Estudio de 2016 sobre los costes de las filtraciones de datos: Análisis global

Investigación de benchmarking patrocinada por IBM
Realizada de forma independiente por Ponemon Institute LLC
Junio de 2016

Informe de investigación del Ponemon Institute©

Estudio de 2016[1] sobre los costes de las filtraciones de datos: Análisis global

Ponemon Institute, Junio de 2016

Parte 1. Introducción

IBM y el Ponemon Institute acaban de presentar el *Estudio de 2016 sobre los costes de las filtraciones de datos: Análisis global*. De acuerdo con nuestra investigación, el coste medio total de una filtración de datos para las 383 empresas que participan en este estudio ha ascendido de 3,79 a 4 millones de dólares[2]. El coste medio pagado por cada registro perdido o robado con información sensible y confidencial ha ascendido de 154$ en 2015 a 158$.

Además de datos de costes, nuestro estudio global analiza la posibilidad de que una empresa sufra una o más filtraciones de datos en los próximos 24 meses. Estimamos una probabilidad del 26 % de una filtración de datos materiales con 10.000 registros perdidos o robados.

Estudio global en cifras

- 383 empresas en 12 países
- 4$ millones es el coste medio de una filtración de datos
- Aumento del 29 % en el coste de una filtración desde 2013
- 158$ es el coste medio por registro perdido o robado
- Incremento del 15 % en el coste per cápita desde 2013

De acuerdo con las conclusiones de este año, las organizaciones con mayor probabilidad de sufrir una filtración de datos materiales con 10.000 registros implicados o más son las ubicadas en Brasil y Sudáfrica. Por el contrario, las organizaciones de Alemania y Australia son las que tienen una probabilidad menor de sufrir una filtración de datos materiales.

En el estudio de este año participaron 383 empresas ubicadas en los siguientes 12 países: Estados Unidos, Reino Unido, Alemania, Australia, Francia, Brasil, Japón, Italia, India, la Región Árabe (Emiratos Árabes Unidos y Arabia Saudí), Canadá y, por primera vez, Sudáfrica. Todas ellas han sufrido una filtración de datos con registros comprometidos que oscilan entre aproximadamente 3.000 a más de 101.500[3]. Definimos un registro comprometido como uno que identifica la persona cuya información ha sido robada o perdida en la filtración de datos.

Siete megatendencias globales extraídas del estudio sobre el coste de las filtraciones

A lo largo de muchos años estudiando las filtraciones de datos sufridas por 2.013 empresas de cada sector, la investigación ha revelado las siguientes siete megatendencias.

1. Desde que se inició esta investigación, el coste de una filtración de datos no ha fluctuado de manera significativa, lo que sugiere que es un coste permanente que las organizaciones tienen que aprender a gestionar e incorporarlo en sus estrategias de protección de datos.

2. La mayor consecuencia financiera para las organizaciones que sufren una filtración de datos es el negocio perdido. Tras una filtración, hay que tomar medidas para mantener la confianza del cliente y reducir el impacto financiero a largo plazo.

3. La mayoría de las filtraciones de datos son causadas por ataques maliciosos y delictivos, que además son las que se tarda más en detectar y contener. Por lo tanto, son las que tienen un coste por registro más elevado.

4. Las organizaciones reconocen que cuanto más se tarde en detectar y contener una filtración, más costará su resolución. Con los años, los costes de detención y escalado se

[1] La fecha de este informe refleja el año de publicación en lugar de la fecha de finalización del trabajo de campo. Tenga en cuenta que la mayoría de los incidentes de filtraciones estudiados en el presente informe se produjeron en el 2015.

[2] Las monedas locales se han convertido a dólares americanos.

[3] Los términos “coste por registro comprometido” y “coste per cápita” tienen un significado equivalente en este informe.

han incrementado. Esto indica que se realizan inversiones en tecnologías y experiencia.

