, un 7,6%. Canadá fue nuevamente el tercer país con coste más alto, con 5,64 millones de dólares, un aumento de 240.000 dólares, un 4,4%. Reino Unido subió al puesto número cuatro, desde el octavo que ocupaba de los 17 países o regiones, superando a Alemania, Japón y Francia en la clasificación. El coste total promedio de una vulneración en Reino Unido fue de 5,05 millones de dólares, lo que respecto a 4,67 millones de dólares, supone un incremento de 380.000 dólares, un 8,1 %.

De los 17 países o regiones estudiados, seis (Alemania, Japón, Francia, Corea del Sur, Escandinavia y Turquía) observaron una disminución en el coste total promedio de una vulneración de datos. Brasil, que ocupa el puesto decimosexto en la lista con 1,38 millones de dólares, vio el mayor aumento relativo en el coste, incrementado en 300.000 dólares, un 27,8%. Turquía, en el puesto decimoséptimo de la lista, tuvo la mayor disminución relativa en el coste, pasando de 1,91 millones de dólares a 1,11 millones de dólares, una reducción de 800.000 dólares, un 42%. Las grandes oscilaciones en los valores de la moneda, como las producidas en Turquía, pueden influir en las variaciones de los costes de un año al otro.

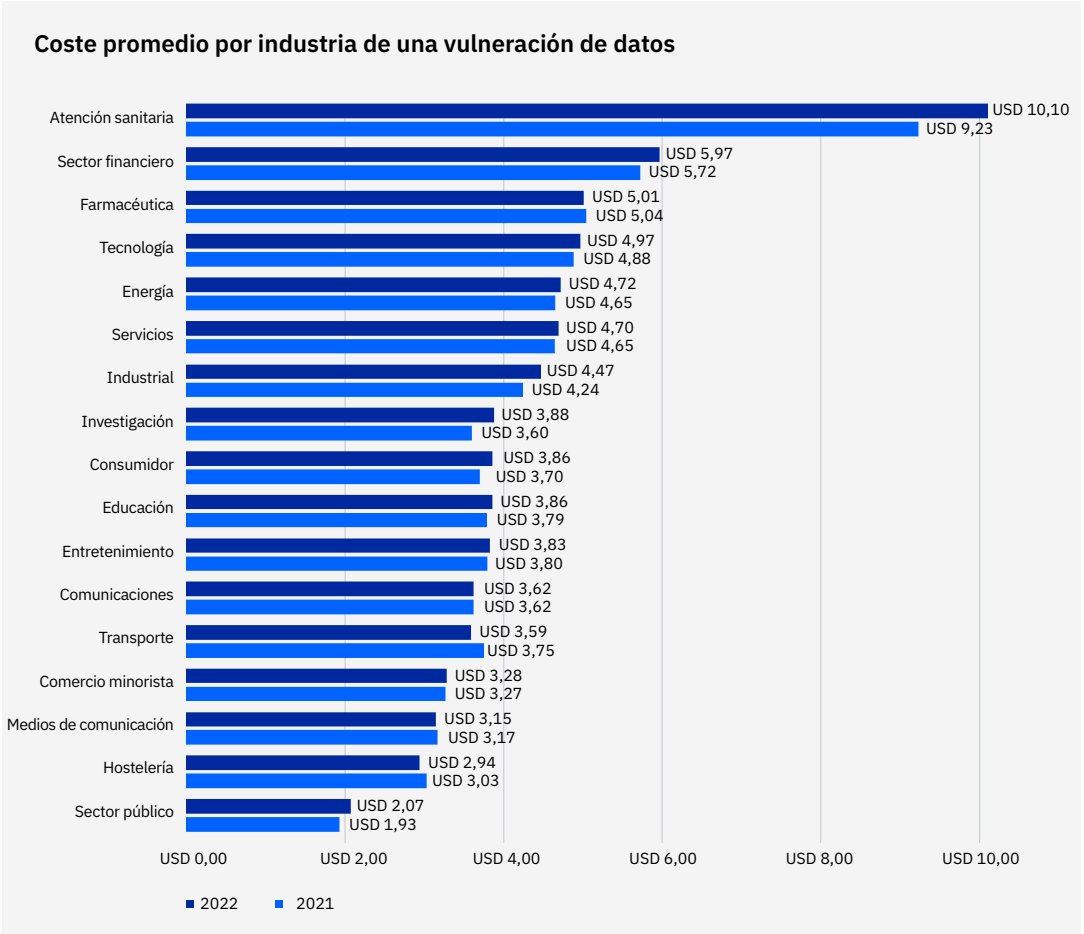


Figura 4: Medido en millones de dólares

La atención sanitaria es una de las industrias más reglamentadas y el Gobierno estadounidense la considera una infraestructura crucial.

Figura 4: La atención sanitaria fue la industria con el coste más alto por duodécimo año consecutivo.
El coste total promedio de una vulneración en el ámbito de la atención sanitaria aumentó de 9,23 millones de dólares en el informe de 2021 a 10,10 millones de dólares en 2022, lo cual representa un incremento de 870.000 dólares, un 9,4%. La atención sanitaria es una de las industrias más reglamentadas y el Gobierno estadounidense la considera una infraestructura crucial.

Las cinco industrias principales por coste permanecieron sin cambios en cuanto al orden de la clasificación realizada en el informe de 2021. Después de la industria de la atención sanitaria se colocan la financiera, farmacéutica, tecnología y energía. El sector financiero observó un aumento de 5,72 millones de dólares en 2021 a 5,97 millones de dólares en 2022, un incremento de 250 000 dólares, un 4,4%. El sector industrial, que incluye organizaciones de química, ingeniería y fabricación, tuvo un aumento de 4,24 millones de dólares a 4,47 millones de dólares en 2022. Es decir, un incremento de 230.000 dólares, un 5,4%. El coste total promedio disminuyó levemente en cuatro industrias: farmacéutica, transporte, medios de comunicación y hostelería.

Figura 5: Los costes de detección y escalamiento superaron los costes por pérdida de negocio, como la mayor de las cuatro categorías de costes que conforman el coste de una vulneración de datos por primera vez en seis años.

Si dividimos en cuatro categorías de costes, pérdida de negocios, detección y escalamiento, notificación y respuesta posterior a la vulneración, la mayor proporción de los costes de vulneración de datos en 2022 la tuvo la detección y escalamiento. Los costes de detección y escalamiento aumentaron de 1,24 millones de dólares en 2021 a 1,44 millones de dólares en 2022. Es decir, un aumento de 200.000 dólares, un 16,1%. Los costes de detección y escalamiento incluyen actividades que permiten que la empresa detecte razonablemente una vulneración. Estos costes incluyen actividades forenses y de investigación, servicios de auditoría y evaluación, gestión de crisis, y comunicaciones con ejecutivos y juntas.

Por primera vez en al menos seis años, la pérdida de negocios, con 1,42 millones en 2022, no fue la mayor proporción de costes de la vulneración de datos. Los costes de pérdida de negocios disminuyeron de los 1,59 millones en 2021, en un 10,7%. Los costes de pérdida de negocios incluyen actividades que intentan minimizar la pérdida de clientes, la interrupción de los negocios y las pérdidas de ingresos. Estos costes incluyen la interrupción de los negocios y las pérdidas de ingresos producidos por el tiempo de inactividad del sistema, el coste de la pérdida de clientes y la adquisición de clientes nuevos, la pérdida de reputación y la disminución del fondo comercial.

Los costes de notificación y los costes de respuesta posterior a la vulneración permanecieron relativamente sin cambios entre 2021 y 2022. Consulte “Cómo calculamos el coste de una vulneración de datos”, en la sección “Metodología de investigación”, para ver las definiciones de cada una de las cuatro categorías de costes.

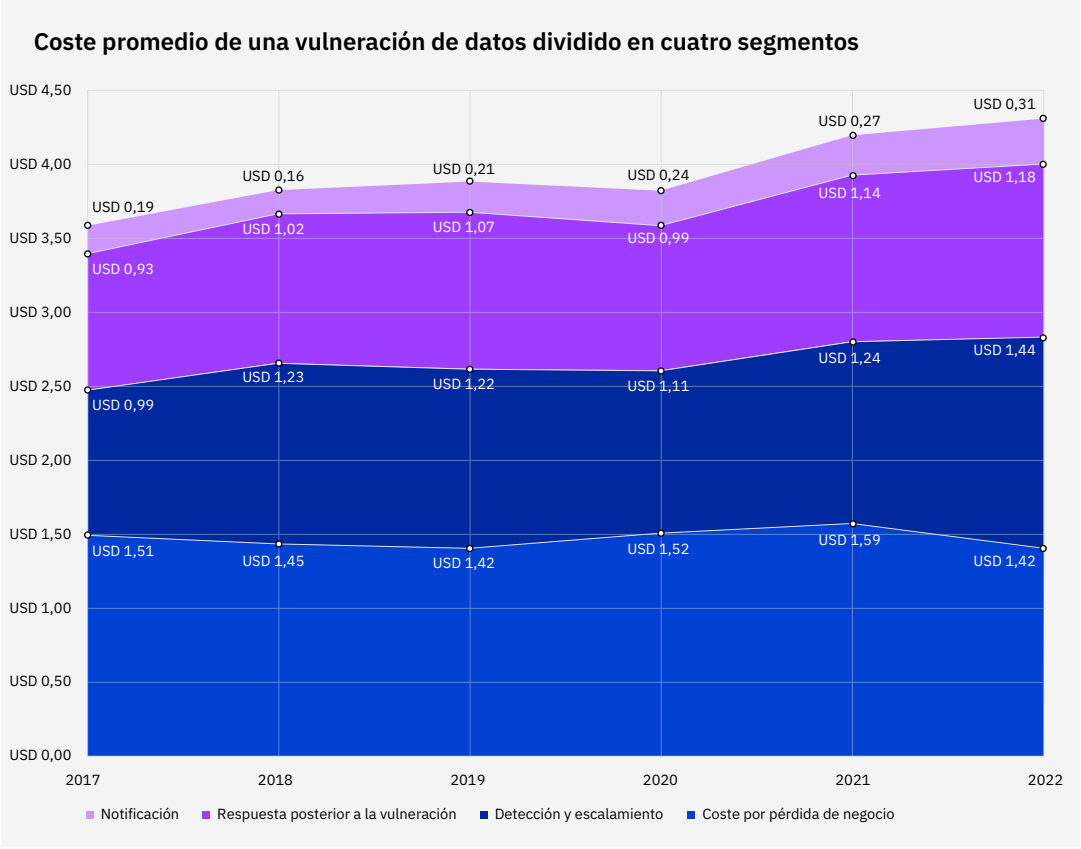


Figura 5: Medido en millones de dólares

¿Fue esta su primera violación de datos?

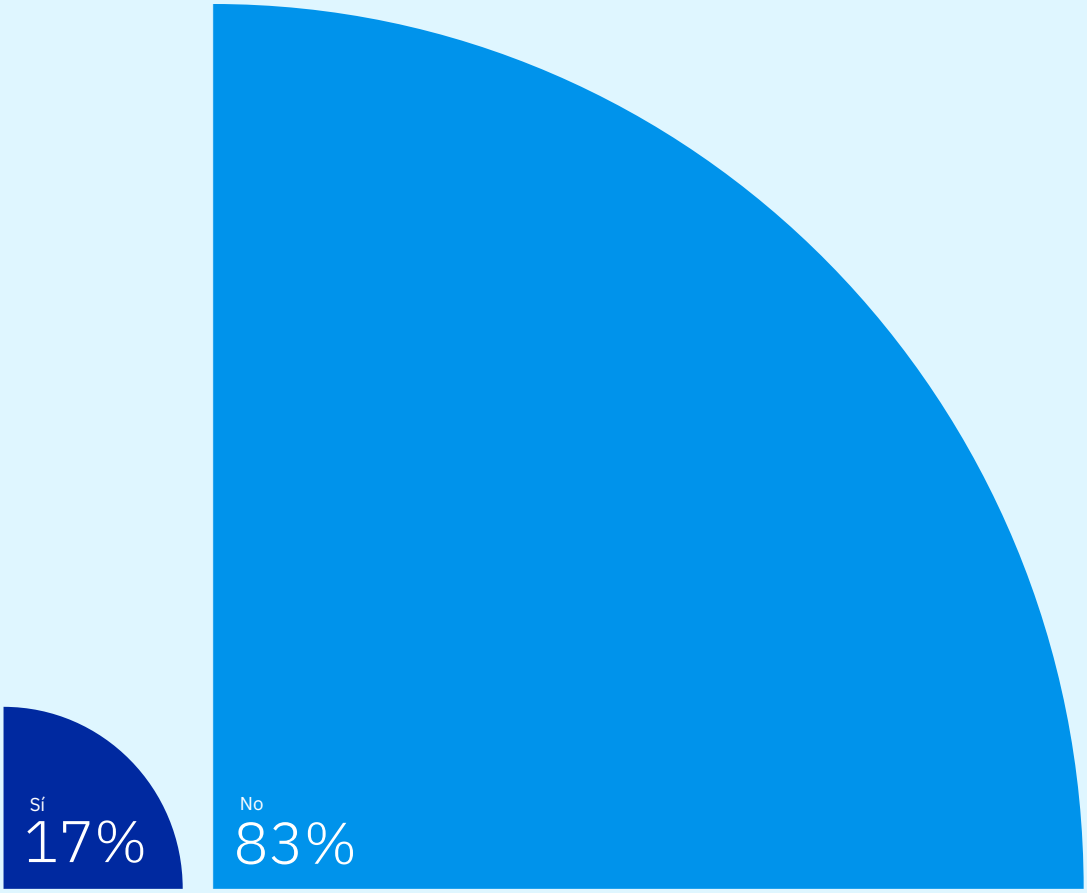


Figura 6

Figura 6: La mayoría de las organizaciones contempladas en el estudio han experimentado más de una vulneración de datos.
De las 550 organizaciones del estudio, solo un 17% indicó que esta fue su primera vulneración de datos. Un 83% dijo que esta no fue su primera vulneración de datos. Con equipos de seguridad que gestionan más incidencias cada año, y considerando el impacto del teletrabajo en la seguridad, es probable que esté aumentando la recurrencia de las vulneraciones.

Figura 7: La mayoría de las organizaciones del estudio indicaron que aumentaron el precio de sus productos y servicios como resultado de la vulneración de datos.
En respuesta a la pregunta, un 60% dijo que aumentaron los precios y un 40% indicó que no.

¿La vulneración de datos hizo que su organización aumentara el precio de productos y servicios?

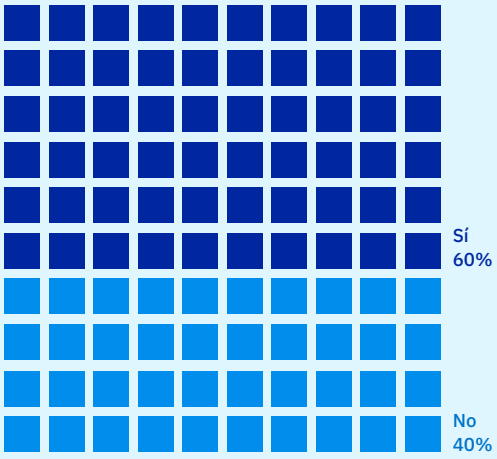


Figura 7

277 días

Tiempo promedio hasta identificar y contener una vulneración de datos

Ciclo de vida de la vulneración de datos

El tiempo transcurrido entre la primera detección de la vulneración y su contención se conoce como el ciclo de vida de la vulneración de datos. El tiempo para identificar una vulneración describe el tiempo que lleva detectar que se ha producido un incidente. El tiempo para contener una vulneración hace referencia al tiempo que le toma a la organización resolver una situación cuando se ha detectado y, finalmente, restaurar el servicio. Estas métricas pueden usarse para determinar la eficacia de los procesos de respuesta a incidencias y contención de una organización.

Figura 8: El tiempo medio hasta identificar y contener una vulneración de datos disminuyó de 287 días en 2021 a 277 días en 2022. Es decir, una reducción de 10 días, un 3,5%.
En 2022, fue necesario un promedio de 207 días para identificar la vulneración y 70 días para contenerla. En 2021, se necesitó un promedio de 212 días para identificar la vulneración y 75 días para contenerla. El promedio de 277 días en 2022 implica que si se produjo una vulneración el 1 de enero, llevó hasta el 4 de octubre de ese año identificarla y contenerla. El promedio de 277 días guarda coherencia con el promedio de los últimos siete años, con una diferencia máxima de un 11% entre el total más bajo, 257 días en 2017, y el total más alto, 287 días en 2021.

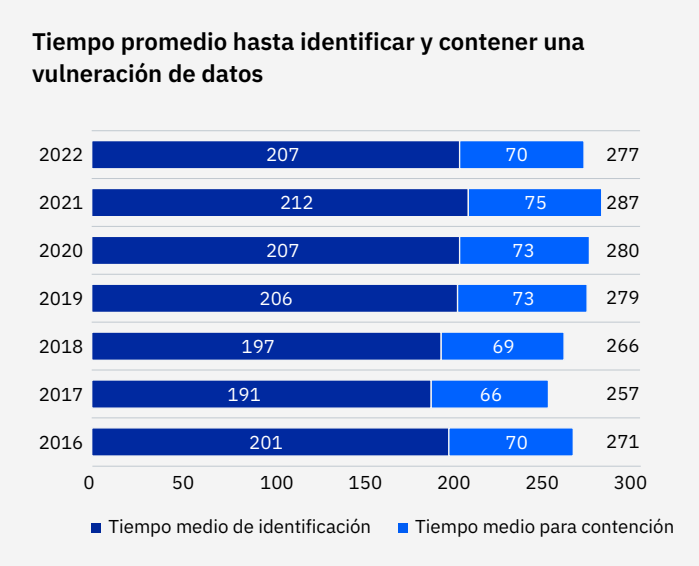


Figura 8 Medido en días

Figura 9: Un ciclo de vida de la vulneración de datos más corto sigue estando asociado con menores costes de la vulneración de datos. Un ciclo de vida de la vulneración de datos de menos de 200 días se asoció con un coste promedio de 3,74 millones de dólares en 2022, en comparación con 4,86 millones de dólares para las vulneraciones con un ciclo de vida de más de 200 días. Esta diferencia representa un ahorro promedio de costes de 1,12 millones de dólares, o del 26,5%, para las vulneraciones con un ciclo de vida de menos de 200 días.

La diferencia entre los costes entre un ciclo de vida de más de 200 días y un ciclo de vida de menos de 200 días fue menor en 2022 que en 2021, cuando fue de 1,26 millones de dólares. La diferencia entre costes en 2022, 1,12 millones de dólares, tiene la misma magnitud que la diferencia entre costes de 2020. La diferencia entre costes ha aumentado levemente durante los últimos siete años, mientras que el coste promedio de una vulneración de datos también se ha incrementado gradualmente. La diferencia entre costes en 2021 de 1,26 millones de dólares fue la mayor de los últimos siete años.

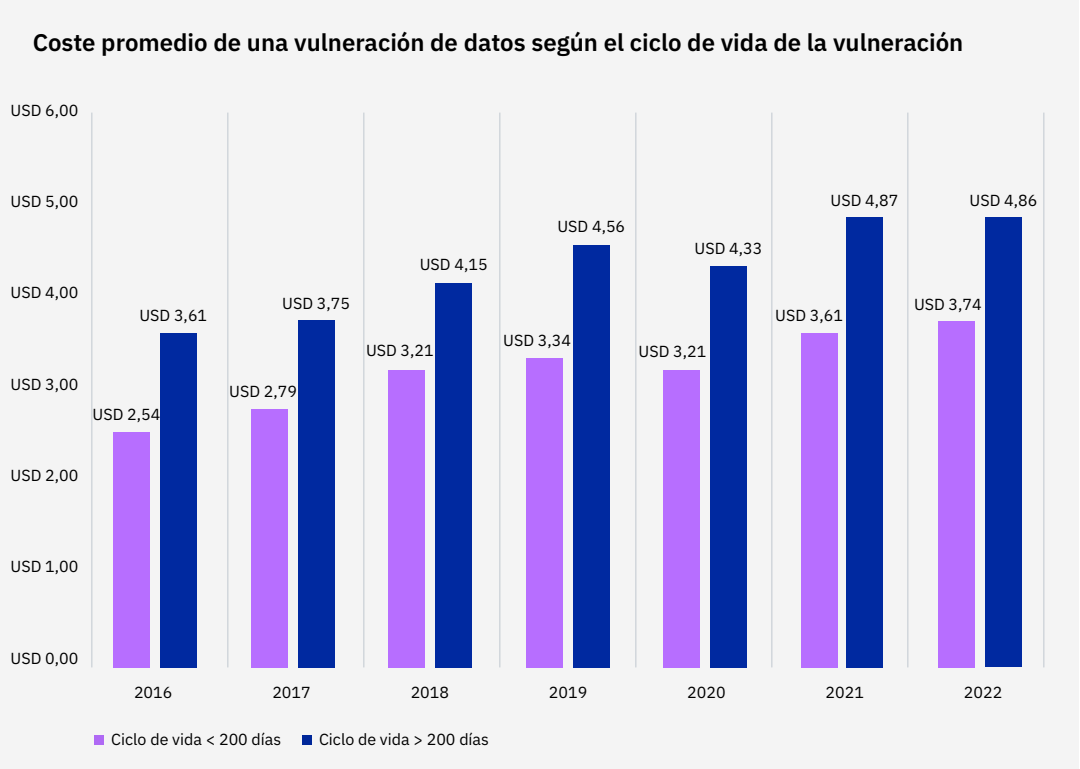


Figura 9: Medido en millones de dólares. La suma de los días para identificarla y los días para contenerla equivale al ciclo de vida de la vulneración

Tiempo transcurrido	Porcentaje del coste total		
	Promedio de 2022	Bajo	Alto
Primer año	52%	66%	45%
Segundo año	29%	26%	31%
Dos años o más	19%	8%	24%

Figura 10a

Figuras 10a y 10b: Las vulneraciones de datos en entornos con mucha normativa de protección de los mismos, como las industrias de la atención sanitaria, finanzas, energía, farmacéutica y formación, vieron cómo se generaban costes en los años posteriores a la vulneración. La diferencia entre entornos con un nivel normativo bajo o alto, apareció de forma pronunciada dos años o más, después de la vulneración de datos: los costes "en el largo plazo". En las industrias altamente reglamentadas, un promedio del 24% de los costes de la vulneración de datos se generó más de dos años después de que se produjera la vulneración. Este resultado es comparable, con un promedio del 8% de los costes generados más de dos años después de una vulneración, en los entornos con bajo nivel normativo.