5. Sectores regulados, como la sanidad y los servicios financieros registran las filtraciones más costosas debido a las multas y a que el porcentaje de clientes o negocios perdidos es superior al promedio.
6. Mejoras en programas de gobierno de datos reducirían el coste de las filtraciones. Los planes de respuesta ante incidentes, el nombramiento de un CISO, la formación de empleados y programas de concienciación, así como una estrategia de gestión de continuidad del negocio son medidas que suponen un ahorro de costes.
7. Las inversiones en determinados controles y actividades de prevención de pérdida de datos, como las soluciones de seguridad de puntos finales y el cifrado son importantes para prevenir filtraciones. Este estudio ha revelado una reducción del coste cuando las empresas compartieron amenazas y desplegaron tecnologías de prevención de pérdida de datos.

Estos son los principales hallazgos e implicaciones para las organizaciones:

Las filtraciones de datos tienen el mayor coste en Estados Unidos y Alemania, y el menor en Brasil e India. El coste medio per cápita de una filtración de datos fue de 221$ en Estados Unidos y de 213$ en Alemania. El coste más bajo fue en Brasil (100$) e India (61$). El coste organizativo medio total en Estados Unidos fue de 7,01 millones y en Alemania de 5,01 millones. El coste más bajo para la organización fue en India (1,6 millones) y Sudáfrica (1,87 millones).

El coste de una filtración de datos varía según el sector. El coste medio global de una filtración de datos por registro perdido o robado fue de 158$. Sin embargo, las organizaciones sanitarias tuvieron un coste medio de 355$ y en educación el coste medio fue de 246$. El transporte (129$), investigación (112$) y el sector público (80$) fueron las que registraron un coste inferior.

Los hackers y los delincuentes internos provocaron la mayoría de las filtraciones de datos. El 48 % de todas las filtraciones del estudio de este año fueron consecuencia de ataques maliciosos o delictivos. El coste medio por registro para resolver esta clase de ataques fue de 170$. En contraste, los fallos del sistema costaron 138$ por registro y el error humano o la negligencia 133$ por registro. Las empresas de Estados Unidos y Canadá son las que más gastaron en resolver un ataque malicioso o delictivo (236$ y 230$ por registro, respectivamente). India gastó mucho menos (76$ por registro).

Los ataques maliciosos o delictivos varían significativamente por país. El 60 % de todas las filtraciones en los países árabes y el 54 % de todas las filtraciones en Canadá fueron causadas por hackers o delincuentes internos. Solo el 37 % de todas las filtraciones de datos que se producen en Sudáfrica fueron consecuencia de ataques maliciosos. Por el contrario, las empresas sudafricanas presentaron el porcentaje más alto de filtraciones de datos por error humano, y las de la India la mayor probabilidad de sufrir una filtración de datos debido a un fallo del sistema o del proceso de negocio (37 % y 35 %, respectivamente).

Los equipos de respuesta ante incidentes y un amplio uso de cifrado disminuyeron el coste de las filtraciones. Un equipo de respuesta ante incidentes redujo el coste de las filtraciones 16$ por registro, de 158 a 142. En cambio, las filtraciones debidas a la implicación de terceros aumentaron 14$, de 158 a 172 por registro.

Las medidas revelan por qué se incrementó el coste. El coste medio total de una filtración de datos aumentó un 5,4 % y el coste per cápita o registro un 2,9 %. El tamaño medio de la filtración (número de registros perdidos o robados) aumentó un 3,2 %. El abandono anómalo creció un 2,9 %, que se define como una pérdida de clientes mayor de lo esperado en el transcurso normal del negocio.

La pérdida de clientes incrementó el coste de las filtraciones de datos. Determinados países tuvieron más problemas para retener clientes tras una filtración y, por tanto, mayores costes.

Es el caso de Francia, Japón e Italia. Los países con tasas de abandono inferiores son Brasil, Sudáfrica y la India. Los sectores con el abandono más alto son el financiero, sanidad y servicios.

Determinados países y sectores son más vulnerables al abandono. Francia mantiene la tasa de abandono más alta, seguido de Japón. El sector público y minorista presentaron el abandono anómalo o rotación más bajo. Aunque no podemos generalizar el efecto del sector sobre las tasas de abandono de clientes debido al tamaño de la muestra, el sector financiero, la sanidad y las empresas de servicios sufrieron un abandono anómalo relativamente alto, mientras que el sector público y la educación, un abandono anómalo relativamente bajo.