En los entornos no muy reglamentados, los costes de la vulneración de datos tendieron a acumularse entre los primeros tres y seis meses, período en el que se generó un promedio del 24% de los costes de la vulneración de datos. En el promedio global para 2022, el 52% de los costes se acumularon los primeros 12 meses, el 29% en el segundo año tras la vulneración y el 19%, más de dos años después de la vulneración. Para las industrias con un alto nivel de reglamentación, el 45% de los costes se acumuló en el primer año, el 31% en el segundo, y el 24% más de dos años después de la vulneración.

En el análisis de las industrias en los sectores muy reglamentadas, concluimos que los costes normativos y legales pueden contribuir a los mayores costes en los años posteriores a la vulneración.

Nota: este análisis está formado por un grupo de 218 empresas con datos históricos de vulneraciones anteriores.

Distribución promedio en el transcurso del tiempo, de los costes de la vulneración de datos en entornos de nivel de regulación de datos bajo vs alto

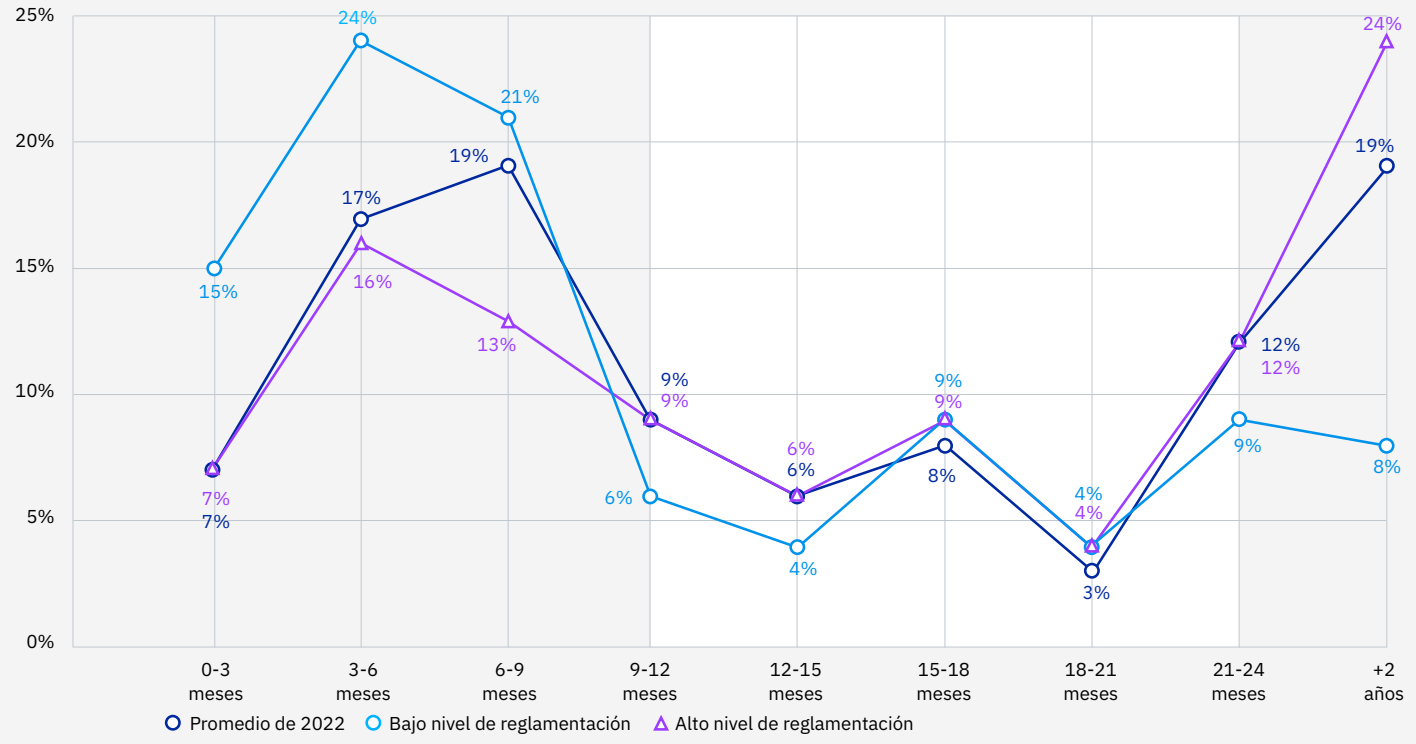


Figura 10b: Porcentaje de costes totales acumulados en intervalos de tres meses

4.91 millones de dólares

Coste promedio de la vulneración de datos con un vector de ataque inicial de phishing

Vectores iniciales del ataque

Esta sección analiza la prevalencia y el coste de los vectores de ataque iniciales en las vulneraciones de datos. Las vulneraciones en el estudio, se dividen en 10 vectores de ataque iniciales, que van desde pérdida accidental de datos y configuración incorrecta del cloud, hasta phishing, amenazas internas y credenciales robadas o comprometidas. Esta sección también compara el tiempo promedio que lleva identificar y contener vulneraciones, dependiendo de su vector de ataque inicial.

Figura 11: El vector de ataque inicial más común en 2022 fueron las credenciales robadas o comprometidas, el cual fue responsable de un 19% de las vulneraciones en el estudio, con un coste promedio de 4,50 millones de dólares.
En 2022, los vectores de ataque iniciales más comunes fueron las credenciales comprometidas en un 19% de las vulneraciones, el phishing en un 16%, la configuración incorrecta del cloud en un 15%, y la vulnerabilidad en software de terceros en un 13%. En el informe de 2021 se vio el mismo orden de los cuatro vectores principales.

El vector de ataque inicial más costoso en 2022, en promedio, fue el phishing con 4,91 millones de dólares. Después del phishing, estuvo el ver comprometido el correo empresarial, con 4,89 millones de dólares y un 6% de las vulneraciones, la vulnerabilidad en software de terceros con 4,55 millones de dólares y las credenciales comprometidas con 4,50 millones de dólares.

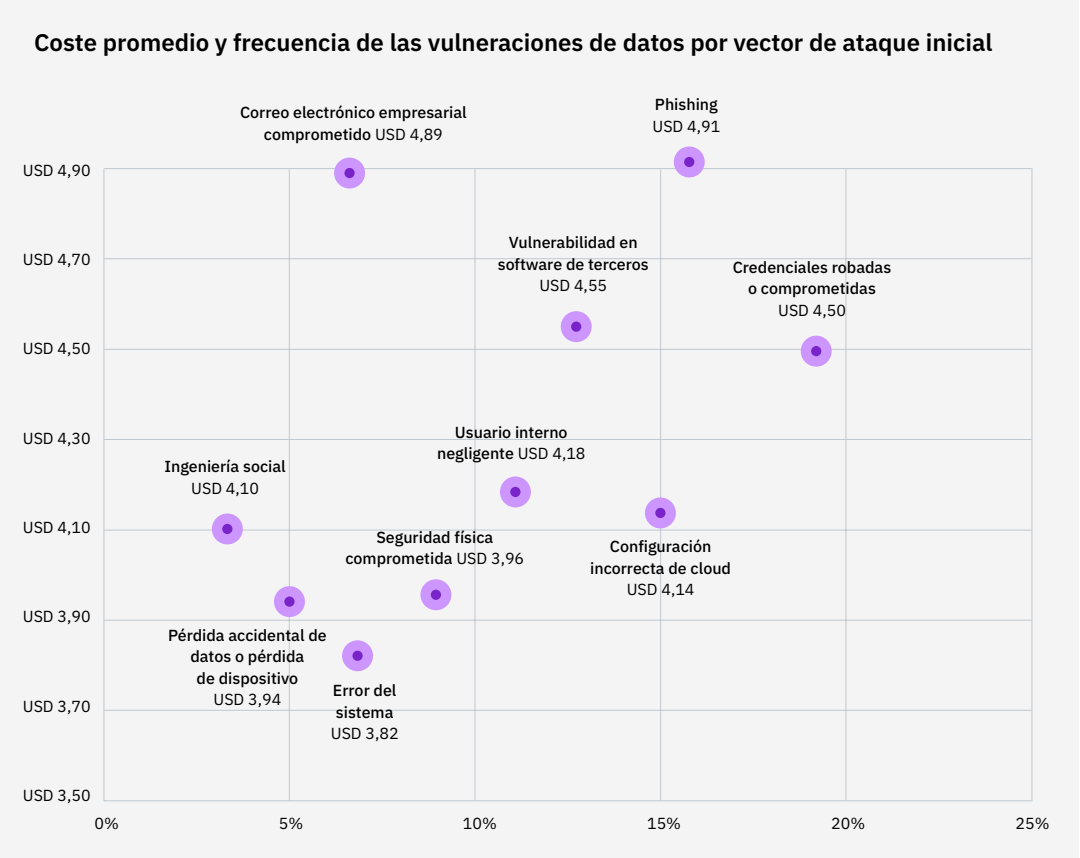


Figura 11: Medido en millones de dólares

Figura 12: Los vectores de ataque con tiempos medios más prolongados para identificar y contener, como el phishing o el compromiso del correo electrónico empresarial, también estuvieron entre las formas más costosas de vulneraciones.
Las credenciales robadas o comprometidas, fueron el vector de ataque inicial con el tiempo medio más prolongado hasta identificar y contener la vulneración, con 327 días. Ese tiempo es un 16,6% mayor que el tiempo medio general hasta identificar y contener una vulneración de datos. Las credenciales comprometidas también fueron el vector de ataque inicial más común, un 19% de las vulneraciones de datos en el estudio.

Las vulneraciones causadas por un compromiso del correo electrónico empresarial, tuvieron el segundo tiempo medio más alto hasta identificar y contener, con 308 días. El compromiso del correo electrónico empresarial fue el segundo vector de ataque inicial más costoso, con vulneraciones que costaron un promedio de 4,89 millones de dólares. Las vulneraciones causadas por phishing tuvieron el tercer tiempo medio más alto hasta identificar y contener la vulneración con 295 días, y tuvieron el mayor coste promedio con 4,91 millones de dólares. La vulnerabilidad en software de terceros tuvo el cuarto tiempo medio más alto hasta identificar y contener la vulneración, con un promedio que superó el promedio general: 284 días versus 277 días.

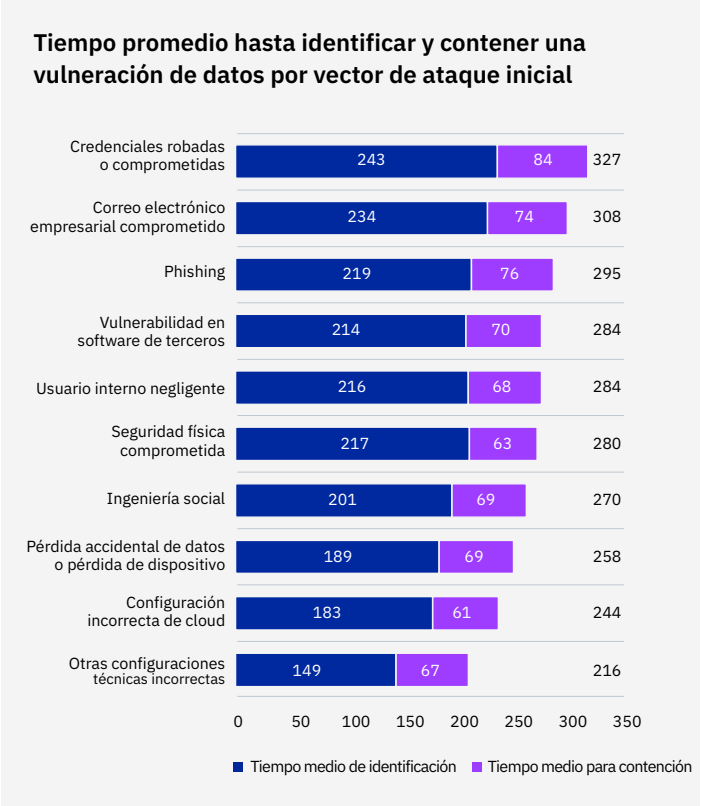


Figura 12: Medido en días

5,57 millones de dólares

Coste promedio de una vulneración para organizaciones con altos niveles de incumplimiento

Principales factores de los costes

Esta sección analiza los múltiples factores que influyen en el coste de una vulneración de datos, además de varios tipos de tecnologías y prácticas de seguridad. Un análisis especial a 28 factores de coste examina su impacto en el coste medio de una vulneración de datos. Estos 28 factores estuvieron asociados con costes de vulneración inferiores al promedio, derivados de una influencia reductora, o con costes de vulneración superiores al promedio, derivados de una influencia amplificadora.

Los siguientes factores de costes aparecen por primera vez en el informe de este año: gestión de identidad y acceso (IAM); tecnologías de XDR; autenticación de múltiples factores (MFA), y equipos de gestión de crisis.

Estos factores de costes no son acumulables, por lo que no es coherente para esta investigación sumar varios factores de coste para calcular el coste de una vulneración.

La figura 13 muestra el impacto de 28 factores en el coste promedio de una vulneración de datos.
El gráfico muestra la diferencia en el coste promedio de las vulneraciones en organizaciones con estos factores que influyen en el coste, en comparación con el coste medio de una vulneración de datos de 4,35 millones de dólares. El gráfico se divide en los factores que están asociados con un coste de vulneración inferior al promedio, que son mitigantes de costes, y en aquellos factores que están asociados con un coste de vulneración superior al promedio, que amplifican los costes.

Las plataformas de IA, el método DevSecOps y el uso de un equipo de respuesta a incidencias (RI) fueron los tres factores asociados con la disminución de costes más alta en comparación con el coste medio de una vulneración. Por ejemplo, las vulneraciones en organizaciones con plataformas de IA tuvieron un coste promedio de 300.075 dólares menos que el coste medio de una vulneración de datos de 4,35 millones de dólares en empresas sin plataformas de IA. Es decir, aproximadamente 4,05 millones de dólares.

Por otro lado, la complejidad del sistema de seguridad, el proceso de migración al cloud de la organización y los incumplimientos fueron los tres factores asociados con el aumento neto más alto en el coste promedio. Por ejemplo, las vulneraciones en organizaciones con complejidad en el sistema de seguridad tuvieron un coste promedio de 4,35 millones de dólares, 290.655 dólares menos que el coste medio de 4,64 millones de dólares.

Por primera vez, el informe de este año midió el impacto de los siguientes cuatro nuevos factores de coste: gestión de identidad y acceso (IAM); tecnologías de XDR; autenticación de múltiples factores (MFA) y equipos de gestión de crisis. Cada uno de estos factores está asociado con costes de vulneración inferiores al promedio, liderados por la IAM.

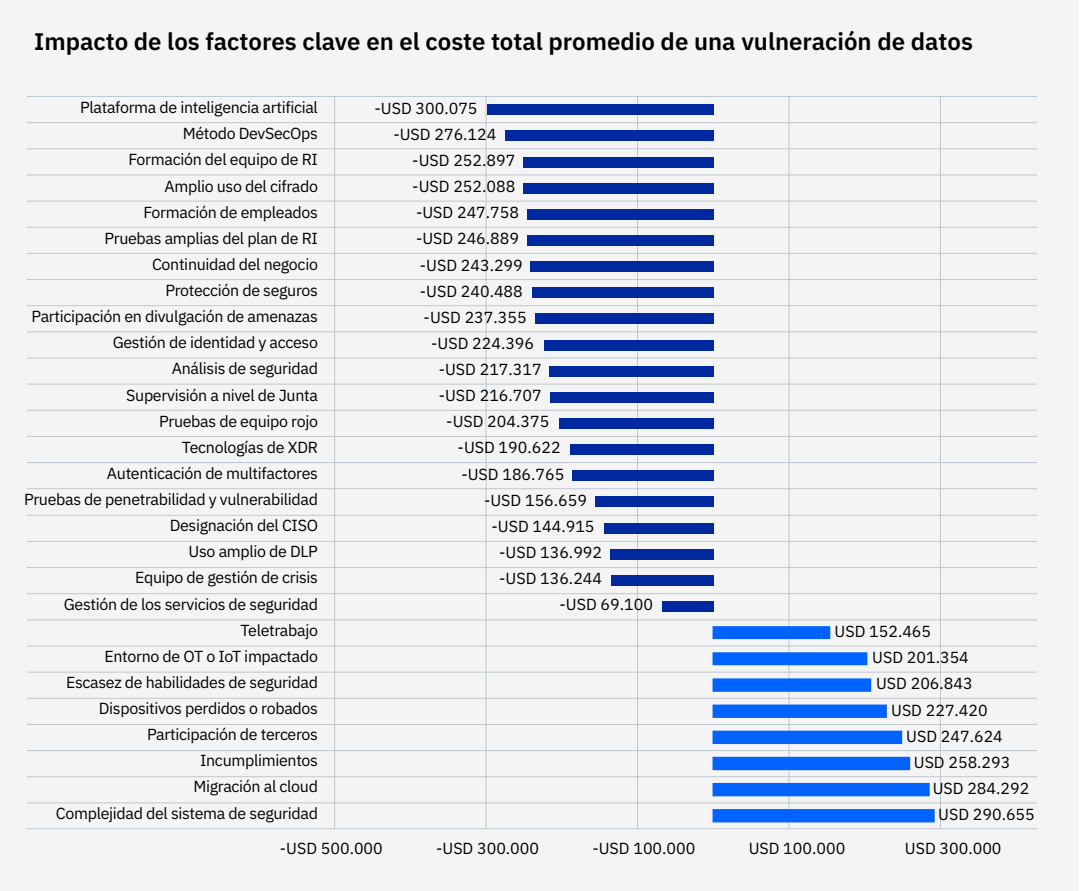


Figura 13: Medido en USD

La figura 14 analiza los tres factores de coste, de los 28 medidos, con el mayor impacto en la potencial amplificación del coste promedio de una vulneración de datos.
Este gráfico compara las organizaciones con un alto nivel en el factor de coste con aquellas con un bajo nivel en el mismo. Hay una diferencia de 2,47 millones de dólares, un 58%, entre los niveles altos y los niveles bajos de complejidad del sistema de seguridad. Hay una diferencia de 2,27 millones de dólares, un 50,5%, entre los niveles altos y los niveles bajos de migración al cloud. Hay una diferencia de 2,26 millones de dólares, un 50,9%, entre los niveles altos y los niveles bajos de incumplimientos. Estos datos muestran que tener presentes los altos niveles de estos factores de coste está asociado también con un coste significativamente superior al promedio para la vulneración de datos. Las organizaciones con un nivel alto de migración al cloud tuvieron un coste promedio de 5,63 millones de dólares, 1,28 millones de dólares más que el coste promedio de una vulneración de datos. Es decir, una diferencia del 25,7%.

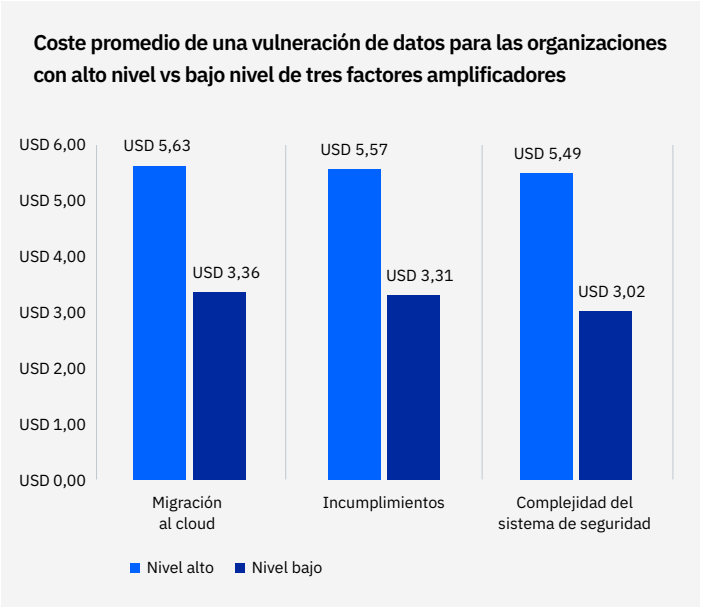


Figura 14: Medido en millones de dólares

La figura 15 detalla los tres factores de costes, de los 28 medidos, con el mayor nivel de impacto en la potencial mitigación del coste promedio de una vulneración de datos.
El gráfico compara las organizaciones con un alto nivel del factor de coste con aquellas con un bajo nivel del factor de coste. Aquellas organizaciones con niveles altos de uso de plataformas de seguridad que utilizan IA tuvieron un coste promedio de vulneración de 2,39 millones de dólares, un 55,3%, inferior que aquellas con niveles bajos de uso de una plataforma de IA. Las organizaciones con altos niveles de uso de un equipo de RI tuvieron un coste promedio de vulneración de 2,02 millones de dólares, un 44,9%, menos que aquellas con un bajo nivel de uso de un equipo de RI. Las organizaciones con un nivel alto de uso de un método DevSecOps tuvieron un coste promedio de vulneración de 1,17 millones de dólares, un 26,7%, menos que aquellas con un nivel bajo de uso de DevSecOps. Las organizaciones con niveles altos en estos factores de coste presentes tuvieron un coste significativamente inferior al promedio en una vulneración de datos. Las organizaciones con un nivel alto de uso de una plataforma de IA tuvieron un coste promedio de 3,13 millones de dólares, 1,22 millones de dólares menos que el coste promedio de una vulneración de datos. Es decir, una diferencia del 32,6%.

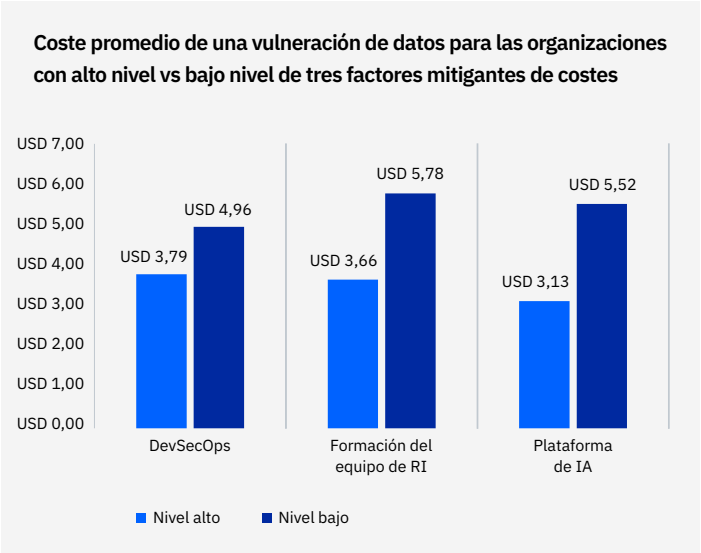


Figura 15: Medido en millones de dólares

3,05 millones de dólares

Ahorro promedio por tener IA y automatización de seguridad implementadas totalmente, en comparación con no tenerlas

IA y automatización de la seguridad

Este fue el quinto año que examinamos la relación entre el coste de la vulneración de dato, las IA y la automatización de la seguridad. En este contexto, IA y automatización de seguridad hace referencia a permitir el uso de tecnologías de seguridad que aumenten o reemplacen la intervención humana, en la identificación y contención de incidencias e intentos de intrusión. Esas tecnologías dependen de la IA, machine learning, análisis y orquestación de seguridad automatizada.

En el lado opuesto del espectro, están los procesos impulsados manualmente, con frecuencia a través de docenas de herramientas y sistemas complejos no integrados, y sin intercambio de datos entre sí.

Figura 16: La proporción de organizaciones con IA y automatización de seguridad, implementadas total o parcialmente, aumentó en cinco puntos porcentuales, del 65% al 70%, entre 2021 y 2022.
La IA y automatización de seguridad totalmente implementadas aumentaron en seis puntos porcentuales, del 25% al 31%, entre 2021 y 2022, y en 10 puntos porcentuales, del 21% al 31%, entre 2020 y 2022. La proporción de organizaciones sin IA y automatización de seguridad implementadas disminuyó del 35% en 2021 al 30% en 2022, cayendo con respecto al 41% de 2020, en una diferencia de 11 puntos porcentuales.

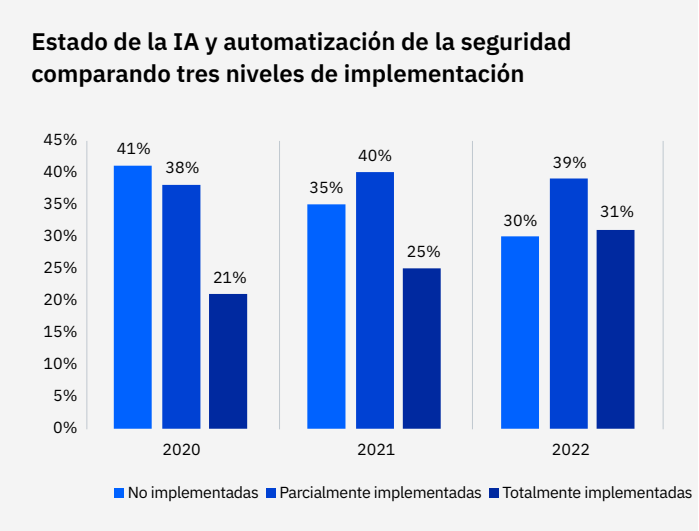


Figura 16: Porcentaje de organizaciones por nivel de implementación

Figura 17: El hecho de tener IA y automatización de seguridad totalmente implementadas está asociado con costes promedio de vulneración de 3,05 millones de dólares menos, una diferencia del 65,2%, con el ahorro de costes más alto en el estudio.
Las organizaciones con IA y automatización de seguridad totalmente implementadas tuvieron un coste total promedio de una vulneración de datos de 3,15 millones de dólares. Este coste promedio total es comparable con los 6,20 millones de dólares de las organizaciones sin IA y automatización de seguridad. La diferencia entre el coste promedio de una vulneración, con automatización de seguridad totalmente implementada y sin IA ni automatización de seguridad implementadas, fue inferior en 2022 que en 2021, cuando la diferencia fue de 3,81 millones de dólares, o que en 2020, cuando el ahorro fue de 3,58 millones de dólares.

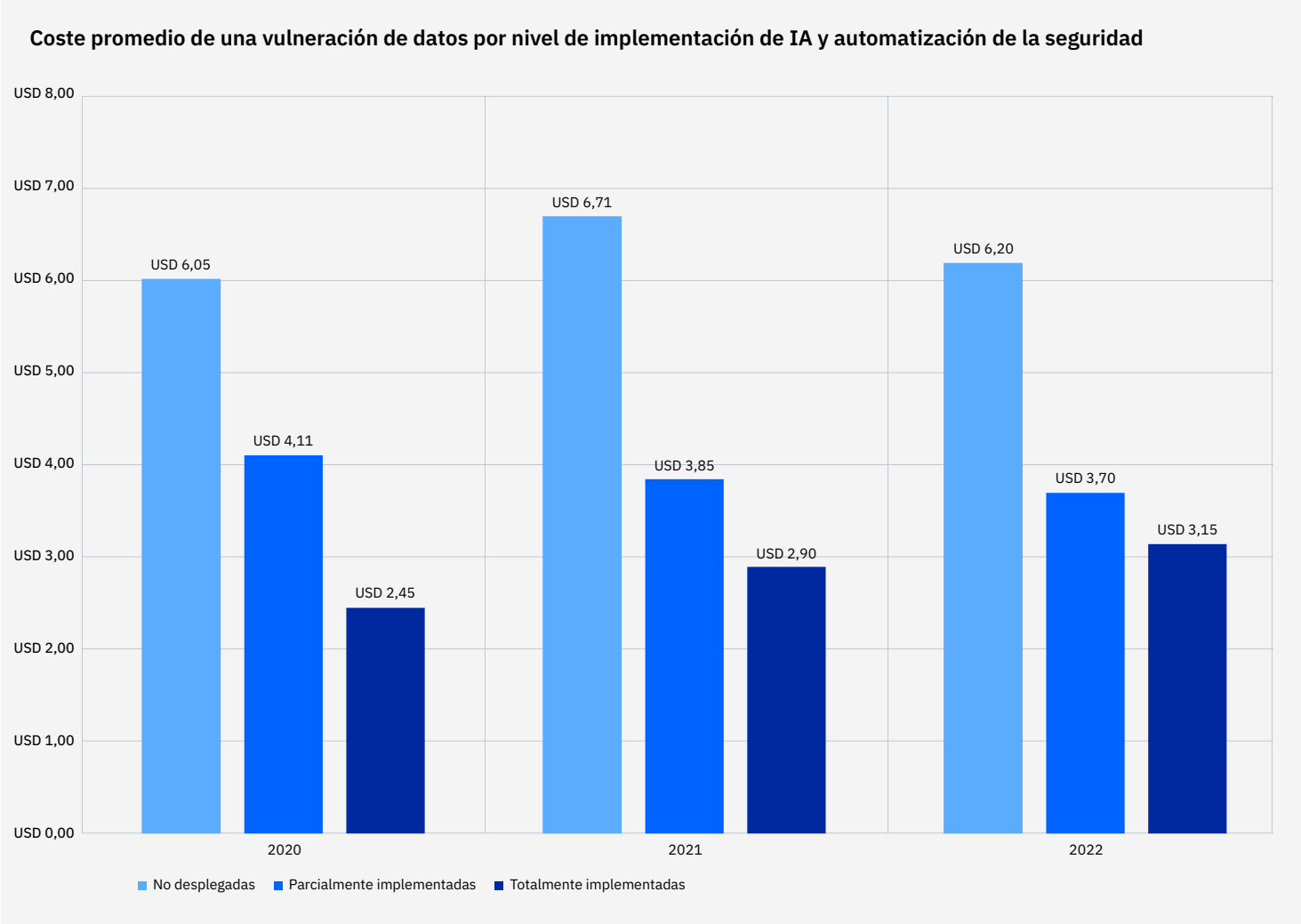


Figura 17: Medido en millones de dólares

Tiempo promedio para identificar y contener una vulneración de datos por nivel de IA y automatización de seguridad

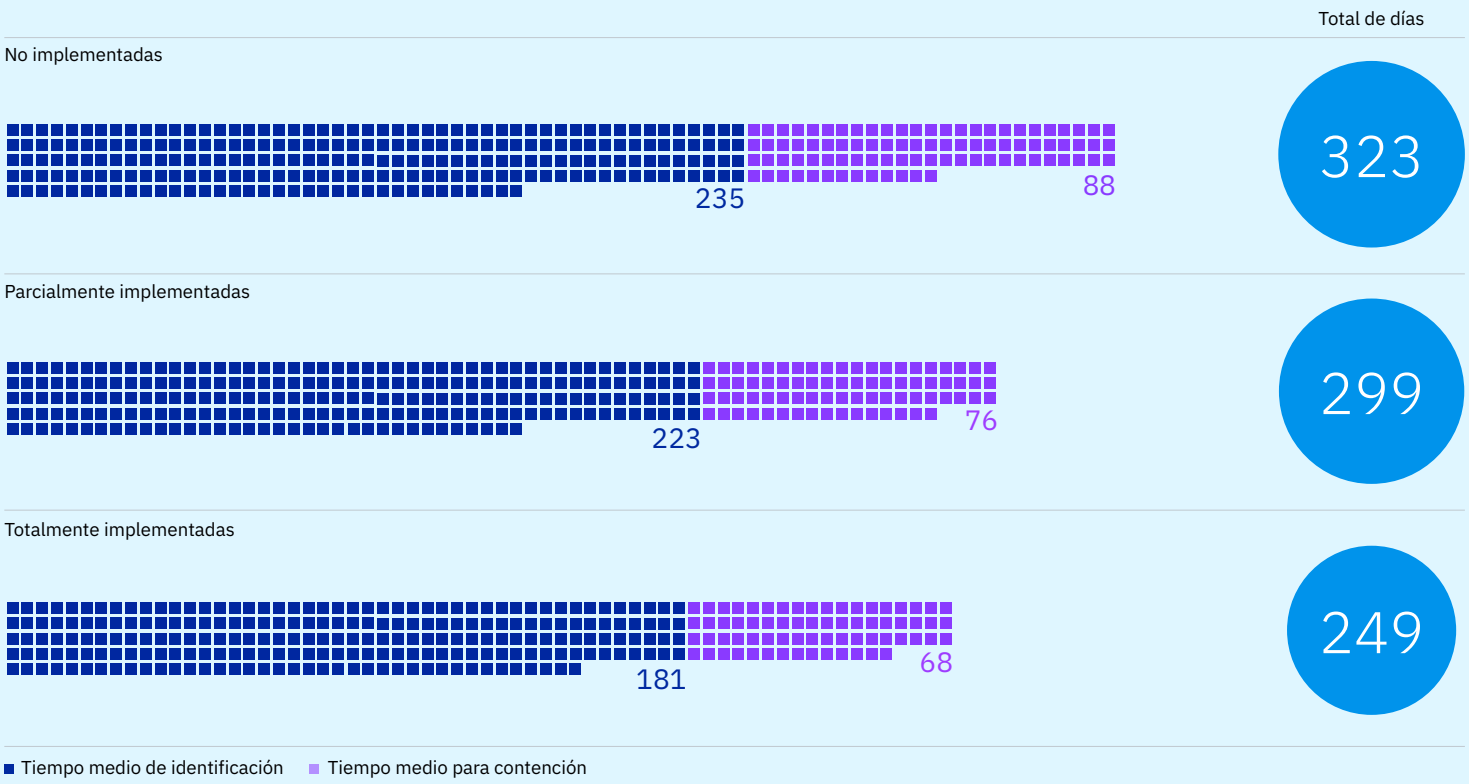


Figura 18: Medido en días

Figura 18: Las organizaciones con IA y automatización de seguridad totalmente implementadas fueron capaces de detectar y contener una vulneración mucho más rápido que las organizaciones sin IA ni automatización de seguridad implementadas.
Las organizaciones con IA y automatización de seguridad totalmente implementadas tardaron un promedio de 181 días en identificar y 68 días en contener la vulneración de datos, para alcanzar un ciclo de vida total de 249 días. Las organizaciones sin IA ni automatización de seguridad implementadas tardaron un promedio de 235 días en identificar y 88 días en contener la vulneración, alcanzando un ciclo de vida total de 323 días. Es decir, 74 días más que las organizaciones con IA y automatización de seguridad totalmente desplegadas. El tiempo promedio hasta identificar y contener una vulneración fue en total de 299 días con IA y automatización de seguridad parcialmente implementadas.

29 días

Las organizaciones con tecnologías de XDR identificaron y contuvieron una vulneración 29 días antes que aquellas sin XDR

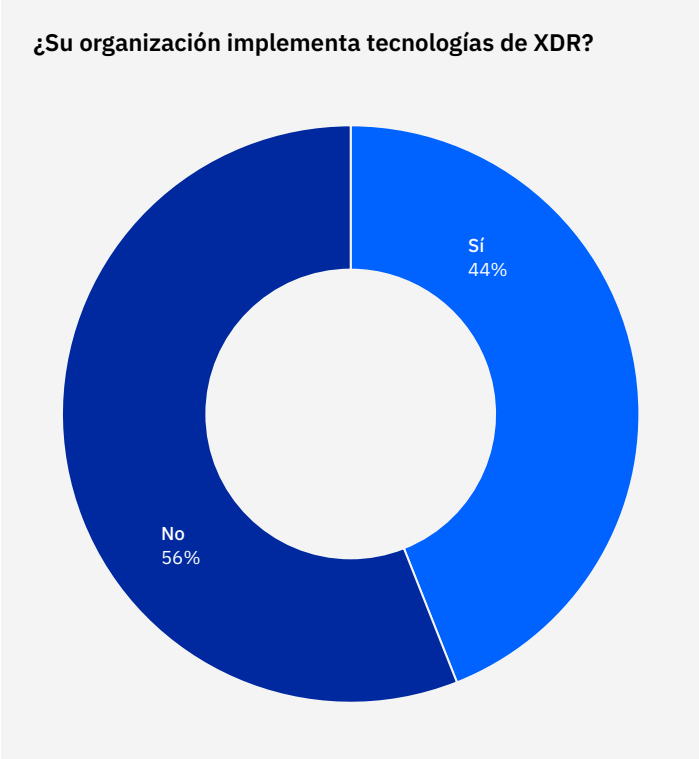


Figura 19

Tecnologías de XDR

Por primera vez, el estudio examina los efectos de las tecnologías de XDR en el coste de una vulneración de datos. Esta sección señala la prevalencia de XDR en las organizaciones estudiadas, su impacto en el coste total promedio y el tiempo promedio, hasta contener las vulneraciones de datos.

Un punto significativo es que XDR impactó en los costes promedios de la vulneración con un ahorro del 9,2%. Aunque estos ahorros pueden parecer modestos a primera vista, el impacto real se observa en el tiempo ahorrado por las organizaciones en la duración de la vulneración cuando usaron XDR. Casi un mes. El tiempo adicional hasta identificar y contener la vulneración puede sumar mucho al coste global de una vulneración y sus consecuencias.

Figura 19: Las prestaciones de XDR son de uso habitual, pero todavía no son utilizadas por la mayoría de las organizaciones.
Según la encuesta a 550 organizaciones en el estudio, el 44% está implementando tecnologías de XDR, y el 56% no están implementando tecnologías de XDR.

Figura 20: El uso de tecnologías de XDR está asociado con un coste inferior al promedio para una vulneración de datos.
Las organizaciones que están implementando tecnologías de XDR experimentaron un coste promedio de una vulneración de datos de 4,15 millones de dólares. Las organizaciones que no estaban implementando tecnologías de XDR experimentaron un coste promedio de una vulneración de datos de 4,55 millones de dólares. Este coste estuvo por encima del promedio global y fue 400.000 dólares superior que las vulneraciones en las organizaciones que implementaron tecnologías de XDR, una diferencia del 9,2%.

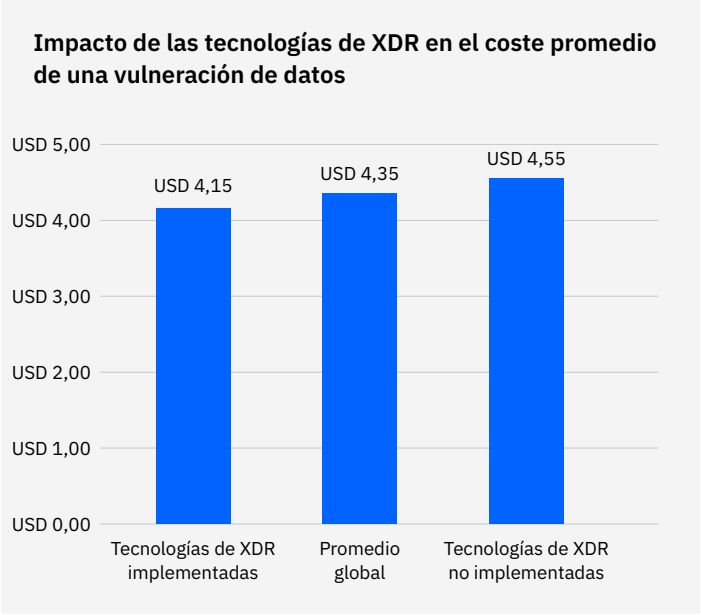


Figura 20: Medido en millones de dólares

Figura 21: El tiempo promedio hasta identificar y contener una vulneración de datos fue significativamente inferior con las tecnologías de XDR.
Se necesita un promedio de 275 días para identificar y contener las vulneraciones en organizaciones con tecnologías de XDR implementadas. Esto representa 29 días menos que las vulneraciones en organizaciones sin tecnologías de XDR desplegadas, que necesitaron 304 días. Esto representa un diferencia del 10% en el tiempo medio hasta identificar y contener una vulneración, entre las organizaciones con tecnologías de XDR y aquellas sin estas tecnologías.

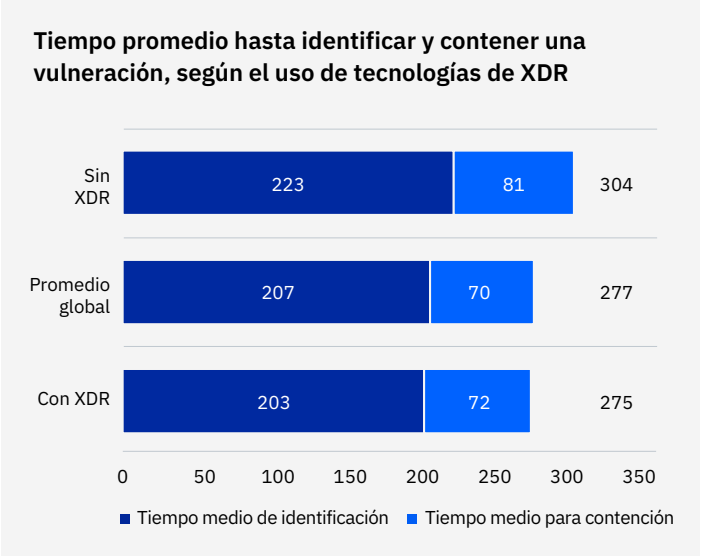


Figura 21: Medido en días

2,66 millones de dólares

Ahorro de costes promedio de una vulneración en organizaciones con un equipo de RI que probó un plan de RI, en comparación con las que carecen de equipo de RI y no habían probado un plan de RI

Respuesta a incidencias

En años anteriores, esta investigación ha demostrado que el uso de equipos de RI y la realización de pruebas del plan de RI reducen significativamente el coste promedio de una vulneración de datos. En el análisis de este año, hemos visto nuevamente como los equipos de RI, las prestaciones y los procesos, impactaron en el coste de la vulneración.