El coste de la filtración de datos es proporcional al número de registros perdidos. En el estudio de este año de 383 organizaciones, el coste comprendió de 2,1 millones de dólares para una pérdida de menos de 10.000 registros a 6,7 millones para más de 50.000.

Los costes más elevados de detección y escalado se registraron en Canadá, y los más bajos en la India. Los costes de las filtraciones asociados a la detección y el escalado se refieren a actividades de investigación, evaluación y servicios de auditorías, gestión de equipos de crisis y comunicaciones a los directivos y al consejo de administración. Estos costes medios fueron de 1,60$ en Canadá, en claro contraste con el promedio de 0,53$ de la India.

Los costes de notificación más elevados se registraron en Estados Unidos. Los costes de negocio perdido incluyen las rotaciones anómalas de clientes, el aumento de las actividades de adquisición de clientes, las pérdidas de reputación y una menor buena disposición. En Estados Unidos, el coste fue de 0,59$ y en la India de 0,02$.

Los costes de respuesta tras la filtración fueron más elevados en Estados Unidos y Alemania. Los costes asociados a la detección y respuesta tras la filtración en Estados Unidos fueron de 1,72$ y 1,54$ en Alemania. Estos costes incluyen actividades del servicio técnico, comunicaciones internas, actividades especiales de investigación, remediación, gastos legales, descuentos en productos, servicios de protección de identidad e intervenciones reguladoras.

Estados Unidos pagó el precio más alto por la pérdida de clientes tras una filtración. El coste de la pérdida de negocio fue especialmente alto para las empresas estadounidenses (3,97$). Este coste incluye la rotación anómala de clientes, el aumento de las actividades de adquisición de clientes, las pérdidas de reputación y una menor buena disposición.

La Región Árabe presentó los costes directos más altos y Estados Unidos los costes indirectos más altos. Los costes directos se refieren al desembolso directo para realizar una actividad determinada, como contratar expertos y abogados u ofrecer a las víctimas servicios de protección de identidad. Los costes indirectos engloban el tiempo, el esfuerzo y otros recursos de la organización destinados a la resolución de la filtración. Incluyen la asistencia de los empleados en las notificaciones o en la investigación del incidente, así como la pérdida de la buena disposición y el abandono de clientes. La Región Árabe registró el porcentaje más alto (57 %) de costes directos y Estados Unidos el porcentaje más alto (66 %) de costes indirectos.

Determinados países tienen más probabilidades de sufrir una filtración de datos. En los últimos tres años, se ha estudiado la probabilidad de uno o más casos de filtración. Brasil y Sudáfrica presentan la mayor probabilidad estimada, mientras que Alemania y Australia la inferior.

El tiempo dedicado a identificar y contener una filtración afecta al coste. Por segundo año, nuestro estudio muestra la relación entre la velocidad de una empresa en identificar y contener filtraciones y sus consecuencias financieras. El tiempo de identificación y el de contención fueron más elevados en ataques maliciosos y delictivos (229 y 82 días, respectivamente) y muy inferiores para aquellas causadas por error humano (162 y 59 días, respectivamente).

Preguntas frecuentes sobre el coste de las filtraciones de datos

¿Cuál es la finalidad de este estudio? Nuestro objetivo consiste en cuantificar el impacto económico de las filtraciones de datos y observar tendencias de costes. Creemos que una mejor comprensión del coste, las causas raíz y los factores que influyen sobre el coste ayudarán a las empresas a determinar la inversión y los recursos necesarios para prevenir o mitigar las consecuencias de un ataque.

¿Qué es una filtración de datos? Una filtración se define como un suceso en el cual el nombre de una persona más un registro médico y/o un registro financiero o tarjeta de débito se expone a un riesgo potencial, ya sea en formato electrónico o papel. En nuestro estudio, hemos identificado las tres causas principales: un ataque malicioso o delictivo, un fallo del sistema o un error humano. Los costes de una filtración de datos varían en función de la causa y las protecciones establecidas en el momento de la filtración de los datos.

¿Qué es un registro comprometido? Definimos un registro como información que identifica a la persona natural cuya información se ha perdido o ha sido robada en una filtración. Un ejemplo sería la base de datos de una empresa minorista con el nombre de una persona asociado a la información de la tarjeta de crédito y otra información personalmente identificable. O bien, el registro de una aseguradora sobre un asegurado con información médica y de pago. En el estudio de este año, el coste medio para la organización si uno de estos registros se pierde o es robado es de 158 dólares.

¿Cómo se recopilan los datos? Los investigadores del Ponemon Institute recopilaron datos cualitativos a través de 1.500 entrevistas individuales realizadas durante 10 meses. La selección de organizaciones para el estudio de 2016 empezó en enero de 2015 y las entrevistas se completaron en marzo de 2016. De cada una de las 383 organizaciones que participaron, hablamos con profesionales de TI, cumplimiento normativo y seguridad de la información, con conocimientos sobre las filtraciones de datos y los costes asociados a su resolución. Por motivos de privacidad, no recopilamos información específica de ninguna organización.

¿Cómo se calcula el coste? Para calcular el coste medio de una filtración, recopilamos los gastos directos e indirectos de la organización. Los gastos directos incluyen la contratación de expertos, la subcontratación de asistencia telefónica y proporcionar suscripciones de control de crédito gratuitas y descuentos para futuros productos y servicios. Los costes indirectos incluyen la comunicación y las investigaciones internas, así como el valor extrapolado de la pérdida de clientes como resultado de la rotación o de una menor tasa de adquisición de clientes.

¿En qué se diferencia la investigación de benchmarking de la investigación de encuestas? La unidad de análisis del estudio *Costes de las filtraciones de datos* es la organización. En la investigación de encuestas, la unidad de análisis es la persona individual. Seleccionamos 383 organizaciones para participar en este estudio. Las filtraciones de datos oscilan entre aproximadamente 3.000 a más de 101.500 registros comprometidos.

¿Se puede utilizar el coste medio de una filtración para calcular las consecuencias financieras de una mega-filtración, con millones de registros perdidos o robados? El coste medio de una filtración de datos en nuestro estudio no se aplica a filtraciones de datos de gran magnitud, como la de Sony. A fin de representar a las organizaciones globales y extraer conclusiones de la investigación que ayuden a comprender los costes de un robo o pérdida de información, no hemos incluido las filtraciones de más de 100.000 registros comprometidos.

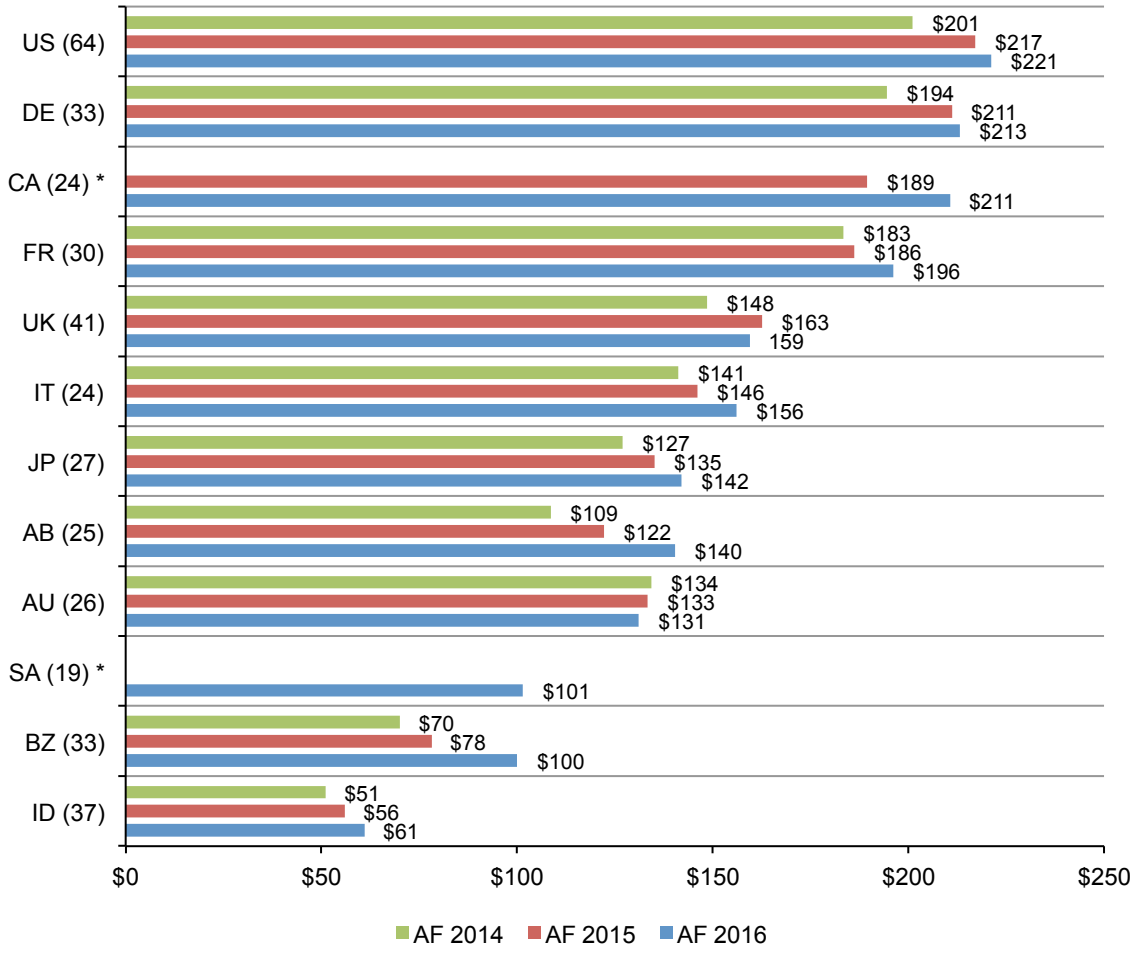
¿Cada año se realiza el seguimiento de las mismas organizaciones? Cada año participan diferentes empresas en el estudio, es decir, no realizamos el seguimiento de las mismas. Para ser coherentes, seleccionamos y cotejamos empresas con características similares, como sector, plantilla, distribución geográfica y tamaño de la filtración. Desde 2005, hemos estudiado las incidencias de filtraciones de datos de 2.013 organizaciones de todo el mundo.