Figura 22: Una mayoría de las organizaciones del estudio tenían planes de RI y probaban los planes de RI de forma regular.
Casi tres cuartas partes de las organizaciones del estudio indicaron que tenían un plan de RI, con un 73% que dijo que tenía un plan de RI y un 27% que dijo que no tenía ningún plan. De las organizaciones con un plan de RI, el 63% indicó que probaba regularmente el plan de RI, con un 37% que dijo no probar regularmente el plan de RI.

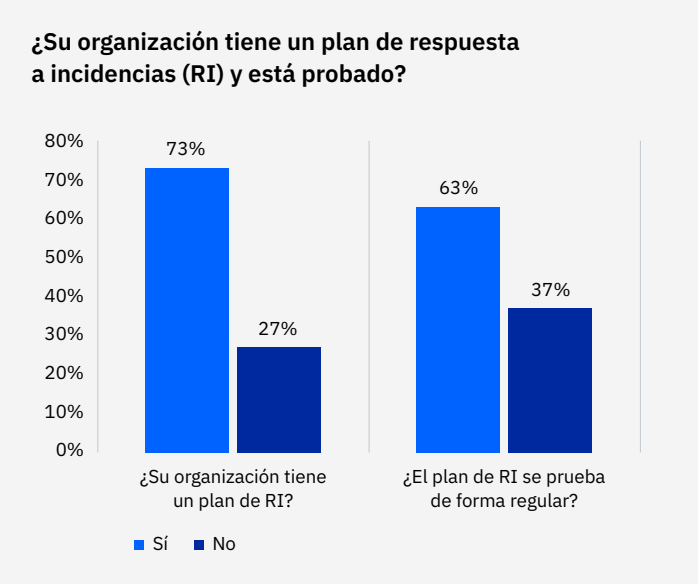


Figura 22

Coste promedio de una vulneración de datos con equipo de respuesta a incidencias (RI) y prueba del plan de RI

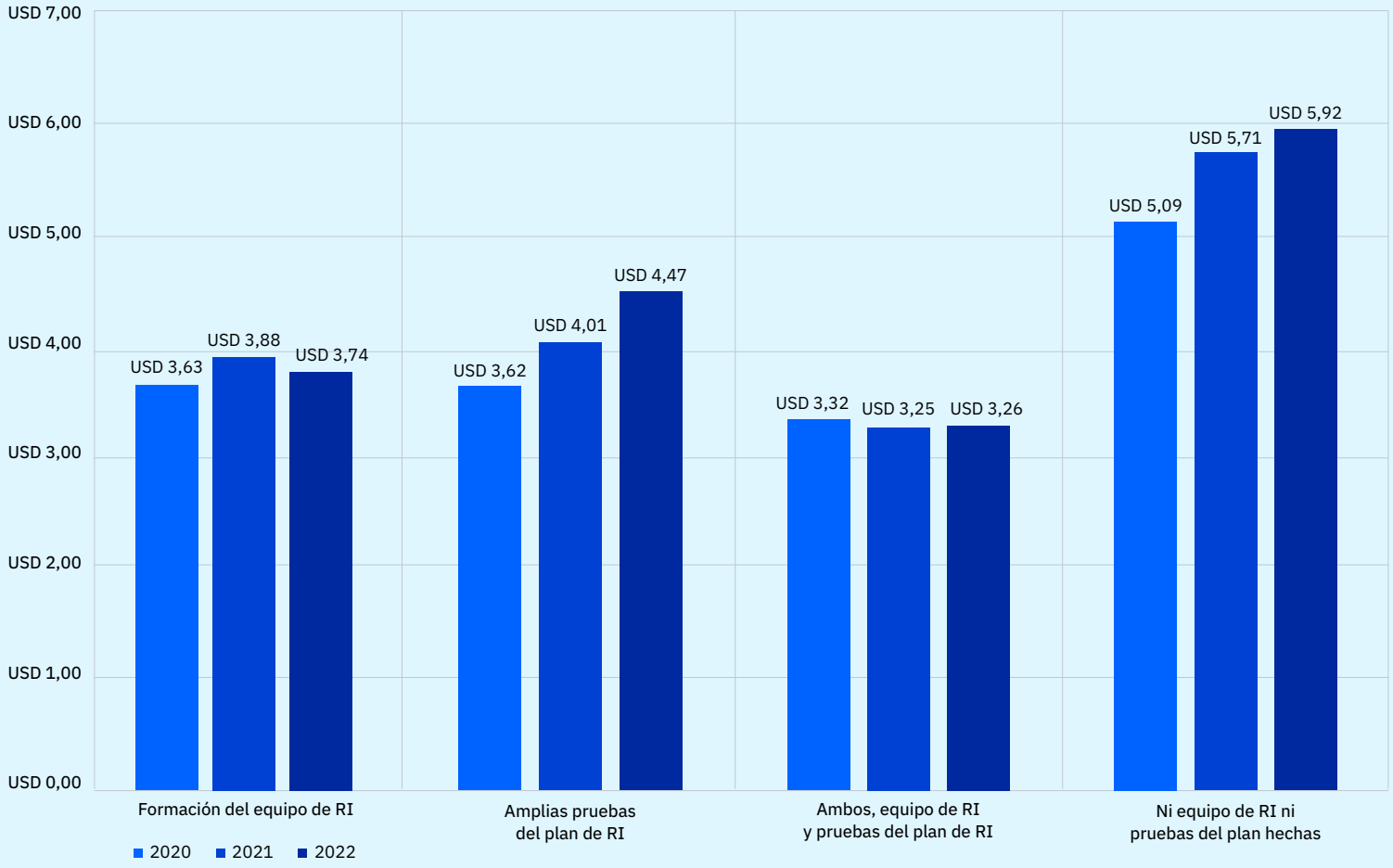


Figura 23: Medido en millones de dólares

Figura 23: Los equipos de RI y las pruebas amplias del plan de RI han seguido mitigando los costes de las vulneraciones de datos en 2022. La diferencia entre el coste promedio de una vulneración de datos en organizaciones con equipos de RI y pruebas del plan de RI, y aquellas otras sin equipos de RI ni pruebas realizadas en el plan de RI, siguió creciendo entre el informe de 2020 y el informe de 2022. Las vulneraciones en las organizaciones con prestaciones de RI tuvieron un coste promedio de vulneración de 3,26 millones de dólares en 2022, en comparación con los 5,92 millones de dólares en organizaciones sin prestaciones de RI. Este coste promedio significa una diferencia de 2,66 millones de dólares, de un 58%. Ese ahorro representa un aumento con respecto a 2021, año en el que el coste promedio de una vulneración en organizaciones con prestaciones de RI tuvo un ahorro de 2,46 millones de dólares. Y con respecto a 2020, cuando la diferencia de coste fue de 1,77 millones de dólares. Este hallazgo indica una eficacia creciente en el ahorro de costes de las prestaciones de RI.

2,10 millones de dólares

Ahorro de costes de las vulneraciones en organizaciones que usan técnicas de cuantificación del riesgo, en comparación con aquellas que no las usan

¿Su organización prioriza los riesgos, las amenazas y los impactos, con base en técnicas de cuantificación del riesgo?

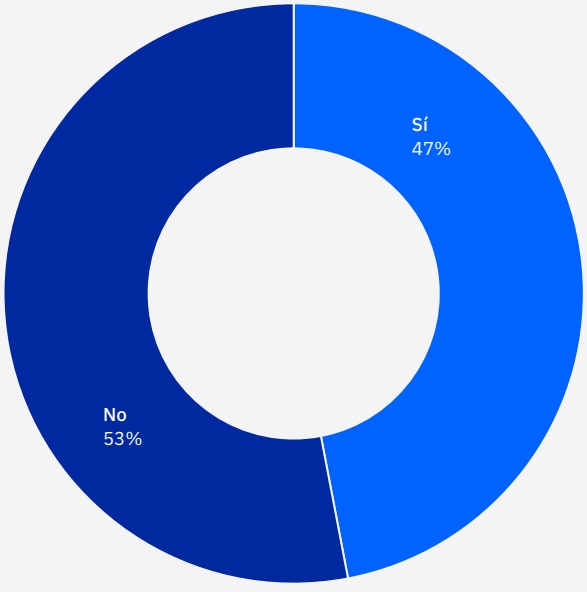


Figura 24

Clasificación de riesgos

La clasificación de riesgos observa los impactos, incluso los financieros, la disponibilidad de los datos y la integridad de estos. Usar la clasificación de riesgos puede hacer destacar los tipos de pérdidas financieras por impacto, incluso los siguientes ejemplos: Pérdida de productividad; coste de respuesta o recuperación, impacto a la reputación, y multas y resoluciones judiciales.

Los directores de seguridad de la información (CISO), los gestores de riesgos y los equipos de seguridad pueden usar las investigaciones de referencia como el informe "Coste de la Vulneración de Datos" para deducir tendencias generales y promedios de costes en su industria o área geográfica.
Sin embargo, usar datos específicos de la organización en lugar de promedios de la industria puede aclarar las potenciales carencias en la seguridad y cómo reducir el riesgo general, mediante la cuantificación del riesgo para la seguridad en términos financieros.

Esta sección analiza cuántas organizaciones están usando técnicas de clasificación de riesgos para priorizar los riesgos, las amenazas y los impactos. Además, repasa el impacto en el coste promedio de las técnicas de clasificación del riesgo.

Figura 24: Menos de la mitad, un 47%, indicó que prioriza los riesgos, las amenazas y los impactos con base en las técnicas de clasificación de riesgos.
Por otro lado, de las 550 organizaciones estudiadas, un 53% no prioriza los riesgos, las amenazas y los impactos con base en técnicas de clasificación de riesgos.

Figura 25: La clasificación de riesgos tuvo un efecto considerable en los costes de la vulneración de datos, generando un ahorro de hasta 2,10 millones de dólares como promedio.
Las organizaciones que priorizaron los riesgos, las amenazas y los impactos con base en técnicas de clasificación de riesgos tuvieron un coste de vulneración promedio de 3,30 millones de dólares. Ese coste fue de 2,10 millones de dólares menos que aquellas que no usaron la clasificación de riesgos, 5,40 millones de dólares. Es decir, un ahorro del 48,3%. La clasificación del riesgo estuvo asociada con costes de vulneración que fueron más de 1 millón de dólares inferiores al promedio global, de 4,35 millones de dólares.

Impacto de las técnicas de cuantificación del riesgo en el coste promedio de una vulneración de datos

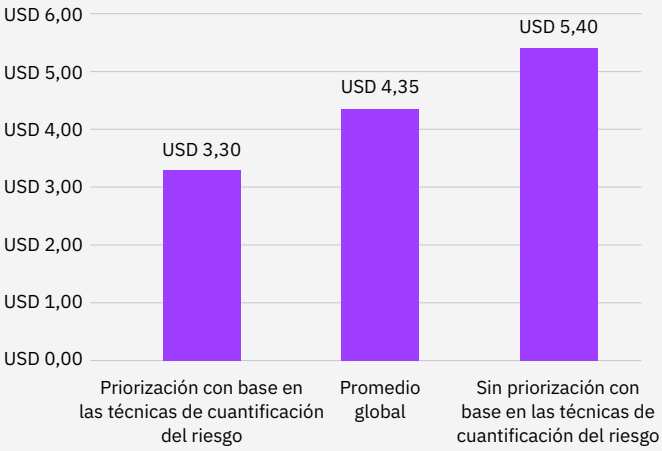


Figura 25: Medido en millones de dólares

1,51 millones de dólares

Ahorro de costes promedio de una vulneración asociado con una implementación desarrollada de Zero trust, versus al inicio de la adopción de Zero trust

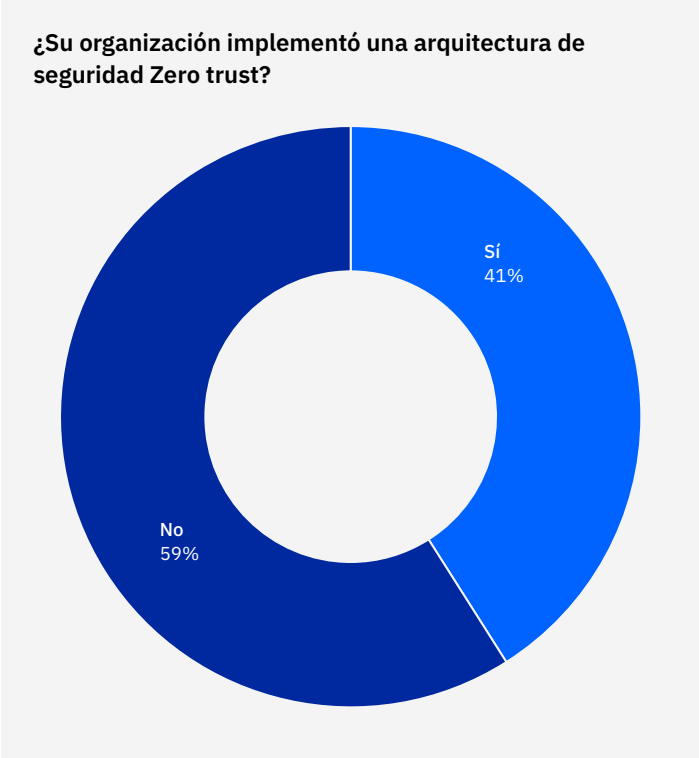


Figura 26

Zero trust

Por segundo año, este estudio examina la prevalencia y el impacto financiero de las vulneraciones de datos con base en la implementación de una infraestructura de seguridad Zero trust. El método Zero trust opera sobre la base de la presunción de que las identidades de usuario o la red en sí ya podrían estar comprometidas, y en su lugar, se basa en la IA y el análisis para validar constantemente las conexiones entre usuarios, datos y recursos. Como muestran los datos en esta sección, Zero trust tiene un impacto positivo neto en los costes de la vulneración de datos.

Figura 26: En el estudio de 2022, el 41 % de las organizaciones indicó que habían implementado una arquitectura de seguridad Zero trust, mientras que el 59% no lo había hecho.
Este hallazgo se puede comparar con el informe de 2021, en el que el 35% dijo que habían implementado total o parcialmente una arquitectura Zero trust.

Figura 27: Las organizaciones con Zero trust implementado ahorraron casi 1 millón de dólares en costes promedio de vulneración, en comparación con organizaciones sin Zero trust implementado.
El coste promedio de una vulneración de datos fue de 4,15 millones de dólares en organizaciones con Zero trust implementado, mientras que el coste de una vulneración fue en promedio de 5,10 millones de dólares en organizaciones sin Zero trust implementado. La diferencia fue de 950.000 dólares, lo que representa un ahorro del 20,5% para las organizaciones con Zero trust implementado.

Figura 28: Contar con una implementación madura de Zero trust está asociado con costes de vulneración más de 1,5 millones de dólares inferiores que las vulneraciones en organizaciones en la etapa inicial de adopción de Zero trust.
Las organizaciones con una implementación en fase de madurez de su arquitectura de seguridad Zero trust, donde Zero trust se aplica uniformemente en todos los dominios, tuvo un coste promedio de vulneración de datos de 3,45 millones de dólares. En la etapa intermedia, en la cual Zero trust se aplica a muchas áreas de la organización, el coste promedio de una vulneración de datos fue de 3,96 millones de dólares. Para las organizaciones en la etapa inicial de adopción que estaban comenzando a implementar algunas prácticas, el coste promedio de una vulneración de datos fue de 4,96 millones de dólares. Este coste fue de 1,51 millones de dólares más que en las vulneraciones en organizaciones desarrolladas, es decir, una diferencia del 35,9%.

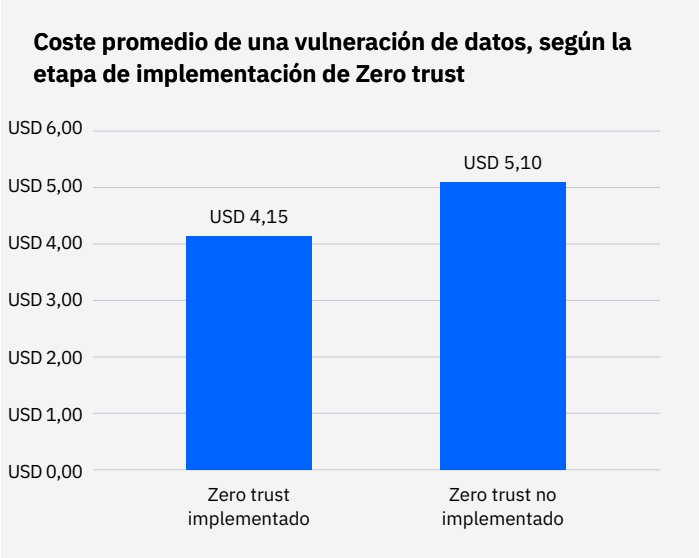


Figura 27: Medido en millones de dólares

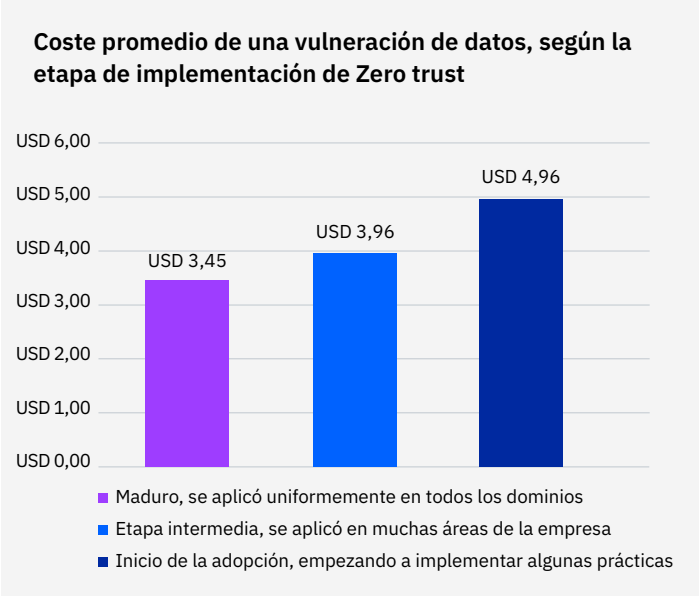


Figura 28: Medido en millones de dólares

49 días

Identificar y contener las vulneraciones por ransomware necesitaron 49 días más que el promedio.

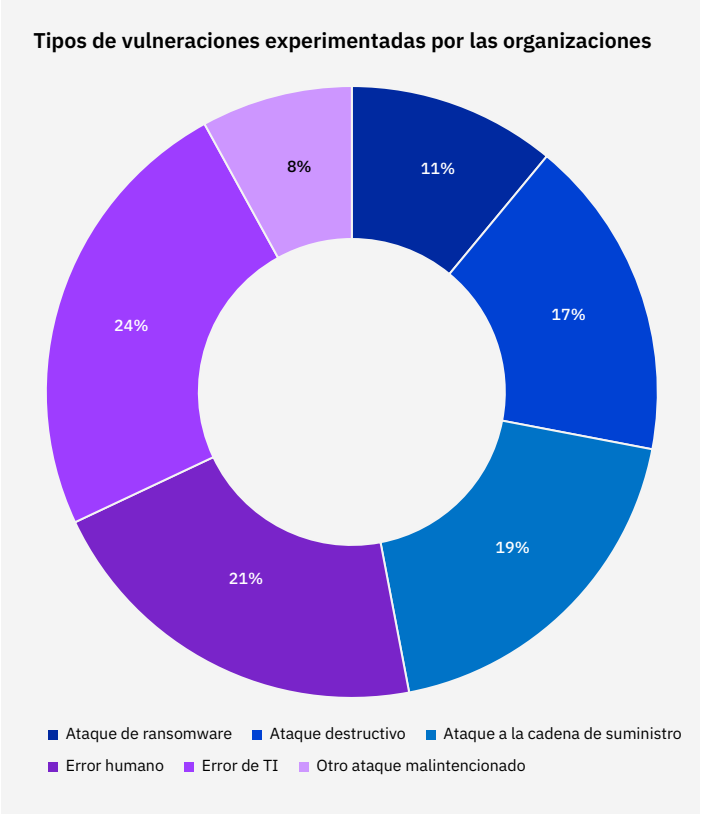


Figura 29

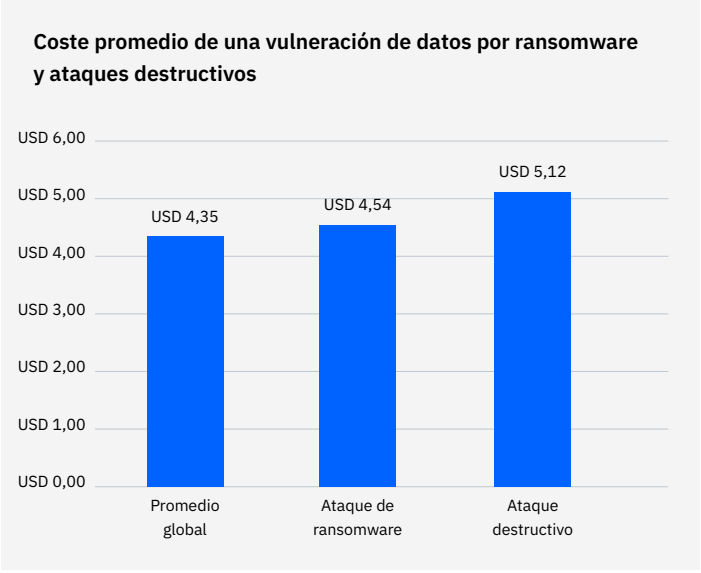


Figura 30: Medido en millones de dólares

Ransomware y ataques destructivos

Este ha sido el segundo año que examinamos el coste de los ataques de ransomware y las vulneraciones. También añadimos al estudio de este año las vulneraciones con malware destructivo. En comparación con el año pasado, los costes de las vulneraciones con ransomware han disminuido levemente, pasando de 4,62 millones de dólares a 4,54 millones de dólares. Sin embargo, la frecuencia de las vulneraciones con ransomware ha aumentado, pasando del 7,8% de las vulneraciones en el informe de 2021 al 11% en el estudio de 2022.

Este año, observamos el ciclo de vida de estas vulneraciones, así como el impacto que tuvo el hecho de pagar un rescate en el coste sin rescate de la vulneración. Nota: Este estudio no incluye el coste del rescate en sí, en el cálculo del coste de un ataque de ransomware.

Figura 29: El ransomware fue responsable del 11% de las vulneraciones, mientras que los ataques destructivos fueron responsables del 17% de las vulneraciones.
Otro 19% de las vulneraciones se produjo por ataques a la cadena de suministro, que fueron vulneraciones causadas por verse comprometido inicialmente un socio comercial. Los errores humanos, es decir, las vulneraciones causadas de forma accidental por acciones negligentes de empleados o contratistas, fueron responsables del 21% de las vulneraciones.

Los errores de TI que se produjeron a causa de una interrupción o un fallo en los sistemas informáticos de la organización, generando una pérdida de datos, fueron responsables del 24% de las vulneraciones. Este tipo de fallos incluye errores en el código fuente o un fallo en un proceso, como errores en las comunicaciones automáticas.
El 8% restante de las vulneraciones fueron otros ataques maliciosos.

Figura 30: El coste promedio de un ataque de ransomware, sin incluir el coste del rescate en sí, fue de 4,54 millones de dólares, levemente superior al coste total promedio global de una vulneración de datos de 4,35 millones de dólares.
El coste promedio de un ataque destructivo o de borrado fue de 5,12 millones de dólares, 770.000 dólares más que el promedio general, un 16,3%.

Figura 31: El tiempo promedio hasta identificar y contener un ataque destructivo o de ransomware fue significativamente superior que el promedio.
Llevó 237 días identificar y 89 días contener un ataque de ransomware, alcanzando un ciclo de vida total de 326 días. Tomó 233 días identificar y 91 días contener un ataque destructivo, para alcanzar un ciclo de vida total de 324 días. En comparación con el ciclo de vida promedio general de 277 días, las organizaciones tardaron 49 días más en identificar y contener un ataque de ransomware. Una diferencia del 16,3%. Además, las organizaciones invirtieron 47 días más en identificar y contener un ataque destructivo, una diferencia del 15,6%.

Figura 32: El coste promedio de una vulneración con ransomware fue superior en los casos en que no pagaron el rescate.
El coste del rescate no se incluye en el cálculo del coste de una vulneración con ransomware. El coste de la vulneración con ransomware se basó en actividades, como la detección del ataque y la pérdida de negocio debido al tiempo de inactividad del sistema. Para las organizaciones que no pagaron el rescate, el coste promedio de la vulneración fue de 5,12 millones de dólares. Para las organizaciones que sí pagaron el rescate, el coste promedio de la vulneración fue de 4,49 millones de dólares. La diferencia en el coste promedio fue de 630.000 dólares, algo más de un 13%.

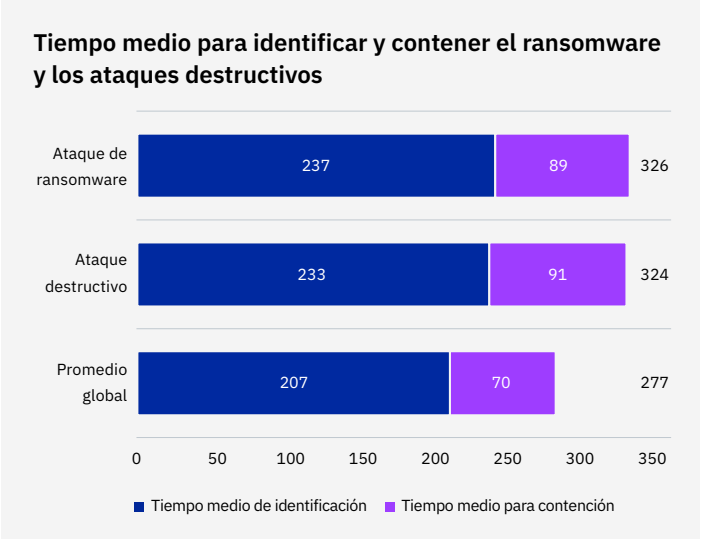


Figura 31: Medido en días

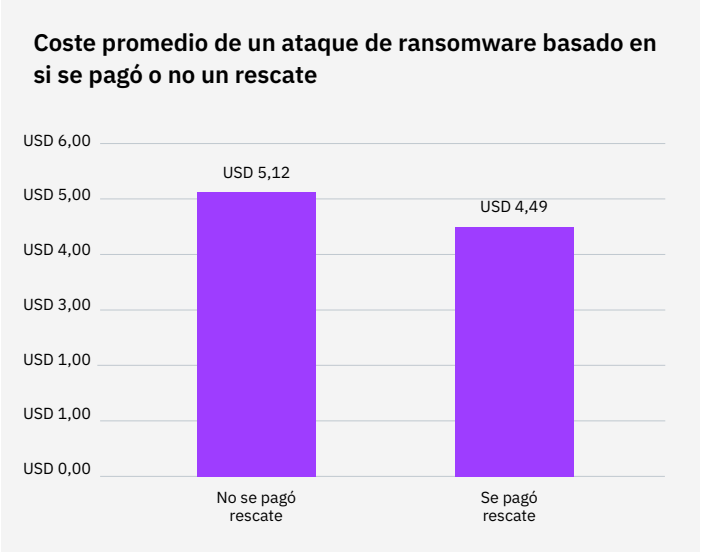


Figura 32: Medido en millones de dólares. El coste del rescate no se incluye en este cálculo

26 días

Identificar y contener una vulneración en la cadena de suministro, tomó un promedio de 26 días más que la media global

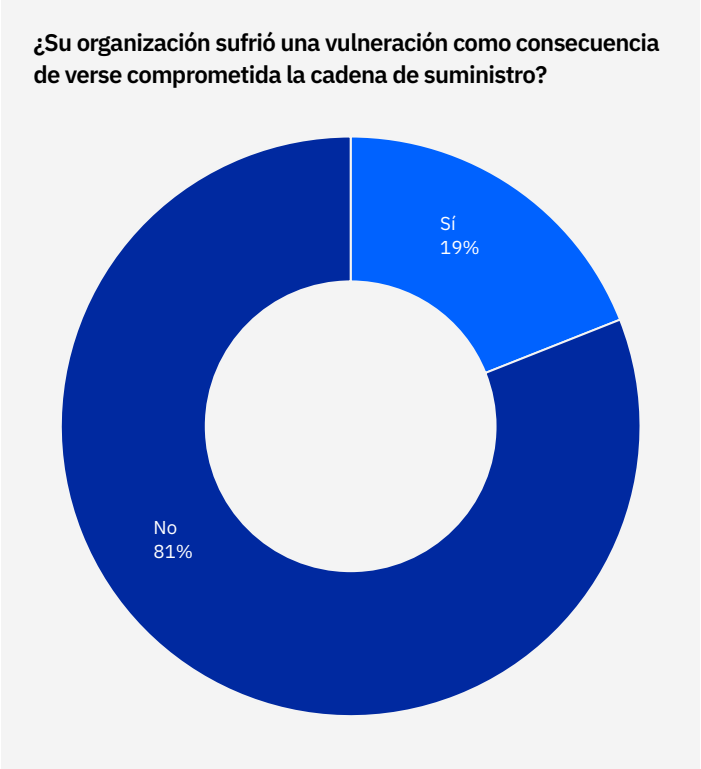


Figura 33

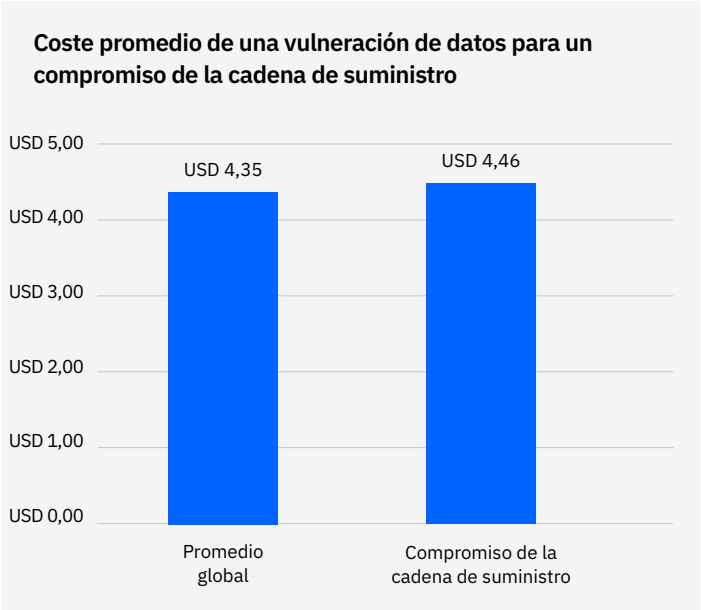


Figura 34: Medido en millones de dólares

Ataques a la cadena de suministro

Debido a una serie de ataques a la cadena de suministro producidos en los últimos años, el informe de este año es el primero que incluye las vulneraciones de datos en el contexto de los ataques a la cadena de suministro. Un compromiso de la cadena de suministro es una vulneración que se produce porque se vio comprometido un socio comercial, por ejemplo, un proveedor. Según la investigación, casi una quinta parte de las vulneraciones se producen porque se compromete la cadena de suministro, haciendo que las vulneraciones sean más costosas, con ciclos de vida más prolongados.

Figura 33: Aproximadamente una quinta parte de las vulneraciones analizadas en el estudio fueron resultado de un compromiso de la cadena de suministro.
Un 19% de las organizaciones señaló que sí habían sufrido una vulneración como resultado de un compromiso de la cadena de suministro. Mientras, el 81% dijo que no.

Figura 34: El coste total promedio de un compromiso de la cadena de suministro fue de 4,46 millones de dólares.
El coste fue mayor que el coste promedio general de una vulneración de datos, 4,35 millones de dólares, una diferencia de 110 000 dólares, un 2,5 %.

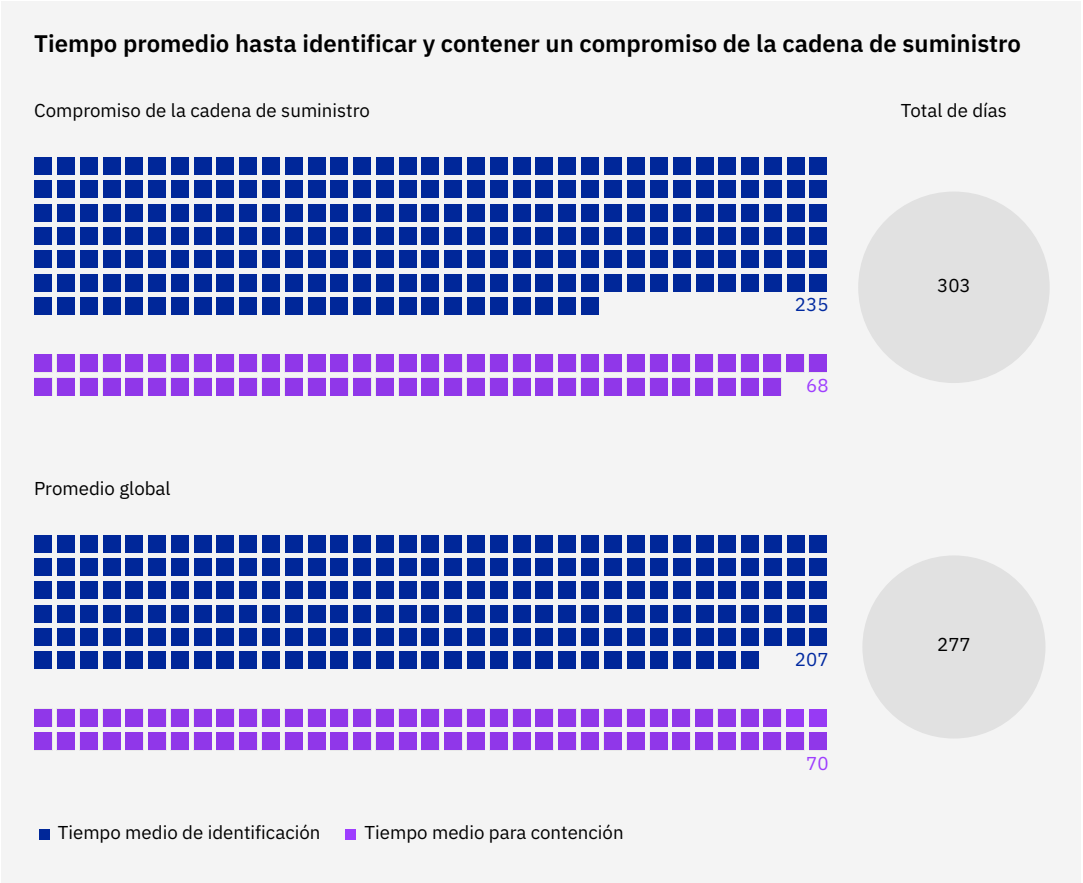


Figura 35: Medido en días

Figura 35: El compromiso de la cadena de suministro tiene un ciclo de vida más prolongado que el promedio global.
Las organizaciones tardan un promedio de 235 días en identificar y 68 días en contener un compromiso de la cadena de suministro, alcanzando un ciclo de vida total de 303 días. El ciclo de vida promedio fue de 26 días más que el ciclo de vida promedio global de las vulneraciones de datos, que es de 277 días. Una diferencia del 9%.

79%

Proporción de las industrias de infraestructura crucial que no adoptaron un método de seguridad zero trust

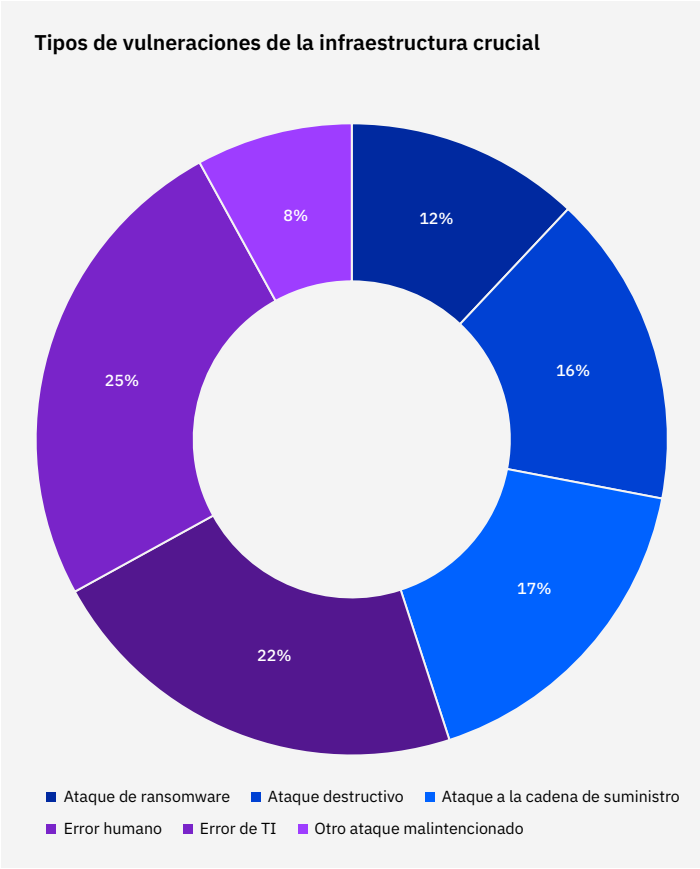


Figura 36

Infraestructura crucial

Este informe estudia, por primera vez, el coste y la contención de vulneraciones de datos en el contexto de las industrias de infraestructura crucial. Según la clasificación de la Agencia de Seguridad de la Infraestructura y Ciberseguridad de los EE.UU. (CISA), los sectores de infraestructura crucial en este estudio incluyen servicios financieros, industria, tecnología, energía, transporte, comunicación, atención sanitaria, educación y sector público.

Este análisis revela que las industrias de infraestructura crucial tuvieron una prevalencia mucho más baja de los métodos de seguridad Zero trust que el promedio global. Las industrias de infraestructura crucial sin estrategias Zero trust implementadas tuvieron costes de vulneración de datos significativamente superiores al promedio.

Figura 36: El ransomware y los ataques destructivos fueron responsables de más de un cuarto de las vulneraciones en industrias de infraestructura crucial.
Los ataques de ransomware representaron el 12% de las vulneraciones de infraestructura crucial, mientras que los ataques destructivos estuvieron detrás del 16% de las vulneraciones de infraestructura crucial, para alcanzar un combinado del 28%. Otro 17% de las vulneraciones en estas industrias fueron ataques a la cadena de suministro, donde un socio comercial externo fue el vector de ataque. Por otro lado, las vulneraciones causadas por errores humanos y errores de TI representaron el 22% y el 25%, respectivamente. El 8% restante de las vulneraciones de infraestructura crucial fueron otros ataques maliciosos.

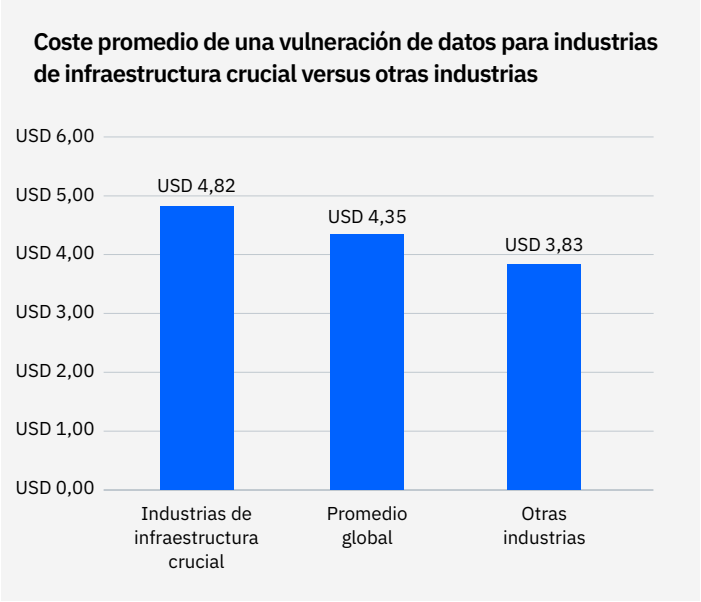


Figura 37: Medido en millones de dólares

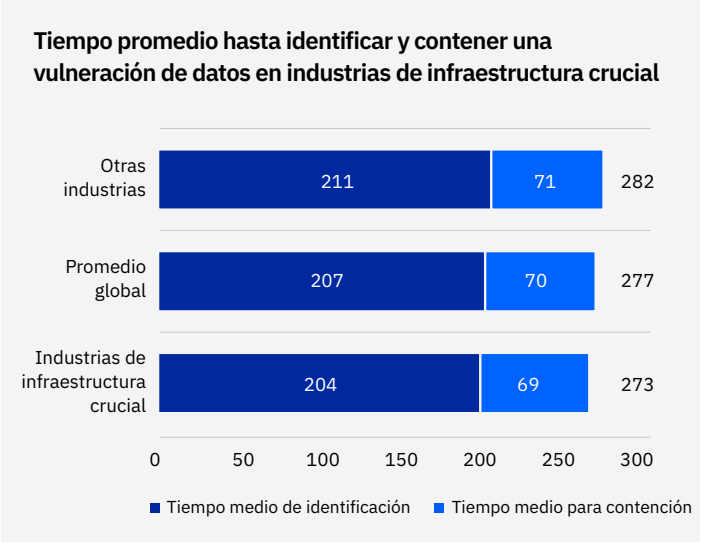


Figura 38: Medido en días

Figura 37: El coste promedio de una vulneración de datos en organizaciones de infraestructura crucial fue de 4,82 millones de dólares.
Las organizaciones de infraestructura crucial tuvieron un coste promedio de una vulneración de datos de 990.000 dólares más con respecto a los 3,83 millones de dólares para las organizaciones en industrias que no son de infraestructura crucial, una diferencia del 22,9%. Las industrias que no son de infraestructura crucial incluyen farmacéutica, servicios, entretenimiento, bienes de consumo, medios de comunicación, hostelería, comercio minorista e investigación.

Figura 38: Las industrias de infraestructura crucial identificaron y contuvieron vulneraciones de datos más rápido que otras industrias.
El ciclo de vida de una vulneración de datos en industrias de infraestructura crucial duró menos días que el promedio global o que las industrias ajenas a la infraestructura crucial. El tiempo medio hasta la identificación en industrias de infraestructura crucial fue de 204 días, en comparación con 211 días para otras industrias. El tiempo medio hasta la contención en industrias de infraestructura crucial fue de 69 días, en comparación con 71 días para otras industrias. El promedio combinado de 273 días hasta identificar y contener una vulneración en la infraestructura crucial fue de cuatro días menos que el promedio global general de 277 días. Asimismo, el promedio combinado para las industrias de infraestructura crucial fue de nueve días menos que el promedio de 282 días para otras industrias.

Figura 39: Solo una quinta parte de las organizaciones de infraestructura crucial había implementado un método Zero trust para la seguridad, es decir, la mitad del promedio global general.
El 21% de las organizaciones de infraestructura crucial había implementado un método Zero trust, mientras que un 79% no lo había hecho. Comparemos ese porcentaje con el promedio global general del 41% de las organizaciones con estrategia Zero trust.

Figura 40: Las organizaciones en industrias de infraestructura crucial que implementaron un método Zero trust para la seguridad tuvieron un coste promedio de una vulneración de datos de 4,23 millones de dólares.
En aquellas organizaciones de infraestructura crucial que no implementaron un método Zero trust, el coste promedio de una vulneración fue de 5,40 millones de dólares. El resultado es una diferencia de 1,17 millones de dólares, el 24,3%, más que aquellas que sí implementaron una estrategia Zero trust.

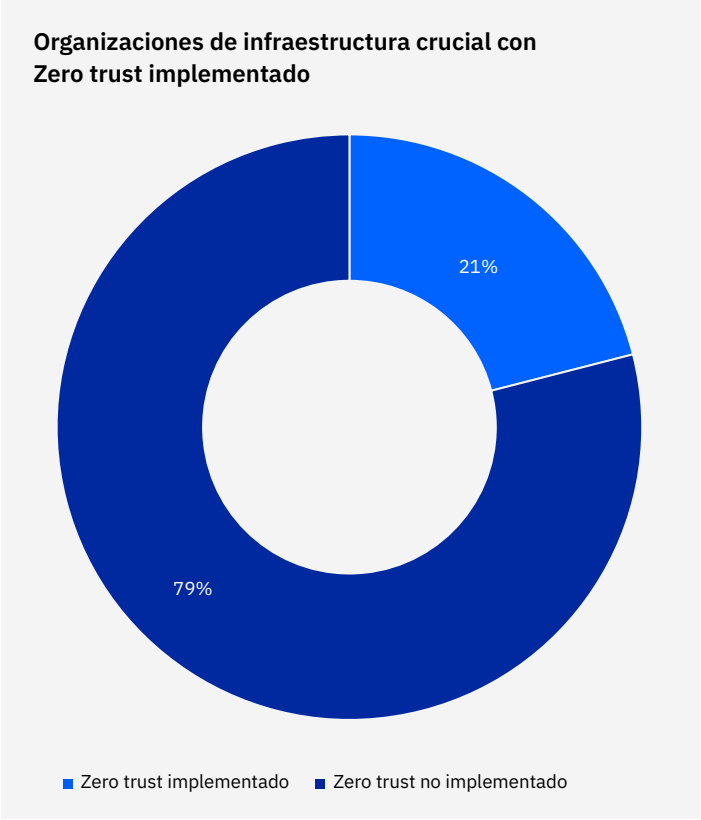


Figura 39

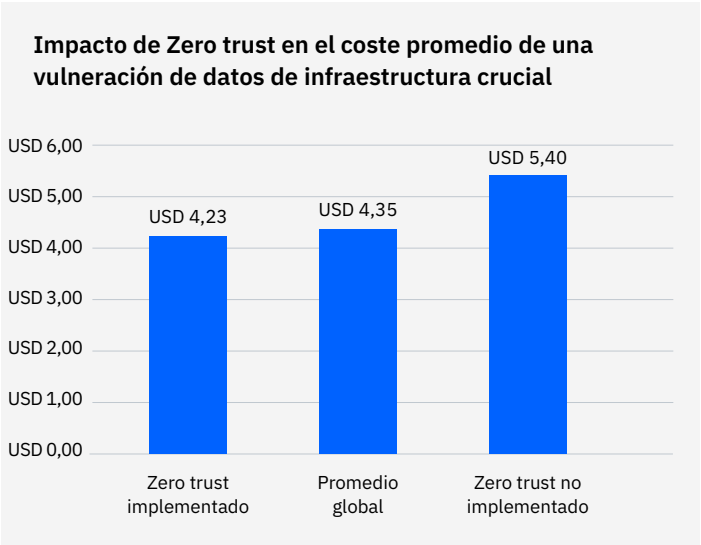


Figura 40: Medido en millones de dólares

43%

Porcentaje de organizaciones que estaban en las etapas iniciales o no habían comenzado a aplicar prácticas de seguridad para proteger sus entornos cloud

Vulneraciones en el cloud y modelo de cloud

Por segundo año en este informe, hemos analizado más de cerca el impacto del modelo de cloud y la madurez de la seguridad en el cloud, en el coste de una vulneración de datos. La investigación encontró que el 45% de las vulneraciones se produjeron en el cloud, pero las producidas en el cloud público costaron considerablemente más que las vulneraciones en organizaciones con un modelo de cloud híbrido. Además, el análisis de la investigación también muestra que las organizaciones todavía necesitan una postura madura en cuanto a la seguridad del cloud, independientemente del modelo de cloud.

Figura 41: Una mayoría de los participantes en el estudio tenía un modelo operativo de TI con cloud híbrido, y un 45% indicó que tenía un modelo de cloud híbrido.
Por otro lado, el 28% indicó que su modelo de TI era totalmente local y el 27% dijo que su modelo de TI se basaba completamente en el cloud.

Figura 42: Casi la mitad de las organizaciones experimentaron una vulneración de datos en el cloud.
El 45% indicó que la vulneración de datos se produjo en el cloud, mientras que el 55% dijo que no se produjo en el cloud.

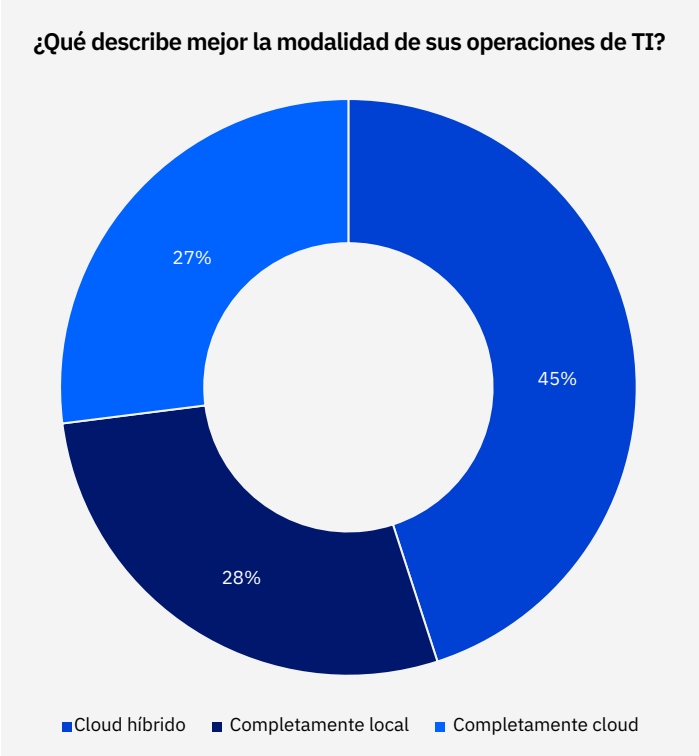


Figura 41

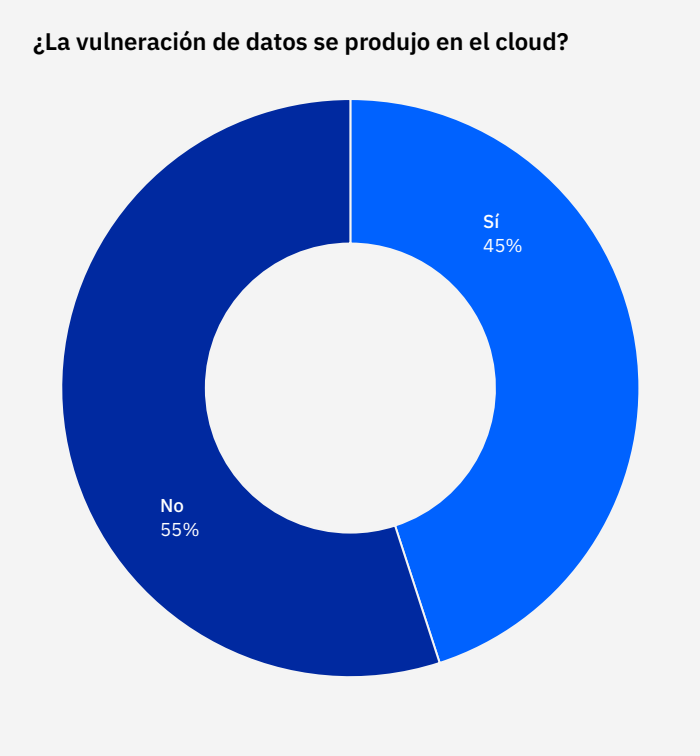


Figura 42

Estado de madurez de la seguridad en el entorno cloud

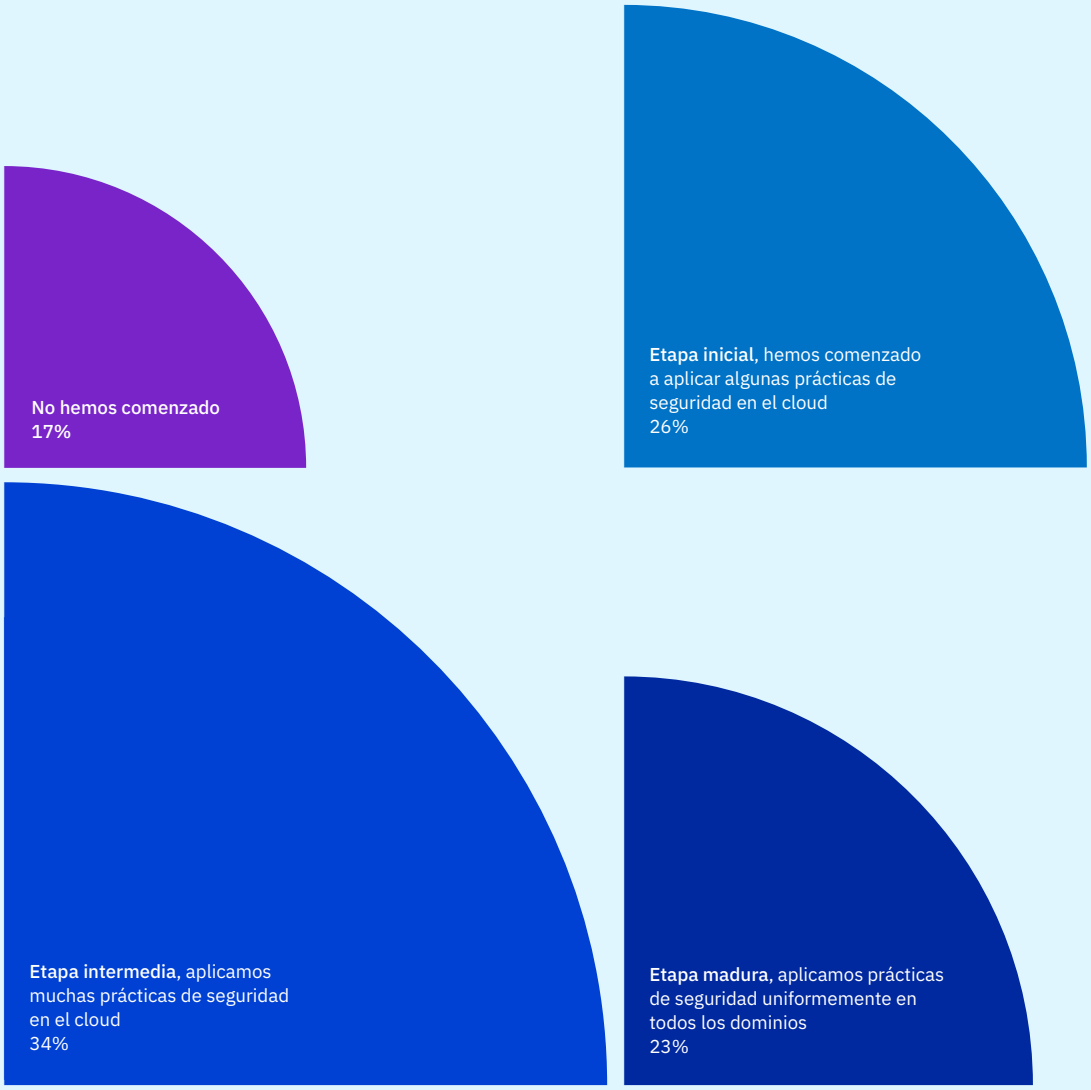


Figura 43

Figura 43: Casi la mitad de las organizaciones, un 43%, no había iniciado o estaba en las primeras etapas de aplicar las prácticas para proteger sus entornos de cloud.
Por otro lado, un 34% estaba en la etapa intermedia, aplicando muchas prácticas de seguridad en el cloud. Un 23% estaba en fase de madurez, aplicando prácticas de seguridad uniformemente en todos los dominios. Otro 26% de las organizaciones dijo que estaban en la etapa inicial, comenzando a aplicar algunas prácticas de seguridad en el cloud. Por último, el 17% de las organizaciones indicaron que no habían iniciado el proceso de proteger sus entornos de cloud.

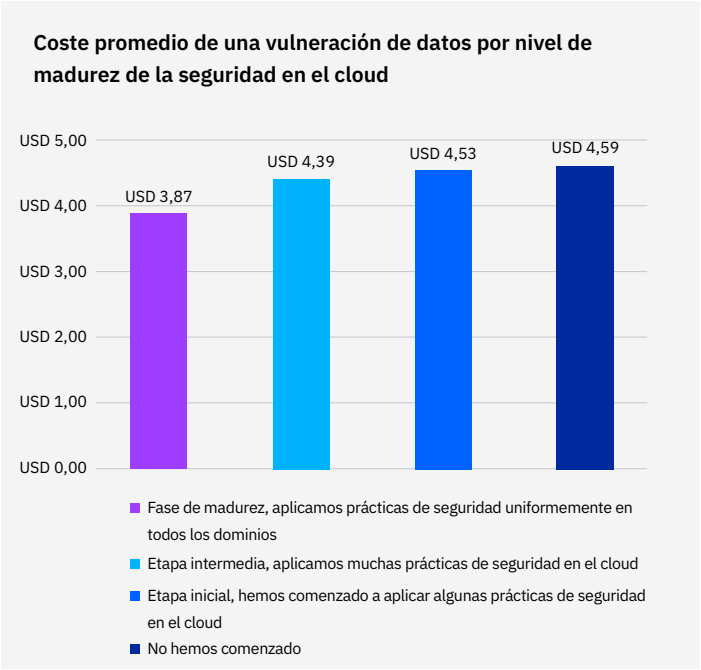


Figura 44: Medido en millones de dólares

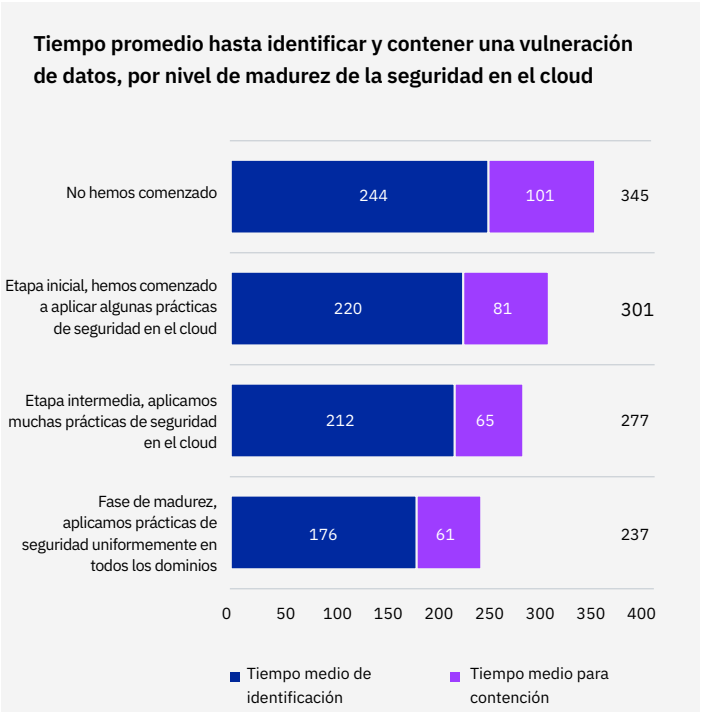


Figura 45: Medido en días

Figura 44: Las organizaciones con una seguridad en el cloud desarrollada tuvieron un coste inferior al promedio de una vulneración de datos.

En las organizaciones en fase de madurez, los costes de las vulneraciones fueron, en promedio, 660.000 dólares inferiores a las de las organizaciones que estaban transitando las primeras etapas de protección de sus entornos de cloud. Las vulneraciones en organizaciones en fase de madurez costaron un promedio de 3,87 millones de dólares, en comparación con los 4,39 millones de dólares en organizaciones en la etapa intermedia, 4,53 millones de dólares en las organizaciones en la etapa inicial y 4,59 millones de dólares en las organizaciones que no habían iniciado su proceso de seguridad en el cloud. La diferencia en el coste entre la etapa madura y la etapa inicial representa un ahorro del 15,7% para las organizaciones en la etapa madura. Nota: los costes de la vulneración en este análisis hacen referencia a cualquier tipo de vulneración, no solo las basadas en el cloud.

Figura 45: Las organizaciones en la etapa madura del proceso de protección de sus entornos de cloud fueron capaces de identificar y contener la vulneración de datos de forma más rápida que las organizaciones en la etapa inicial.

Las organizaciones en fase de madurez tuvieron un promedio de 176 días en identificar y 61 días en contener una vulneración, un total de 237 días combinados. Este ciclo de vida fue de 40 días menos que el promedio global de 277 días y 64 días menos que las organizaciones en la etapa inicial. Es decir, más de dos meses de diferencia, un 23,8%. Las organizaciones que no habían iniciado su proceso de seguridad del cloud se demoraron mucho más en identificar y contener la vulneración. El promedio para esas organizaciones fue de 345 días, 100 días más que las organizaciones en fase de madurez. Para las organizaciones en la etapa intermedia, el tiempo promedio hasta identificar y contener la vulneración de datos fue de 277 días, igual al promedio global general.

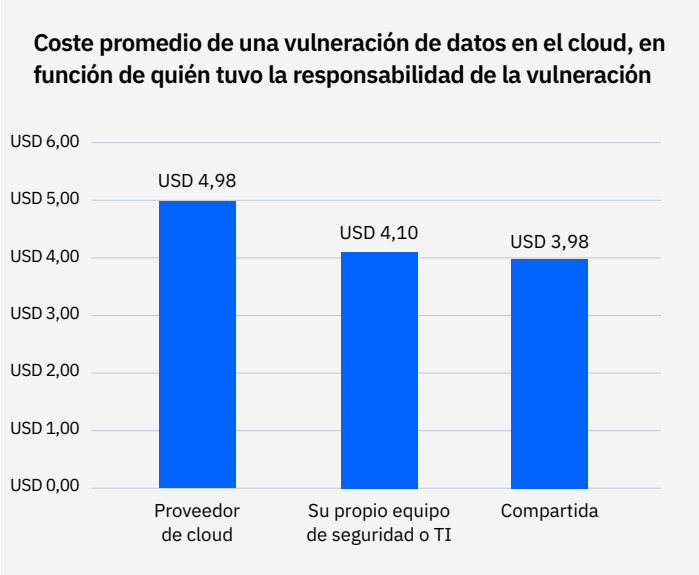


Figura 46: Medido en millones de dólares

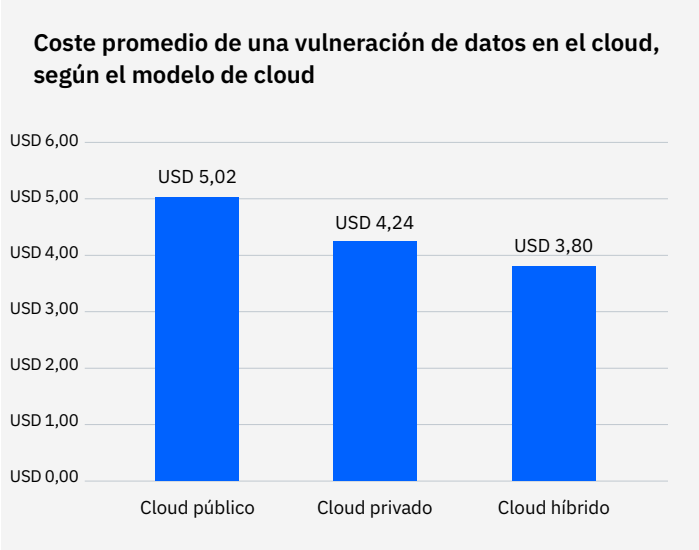


Figura 47: Medido en millones de dólares

Figura 46: Las vulneraciones que se consideraron responsabilidad del proveedor del cloud tuvieron el coste total promedio más elevado de una vulneración basada en el proveedor del cloud.
Las vulneraciones que fueron responsabilidad del proveedor de cloud tuvieron un coste total promedio de 4,98 millones de dólares. Las vulneraciones que se consideraron responsabilidad del propio equipo de TI o seguridad de una organización costaron como término medio 4,10 millones de dólares. Las vulneraciones que fueron responsabilidad compartida entre el proveedor del cloud y el equipo de TI o seguridad de la organización costaron un promedio de 3,98 millones de dólares. El coste promedio en los casos de responsabilidad compartida es 1 millón de dólares inferior al de las vulneraciones en las que el proveedor del cloud tuvo la responsabilidad. Una diferencia del 22,3%.

Figura 47: Las vulneraciones en el cloud público fueron las más costosas.
Las vulneraciones en un cloud público costaron un promedio de 5,02 millones de dólares. Mientras, las vulneraciones dentro de un cloud privado tuvieron un coste medio de 4,24 millones de dólares. Dentro del modelo de cloud híbrido, las vulneraciones costaron un promedio de 3,80 millones de dólares, aproximadamente 1,2 millones de dólares menos que lo que costaron las vulneraciones en una cloud pública, un 27,7% menos.

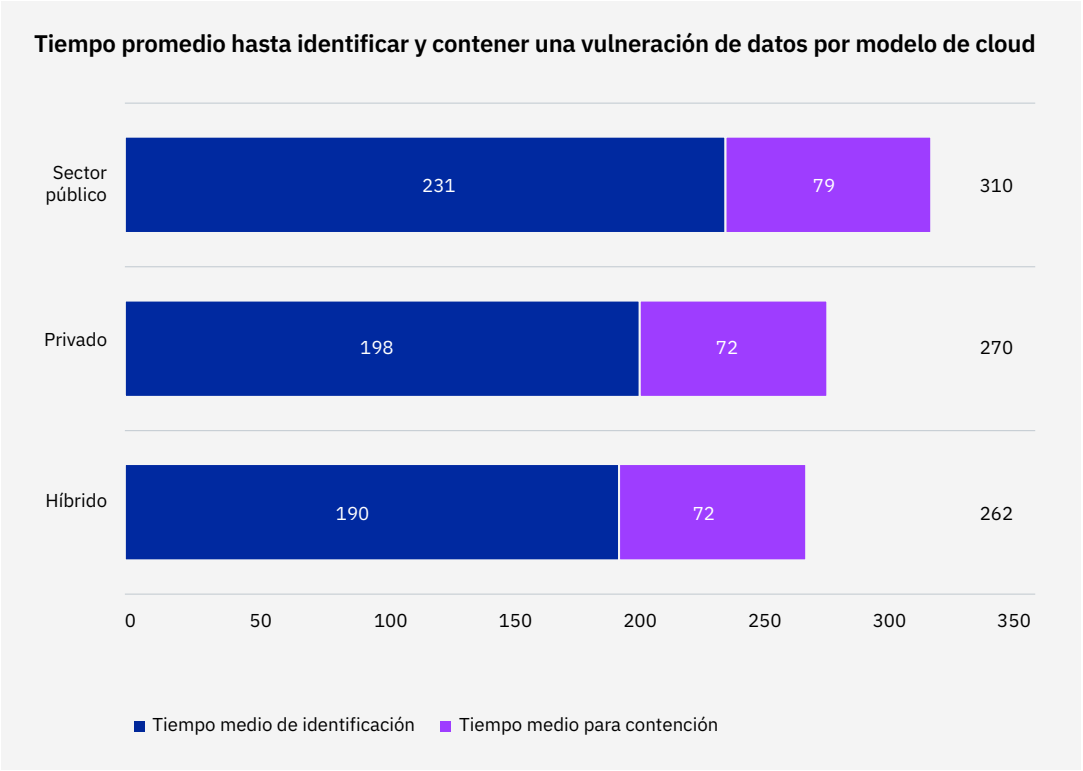


Figura 48: Medido en días

Figura 48: Las organizaciones con un modelo de cloud híbrido pudieron identificar y contener una vulneración significativamente más rápido, en promedio, que aquellas con modelos de cloud pública o privada.

El tiempo promedio hasta identificar y contener una vulneración con un modelo de cloud híbrido fue de 262 días. Este ciclo de vida fue 15 días menor que el promedio global de 277 días y ocho días menos que el del cloud privado. Se tardó un promedio de 310 días en identificar y contener las vulneraciones en organizaciones con un modelo de cloud público. Este ciclo de vida fue 48 días más que el cloud híbrido, un 16,8% más. Nota: dado que las implementaciones de cloud híbrido varían, este análisis incluyó vulneraciones locales, no meramente vulneraciones en el cloud.

1 millón de dólares

Los costes de la vulneración, en los casos en los que el teletrabajo fue un factor que causó la vulneración, fueron de aproximadamente 1 millón de dólares más que en las vulneraciones donde el teletrabajo no fue un factor

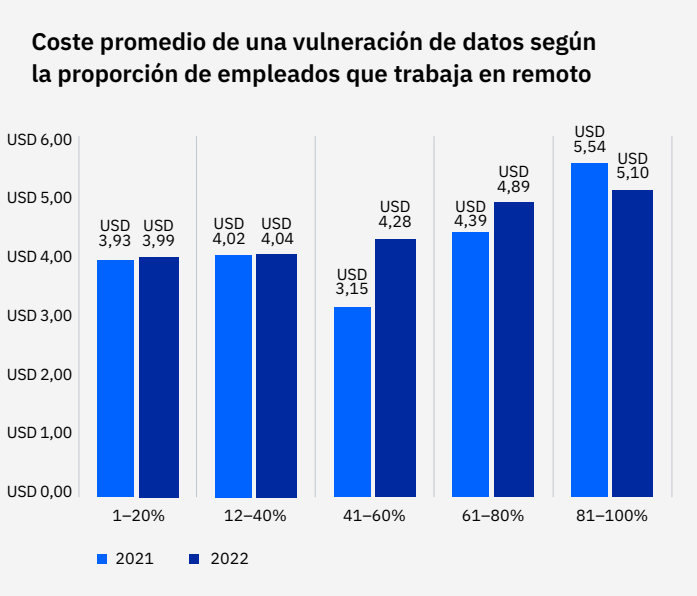


Figura 49: Medido en millones de dólares

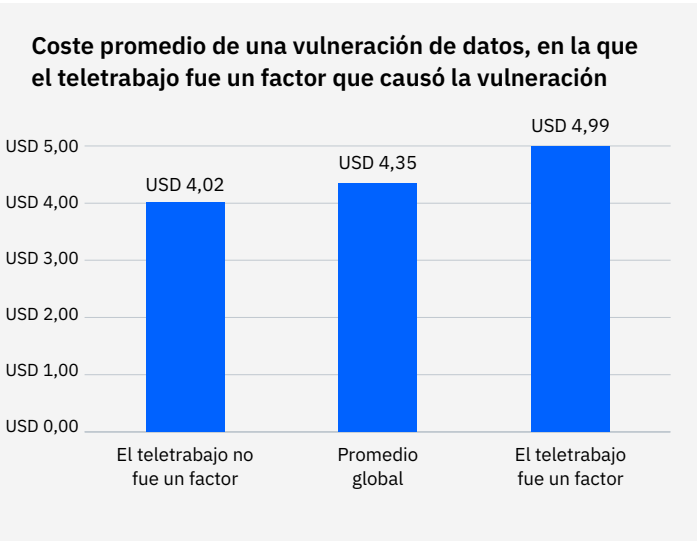


Figura 50: Medido en millones de dólares

Teletrabajo

Esta es la tercera vez que se ha publicado este informe desde el inicio de la pandemia de la COVID-19. En el contexto de la pandemia, a partir del informe del año pasado, hemos examinado los impactos del teletrabajo en los costes de las vulneraciones de datos. El teletrabajo ha tenido efectos considerables en el coste de una vulneración, cuando este fue uno de los factores que causó la vulneración, por ejemplo, en caso de robo de las credenciales a un empleado que realiza teletrabajo. El estudio también encontró que los costes de vulneración fueron más altos para las organizaciones con la mayoría de sus empleados trabajando de forma remota.

Figura 49: Hay una sólida correlación entre el teletrabajo y el coste de una vulneración de datos. El hecho de tener más empleados trabajando remotamente está asociado con costes superiores en la vulneración de datos.
Para las organizaciones con mayor proporción de empleados realizando teletrabajo, del 81% al 100%, el coste promedio de una vulneración de datos fue de 5,10 millones de dólares. Ese coste representó una leve disminución en esta categoría con respecto al año anterior.
Para las organizaciones con menor proporción de empleados realizando teletrabajo, menos del 20%, el coste promedio fue de 3,99 millones de dólares. La diferencia entre la proporción más alta y más baja de empleados realizando teletrabajo fue de 1,11 millones de dólares, una diferencia del 24,4%.

Figura 50: El coste total promedio de una vulneración de datos fue casi de 1 millón de euros más, cuando el teletrabajo fue un factor que causó la vulneración de datos.
Las organizaciones que señalaron el teletrabajo como un factor en la vulneración sufrieron un coste promedio de casi 5 millones de dólares en una vulneración de datos. Por el contrario, el coste promedio de una vulneración de datos fue de 4,02 millones de dólares, cuando el teletrabajo no fue un factor en la causa de la vulneración, una diferencia de 970.000 dólares, un 21,5%. Cuando el teletrabajo fue un factor, el coste también fue 640.000 dólares mayor que el promedio global general, una diferencia del 13,7%.

550.000 dólares

Ahorro promedio de costes de la vulneración de datos de una organización con suficiente dotación de personal versus una sin suficiente personal

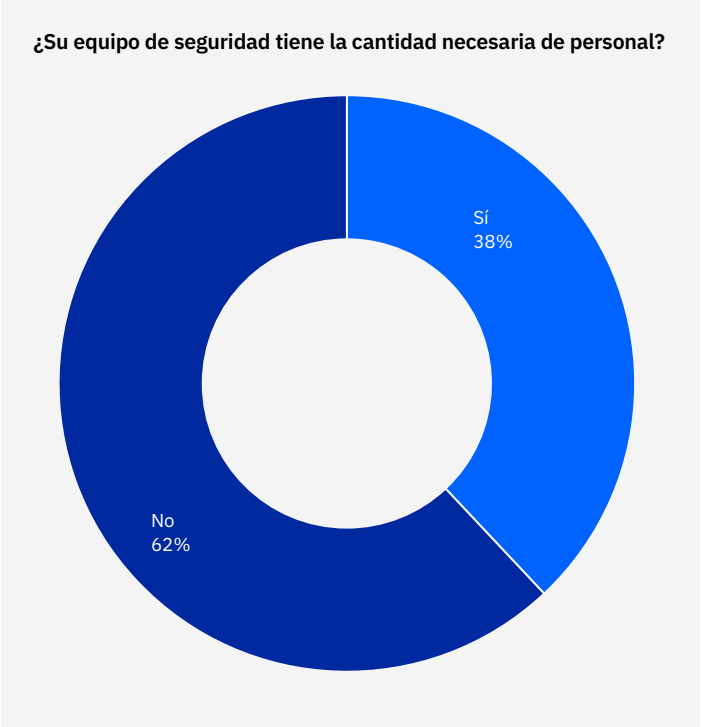


Figura 51

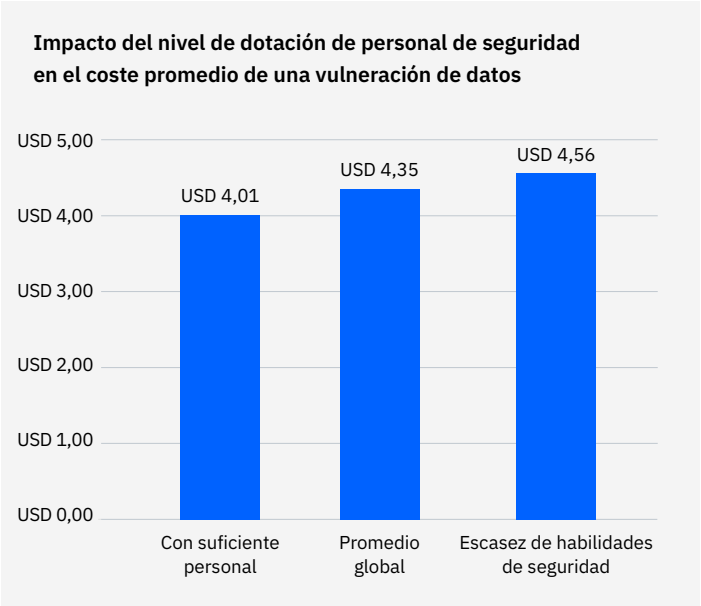


Figura 52: Medido en millones de dólares

Falta de competencias

Muchas organizaciones tienen dificultades para llenar vacantes en sus equipos de seguridad. Las organizaciones que ya contaban con suficiente dotación de personal tuvieron un ahorro de costes considerable en términos de costes de la vulneración de datos, en comparación con las que no tenían suficientes empleados para completar sus equipos. Este año, por primera vez este informe analiza con mayor detenimiento la carencia de competencias en seguridad.

Figura 51: Hubo una escasez generalizada de competencias de seguridad en las organizaciones estudiadas.
Solo algo más de un tercio de las organizaciones tuvieron equipos de seguridad con una dotación de personal suficiente. Solo un 38% de las organizaciones indicaron que sus equipos de seguridad contaban con suficiente personal para satisfacer las necesidades de gestión de la seguridad, mientras que un 62% indicó que no contaban con suficiente personal.

Figura 52: Las organizaciones que dijeron que sus equipos de seguridad tenían escasez de competencias tuvieron un coste superior al promedio de la vulneración de datos.
En las organizaciones con un equipo de seguridad con suficiente dotación de personal, el coste promedio de la vulneración de datos fue inferior al promedio. El coste promedio de una vulneración de datos en las organizaciones con suficiente dotación de personal fue de 4,01 millones de dólares. Por el contrario, el coste promedio de una vulneración de datos fue de 4,56 millones de dólares en las organizaciones con equipos de seguridad sin suficiente personal, una diferencia de 550.000 dólares, el 12,8%.

387 millones de dólares

Coste total promedio para las vulneraciones de 50 millones a 60 millones de registros

Megavulneraciones

Las megabrechas, es decir, aquellas con más de 1 millón de registros comprometidos, no son experiencias normales para la mayoría de las empresas. Pero estas megabrechas tienen un impacto impresionante en los consumidores y las industrias.

Este estudio incluyó 13 empresas que experimentaron una vulneración de datos que involucró la pérdida o el robo de entre 1 millón y 60 millones de registros. El estudio de las megabrechas incluyó una metodología diferente de la de las otras 550 vulneraciones estudiadas, cada una de las cuales no tuvo más de 100.000 registros perdidos. Para ver una explicación completa de la metodología de investigación, consulte “Preguntas frecuentes sobre la vulneración de datos” al final de este informe.

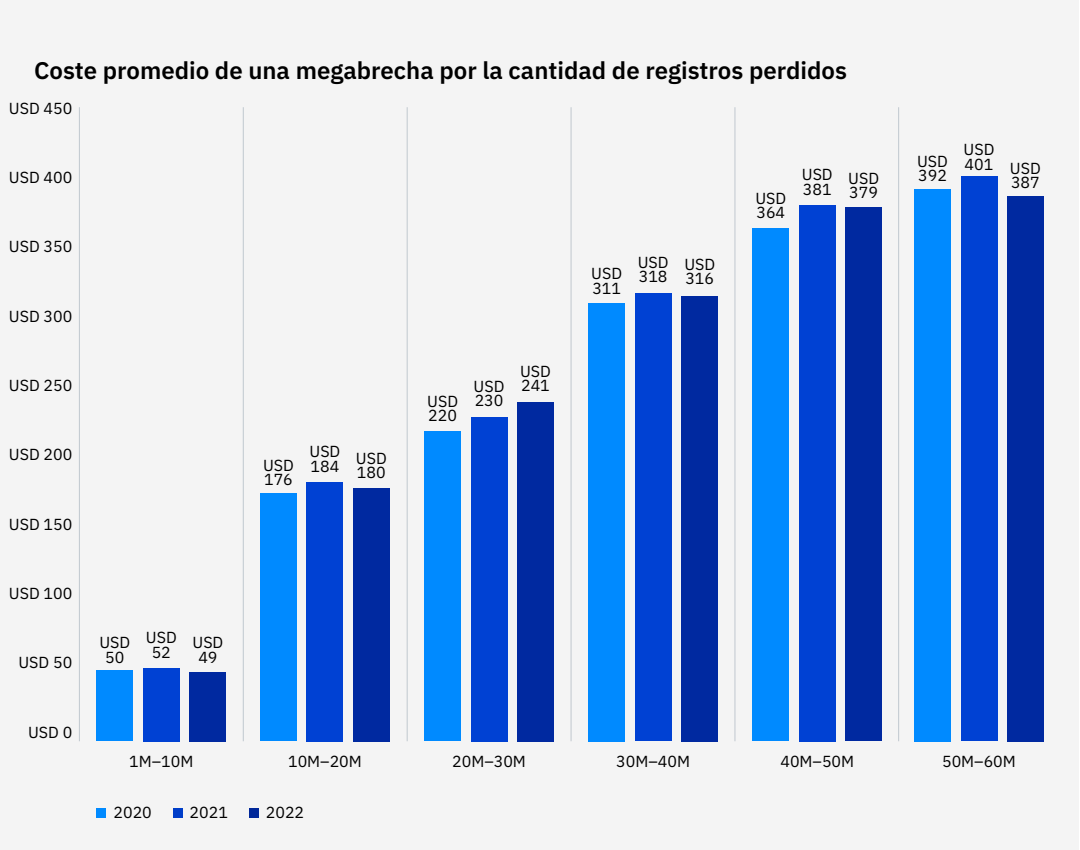


Figura 53: Medido en millones de dólares

Figura 53: En 2022, el coste promedio de una megabrecha disminuyó levemente.
Los costes de las megabrechas tuvieron una reducción con respecto a 2021 en seis de las siete variables de magnitud de la vulneración. El coste de las megabrechas más grandes, entre 50 millones y 60 millones de registros, disminuyó de los 401 millones de dólares en 2021 a 387 millones de dólares, una caída de 14 millones de dólares, un 3,6%. El segmento de 20 millones a 30 millones de registros fue el único que aumentó el promedio con respecto al año pasado. En ese segmento, el coste total promedio de una megabrecha aumentó de 230 millones de dólares a 241 millones de dólares, un incremento de 11 millones de dólares, un 4,8%.

Recomendaciones para ayudar a minimizar los impactos financieros de una vulneración de datos

En esta sección, IBM Security describe las medidas que pueden tomar las organizaciones para ayudar a reducir el coste financiero y las consecuencias para la reputación originadas por una vulneración de datos. Estas recomendaciones incluyen métodos de seguridad exitosos adoptados por organizaciones en el estudio.

Adopte un modelo de seguridad Zero trust para ayudar a prevenir el acceso no autorizado a datos confidenciales.
Los resultados del estudio demuestran que aunque solo un 41% de las organizaciones habían implementado un método de seguridad Zero trust, tuvieron un ahorro potencial de costes de vulneración de 1,5 millones de dólares con una implementación desarrollada. A medida que las organizaciones incorporan el teletrabajo y los entornos de multicloud híbrido, la estrategia Zero trust puede ayudar a proteger los datos y recursos, limitando su accesibilidad y exigiendo contexto.

Las herramientas de seguridad que pueden compartir datos entre sistemas distintos y centralizar las operaciones de seguridad de la información pueden ayudar a los equipos de seguridad a detectar las incidencias en entornos complejos de multicloud híbrido. Puede obtener información más detallada, mitigar riesgos y acelerar la respuesta, con una plataforma de seguridad abierta que hará avanzar su estrategia Zero trust. Al mismo tiempo, puede usar sus entornos existentes dejando su información donde se encuentra, ayudando a su equipo a ser más eficiente y colaborativo.

Proteja los datos confidenciales en los entornos de cloud con políticas y cifrado.
Con el aumento en la cantidad y el valor de los datos que se alojan en los entornos de cloud, las organizaciones deben tomar medidas para proteger las bases de datos alojadas en el cloud. Las prácticas de seguridad maduras en el cloud se asociaron con ahorros en los costes de las vulneraciones por 720.000 dólares, en comparación con la ausencia de prácticas de seguridad en el cloud. Use modelos de clasificación de los datos y programas de retención para ayudar a aportar visibilidad y reducir el volumen de información confidencial que se encuentra expuesta a una vulneración. Proteja la información confidencial con cifrado de datos y cifrado totalmente homomórfico. Usar una infraestructura interna para las auditorías, evaluar el riesgo en toda la empresa y realizar un seguimiento del cumplimiento de los requisitos normativos puede ayudar a mejorar su habilidad para detectar una vulneración de datos y escalar los esfuerzos de contención.

Invierta en orquestación, automatización y respuesta de seguridad (SOAR) y XDR para ayudar a mejorar los tiempos de detección y respuesta.
Acompañadas por la IA y automatización de seguridad, las prestaciones de XDR pueden ayudar a reducir significativamente los costes promedio de las vulneraciones de datos y sus ciclos de vida. Según el estudio, las organizaciones con XDR implementado acortaron el ciclo de vida de la vulneración en 29 días como promedio, en comparación con las organizaciones que no implementaron XDR, con un ahorro de costes de 400.000 dólares. El software de SOAR y gestión de eventos e información de seguridad (SIEM), los servicios de detección y respuesta gestionada, y XDR, pueden ayudar a su organización a acelerar la respuesta a las incidencias, con la automatización, estandarización de procesos e integración con sus herramientas de seguridad existentes.

Use herramientas que ayuden a proteger y supervisar los endpoints y empleados remotos.
En el estudio, las vulneraciones en las que el teletrabajo fue un factor que causó la vulneración costaron casi 1 millón de dólares más que las vulneraciones en las que el teletrabajo no fue el factor desencadenante. Los productos y servicios de gestión unificada de endpoints (UEM), detección y respuesta de endpoint (EDR) y gestión de identidad y acceso (IAM) pueden ayudar a dar una mayor visibilidad a los equipos de seguridad respecto de la actividad sospechosa. Esta supervisión, incluye que traiga su propio dispositivo móvil (BYOD) y los ordenadores portátiles, de escritorio, tabletas, dispositivos móviles e IoT de la empresa, incluyendo los endpoints a los que no tiene acceso físico la empresa. UEM, EDR y IAM aceleran el tiempo de investigación y respuesta para aislar y contener el daño en las vulneraciones, en las que el teletrabajo fue un factor.

Cree y pruebe guías de estrategias de respuesta a incidencias para aumentar la resiliencia cibernética.
Dos de las formas más eficaces de mitigar el coste de una vulneración de datos son formar un equipo de respuesta a incidencias (RI) y realizar pruebas amplias del plan de RI. Las vulneraciones en las organizaciones con equipos de RI que prueban regularmente su plan tuvieron un ahorro de 2,66 millones de dólares, en comparación con las vulneraciones en organizaciones sin equipo de RI ni pruebas del plan de RI. Las organizaciones pueden responder rápidamente para contener las repercusiones de una vulneración si establecen una guía de estrategias detallada para incidencias cibernéticas. Pruebe de forma habitual ese plan mediante ejercicios de sobremesa o ejecute un escenario de vulneración en un entorno simulado, como un campo cibernético.

Los ejercicios de simulación de adversarios, que también se conocen como ejercicios de equipo rojo, pueden aumentar la eficacia de los equipos de RI, dado que descubren las vías y técnicas de ataque omitidas, identificando las carencias en sus prestaciones de detección y respuesta. Una solución de gestión de la superficie de ataque puede ayudar a las organizaciones a mejorar su postura de seguridad mediante la localización de los puntos de exposición previamente desconocidos, mediante simulaciones de una experiencia de ataque auténtica.

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

Datos demográficos de las organizaciones

El estudio de este año incluye a 550 organizaciones de diversos tamaños, ubicaciones geográficas y sectores. Esta sección muestra el desglose de las organizaciones del estudio por ubicación geográfica e industria, además de que incluye las definiciones utilizadas para clasificar a las organizaciones por industria.

17 años

Estados Unidos ha formado parte del estudio durante un largo período de tiempo de 17 años

Datos demográficos geográficos

El estudio de 2022 se realizó en 17 países o muestras regionales.

Panorama general del estudio global

Países	Muestra de 2022	Porcentaje	Años de estudio	Moneda
Estados Unidos	64	12%	17	USD
India	49	9%	11	INR
Reino Unido	43	8%	15	GBP
Brasil	43	8%	10	BRL
Alemania	38	7%	14	EUR
Japón	35	6%	11	JPY
Francia	33	6%	13	EUR
Medio Oriente[1]	31	6%	9	SAR
Corea del Sur	30	5%	5	KRW
Australia	26	5%	13	AUD
Canadá	25	5%	8	CAD
Italia	24	4%	11	EUR
Sudeste Asiático[2]	23	4%	6	SGD
Latinoamérica[3]	23	4%	3	MXN
Sudáfrica	21	4%	7	ZAR
Escandinavia[4]	20	4%	4	NOK
Turquía	20	4%	5	TRY
Total	**550**	**100%**		

1. El Medio Oriente es una muestra de empresas ubicada en Arabia Saudí y los Emiratos Árabes Unidos.
2. ASEAN es una muestra de empresas que se encuentran en Singapur, Indonesia, Filipinas, Malasia, Tailandia y Vietnam.
3. Latinoamérica es una muestra de empresas localizadas en México, Argentina, Chile y Colombia.
4. Escandinavia es una muestra de empresas en Dinamarca, Suecia, Noruega y Finlandia.

Figura 54

Las muestras más grandes de industrias pertenecen a estos sectores.

16% Sector financiero

12% Servicios

12% Industrial

11% Tecnología

Datos demográficos de las industrias

El estudio de este año se realizó en 17 industrias, las mismas que se han incluido en el estudio durante varios años.

Distribución de la muestra por sector

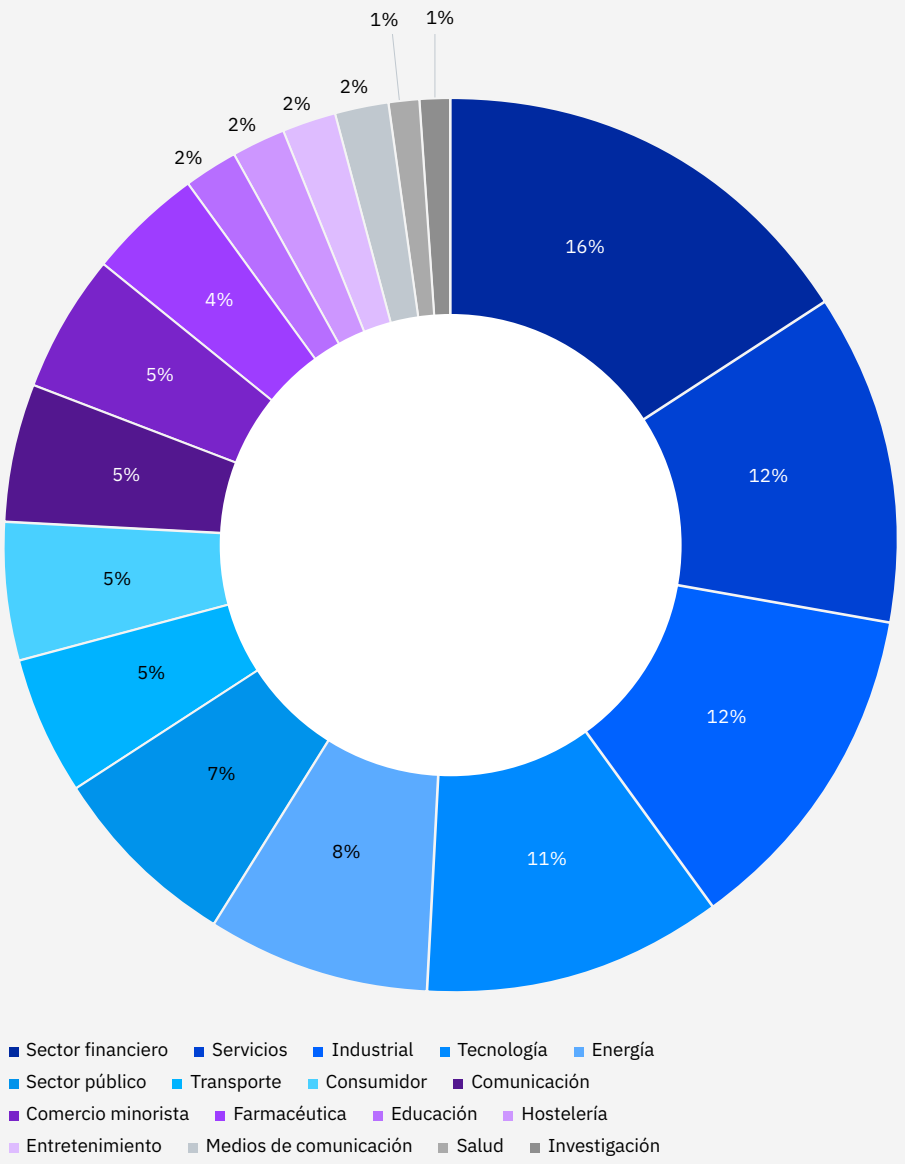


Figura 55

Definiciones de las industrias

Atención sanitaria
Hospitales, clínicas

Sector financiero
Bancos, empresas de seguros, empresas de inversiones

Energía
Empresas de petróleo y gas, servicios públicos, productores y proveedores de energías alternativas

Farmacéutica
Farmacéutica, incluye ciencias biomédicas de la salud

Industrial
Empresas de procesamiento de sustancias químicas, ingeniería y fabricación

Tecnología
Empresas de software y hardware

Educación
Universidades y escuelas superiores públicas y privadas, empresas de formación y desarrollo

Servicios
Servicios profesionales como empresas de asesoramiento legal, contable y consultoría

Entretenimiento
Producción de películas, deportes, juegos y casinos

Transporte
Compañías aéreas, ferroviarias, de camiones y de reparto

Comunicación
Periódicos, editoriales de libros, relaciones públicas y agencias publicitarias

Consumidor
Fabricantes y distribuidores de productos de consumo

Medios de comunicación
Televisión, satélites, redes sociales, Internet

Hostelería
Hoteles, cadenas de restaurantes, líneas de cruceros

Comercio minorista
Tiendas tradicionales y comercio electrónico

Investigación
Investigación de mercado, think tanks, investigación y desarrollo

Sector público
Organismos gubernamentales federales, estatales y locales y organizaciones no gubernamentales (ONG)

Metodología de investigación

Para mantener la confidencialidad, el instrumento de referencia no capturó información específica de ninguna empresa. Los métodos de recopilación de datos excluyeron la información contable real, basándose en la estimación que hicieron los participantes de los costes directos, al marcar una variable en un rango de una línea numérica. Se indicó a los participantes que marcaran la línea numérica en un punto entre los límites inferior y superior del rango para cada categoría de costes.

El valor numérico obtenido de esa línea, en lugar de un punto estimado para cada categoría de costes presentada, conservó la confidencialidad, garantizando una tasa superior de respuesta. El instrumento de referencia también solicitó a los encuestados que proporcionaran una segunda estimación para los costes de oportunidad y costes indirectos, por separado.

Para asegurarnos de tener un tamaño manejable para la evaluación comparativa, limitamos minuciosamente los elementos únicamente a centros de actividad de costes que consideramos cruciales, para medir los costes de las vulneraciones de datos. Con base en lo hablado con los expertos, el conjunto final de elementos incluyó un grupo fijo de actividades de costes. Después de recopilar la información de referencia, volvimos a examinar cada instrumento detenidamente para comprobar la uniformidad e integridad.

Limitamos el ámbito de los costes de la vulneración de datos a las categorías de costes conocidas que aplicamos a un conjunto amplio de operaciones comerciales que gestionan información personal. Nuestra creencia fue que un estudio centrado en los procesos de la empresa, no en las actividades de cumplimiento de la privacidad o protección de datos, daría resultados de mejor calidad.

Esta investigación utilizó un costeo basado en la actividad, que identifica las actividades y asigna un coste según el uso real.

Cómo calculamos el coste de una vulneración de datos

Para calcular el coste promedio de una vulneración de datos, esta investigación excluyó a las vulneraciones muy pequeñas y muy grandes. Las vulneraciones de datos examinadas en el estudio de 2022 variaron en tamaño entre 2200 y 102.000 registros comprometidos. Usamos un análisis separado para examinar los costes de las megabrechas mayores, lo cual se explica en mayor detalle en la sección “Preguntas frecuentes sobre la vulneración de datos” del informe.

Esta investigación utilizó un costeo basado en la actividad, que identifica las actividades y asigna un coste según el uso real. Hay cuatro actividades relacionadas con los procesos que impulsan un rango de gastos asociado con la vulneración de datos de una organización: detección y escalamiento, notificación, respuesta posterior a la vulneración y pérdida de negocios.

Detección y escalamiento
Las actividades que permiten que una empresa detecte razonablemente la vulneración, incluidas las siguientes:
- Actividades forenses y de investigación
- Servicios de evaluación y auditoría
- Gestión de crisis
- Comunicaciones para ejecutivos y Juntas

Notificación
Actividades que permiten que la empresa avise a los sujetos de los datos, a los organismos de control de protección de datos y a otros terceros, incluidas las siguientes:
- Correos electrónicos, cartas, llamadas salientes o avisos generales a los sujetos de los datos
- Determinación de los requisitos normativos
- Comunicación con los organismos de control
- Involucramiento de expertos externos

Respuesta posterior a la vulneración
Actividades que ayudan a las víctimas de una vulneración a comunicarse con la empresa y actividades de compensación para víctimas y organismos de control, incluyendo las siguientes:
- Servicio de asistencia técnica y comunicaciones entrantes
- Servicios de protección de identidad y supervisión del crédito
- Emisión de cuentas o tarjetas de crédito nuevas
- Gastos legales
- Descuentos en productos
- Multas normativas

Pérdida de negocios
Actividades que intentan minimizar la pérdida de clientes, la interrupción del negocio y las pérdidas de ingresos, incluyendo las siguientes:
- Interrupción del negocio y pérdidas de ingresos por tiempo de inactividad del sistema
- Coste de pérdida de clientes y adquisición de clientes nuevos
- Pérdidas de reputación y fondo comercial perjudicado

Preguntas frecuentes sobre la vulneración de datos

¿Qué es una vulneración de datos?
Una vulneración de datos se define como un evento en el que quedan potencialmente en riesgo el nombre de una persona y un registro médico, un registro financiero o ambos o una tarjeta de débito. Estos registros pueden tener formato en papel o electrónico. Las vulneraciones incluidas en el estudio abarcaron entre 2200 y 102.000 registros comprometidos.

¿Qué es un registro comprometido?
Un registro es información que identifica a la persona física o al individuo, cuya información se ha perdido o ha sido robada en una vulneración de datos. Entre otros, un ejemplo es una base de datos con el nombre de la persona, la información de su tarjeta de crédito y otra información de identificación personal, o un registro médico con el nombre del titular de la póliza y la información de pago.

¿Cómo recopilamos la información?
Nuestros investigadores recopilaron información cualitativa de alta calidad a través de 3600 entrevistas separadas, con personas de 550 organizaciones que sufrieron una vulneración de datos entre marzo de 2021 y marzo de 2022. Las personas entrevistadas incluyeron profesionales de TI, cumplimiento y seguridad de la información, que estaban familiarizadas con la vulneración de datos de la organización y los costes asociados a la resolución de ésta. Por motivos de privacidad, no recopilamos información específica de las organizaciones.

¿Cómo calculamos el coste promedio de una vulneración de datos?
Reunimos tanto los gastos directos como indirectos en los que incurrió la organización. Los gastos directos incluyen la contratación de expertos forenses, la externalización de la asistencia telefónica y la entrega de suscripciones gratuitas de supervisión del crédito y descuentos, para productos y servicios futuros. Los costes indirectos incluyen investigaciones y comunicaciones internas y el valor extrapolado de la pérdida de clientes producida en la facturación o la disminución en los porcentajes de adquisición de clientes.

Esta investigación representa únicamente eventos directamente relevantes para la experiencia de vulneración de datos. Las normas como el “Reglamento General de Protección de Datos (RGPD)” y la “Ley de Privacidad de los Consumidores de California (CCPA)”, podrían alentar a las organizaciones a aumentar la inversión en tecnologías de regulación de la ciberseguridad. Sin embargo, este tipo de actividades no afectó directamente al coste de una vulneración de datos para esta investigación.

Para mantener una uniformidad con los años anteriores, usamos el mismo método de conversión de moneda en lugar de ajustar los costes contables.

¿En qué se diferencia la investigación estándar de la investigación mediante encuestas?
La unidad de análisis en el informe de Coste de la vulneración de datos fue la organización. En la investigación mediante encuesta, la unidad de análisis es la persona. Contactamos con 550 organizaciones para que participaran en este estudio.

¿El coste promedio por registro se puede usar para calcular el coste de las vulneraciones que incluyeron millones de registros perdidos o robados?
El coste promedio de las vulneraciones de datos en nuestra investigación no es aplicable a las megavulneraciones o a las vulneraciones de datos catastróficas, como Equifax, Capital One o Facebook. Estos eventos no son típicos de las vulneraciones que experimentan muchas organizaciones. Para extraer conclusiones útiles y comprender el comportamiento de los costes de las vulneraciones de datos, pusimos el foco en incidentes de vulneración de datos que no excedieron los 102.000 registros.

No es consistente con esta investigación el uso del coste por registro para calcular el coste de una vulneración o varias cuándo se superan los millones de registros. No obstante, el estudio utiliza una infraestructura de simulación para medir el impacto en el coste de una megabrecha con 1 millón de registros o más, con base en una muestra de 13 vulneraciones muy grandes con este volumen.

¿Por qué se usaron métodos de simulación para estimar el coste de una megavulneración de datos?
El tamaño de la muestra con 13 empresas que experimentaron una megabrecha fue demasiado pequeño para realizar un análisis estadístico significativo mediante métodos de costes basados en actividades. Para subsanar esta cuestión, implementamos la simulación Monte Carlo para estimar un rango de resultados posibles, es decir, aleatorios, mediante pruebas repetidas.

En total, realizamos más de 150.000 pruebas. La media global de todas las medias de la muestra proporcionó un resultado más probable en cada magnitud de vulneración de datos, en el rango de 1 millón hasta 60 millones de registros comprometidos.

¿Se realiza un seguimiento de las mismas organizaciones cada año?
Cada estudio anual incluye una muestra diferente de empresas. Para guardar uniformidad con informes anteriores, captamos y combinamos cada año a empresas con características similares, como el sector al que pertenecen, la cantidad de empleados, la magnitud geográfica y el tamaño de la vulneración de datos. Desde que iniciamos esta investigación en 2005, hemos estudiado las experiencias de vulneración de datos de 5027 organizaciones.

La evaluación de referencias no captó información que identificara a las empresas.

Limitaciones de la investigación

Nuestro estudio empleó un método patentado y confidencial para la evaluación comparativa que se ha implementado exitosamente en investigaciones anteriores. Sin embargo, las limitaciones inherentes en este tipo de investigaciones deben considerarse detenidamente, antes de extraer conclusiones a partir de esos hallazgos.

Resultados no estadísticos
Nuestro estudio tomó una muestra representativa y no estadística de entidades globales. Las inferencias estadísticas, los márgenes de error y los intervalos de confianza, no pueden aplicarse a estos datos, dado que nuestros métodos de muestreo no fueron científicos.

Sin respuesta
El sesgo de la ausencia de respuesta no se evaluó, así que es posible que las empresas que no participaron tengan diferencias sustanciales, en términos del coste subyacente de la vulneración de datos.

Sesgo del marco de muestreo
Como nuestro marco de muestreo se basó en nuestro criterio, la calidad de los resultados se vio influenciada por el grado en el que el marco representó la población de empresas que se estaban estudiando. Creemos que el marco de muestreo actual tuvo un sesgo en pos de las empresas con programas de seguridad de la información o privacidad más desarrollados.

Información específica de las empresas
La evaluación de referencias no capturó información que identificara a las empresas. Las personas podían usar variables de respuestas categóricas para divulgar información demográfica acerca de la empresa y la categoría de la industria.

Factores no medidos
Omitimos variables de nuestros análisis como tendencias principales y características de las organizaciones. No se puede determinar en qué medida las variables omitidas podrían explicar los resultados de las referencias.

Resultados de costes extrapolados
Aunque se pueden incorporar ciertos controles y balances al proceso de evaluación comparativa, siempre es posible que los encuestados no proporcionaran respuestas correctas o verdaderas. Además, el uso de métodos de extrapolación de costes, en lugar de datos de costes reales, podría introducir sesgos e imprecisiones de forma indeseada.

Conversiones de monedas
La conversión de las monedas locales a dólares estadounidenses disminuyó las estimaciones de costes totales promedio en otros países. A fin de mantener la uniformidad con años anteriores, decidimos seguir usando el mismo método contable en lugar de ajustar el coste.

Acerca de Ponemon Institute e IBM Security

Ponemon Institute

Ponemon Institute se dedica a la investigación y formación independiente, fomentando el avance de las prácticas responsables de gestión de la privacidad y la información dentro de las empresas y el gobierno. Nuestra misión es realizar estudios empíricos de alta calidad sobre temas cruciales que afectan a la gestión y seguridad de la información confidencial, sobre personas y organizaciones.

Ponemon Institute mantiene normas estrictas de confidencialidad de la información, privacidad e investigación ética, y no recopila en sus investigaciones información alguna de identificación personal de personas, ni información de identificación de las empresas. Asimismo, las estrictas normas de calidad garantizan que no se realicen a los sujetos preguntas extrañas, irrelevantes ni inadecuadas.

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 renombrada a nivel global IBM Security X-Force®, proporciona soluciones de seguridad que ayudan a las organizaciones a incluir la seguridad en la estructura de sus negocios, para poder prosperar ante la incertidumbre.

IBM opera una de las organizaciones de facilitación, desarrollo e investigación de seguridad más amplias y de mayor rigor. IBM, que supervisa más de 4,7 billones de eventos por mes en más de 130 países, tiene más de 10.000 patentes de seguridad. Para obtener más información, visite ibm.com/es-es/security. Súmese a la conversación en la IBM Security Community.

Si tiene preguntas o comentarios sobre este informe de investigación, incluso si quiere solicitar autorización para citarlo o reproducirlo, no dude en ponerse en contacto por carta, teléfono o correo electrónico:

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City
Michigan 49686 USA

+1.800.887.3118
research@ponemon.org

Dé los siguientes pasos

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

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

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

Orquestación, automatización y respuesta de seguridad
Acelere la respuesta a las incidencias mediante la orquestación y la automatización.
Más información

Gestión de eventos e información de seguridad
Obtenga visibilidad para detectar, investigar y responder a las amenazas.
Más información

Seguridad en el cloud
Integre la seguridad en su transición al multicloud híbrido.
Más información

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

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

Respuesta a incidencias e información de amenazas
Gestione y responda proactivamente a amenazas de seguridad.
Más información

Programe una consulta individual con un experto de IBM Security X-Force
Programe su cita

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

Producido en los
Estados Unidos de América
Julio de 2022