Representación gráfica del alcance global

El estudio de este año se realizó en 12 países: Estados Unidos, Alemania, Canadá, Francia, Reino Unido, Italia, Japón, Región Árabe, Brasil, India y, por primera vez, Sudáfrica. Participaron un total de 383 organizaciones. Los informes específicos de cada país se presentan en 12 informes independientes.

La Figura 1 presenta el coste medio per cápita de las filtraciones de datos durante 3 años, expresadas en dólares, para los 12 países. Como se aprecia, existe una variación importante entre las distintas muestras de los países[4]. El coste medio consolidado per cápita para todos los países fue de 158$, en comparación con el promedio de 154$ del año pasado (excluyendo Sudáfrica). Estados Unidos y Alemania mantienen los costes per cápita más altos, de 221$ y 213$, respectivamente. La India y Brasil presentaron los costes más bajos, de 61$ y 100$.

Figura 1. Coste medio per cápita de las filtraciones de datos durante tres años
Promedio general para AF 2016=158$, AF 2015=154$, AF 2014=145$
*Datos históricos no disponibles en todos los años
(AF 2016=383, AF 2015=350, AF 2014=315)
Calculado en dólares americanos



[4] El coste per cápita se define como el coste total de la filtración de datos divido por el tamaño de la filtración (es decir, el número de registros perdidos o robados).

Parte 2. Conclusiones principales

En este apartado, exponemos detalladamente las conclusiones de nuestro estudio.

Los temas se presentan en el siguiente orden:

- Diferencias globales y por sector del coste de las filtraciones de datos
- Causas raíz de una filtración de datos
- Factores que influyen en el coste de las filtraciones de datos
- Tendencias en la frecuencia de registros comprometidos y rotación o abandono de clientes
- Tendencias en los componentes de costes de las filtraciones de datos
- Probabilidad de que una organización sufra una filtración de datos
- Tiempo medio para identificar y contener una filtración de datos
- El impacto de la gestión de la continuidad del negocio sobre el coste de la filtración

En la siguiente tabla se enumeran los 12 países, leyenda, tamaños de la muestra y ocurrencias utilizadas en este estudio. También muestra el número de años del informe anual para cada país, desde un año para Canadá hasta 11 años para Estados Unidos.

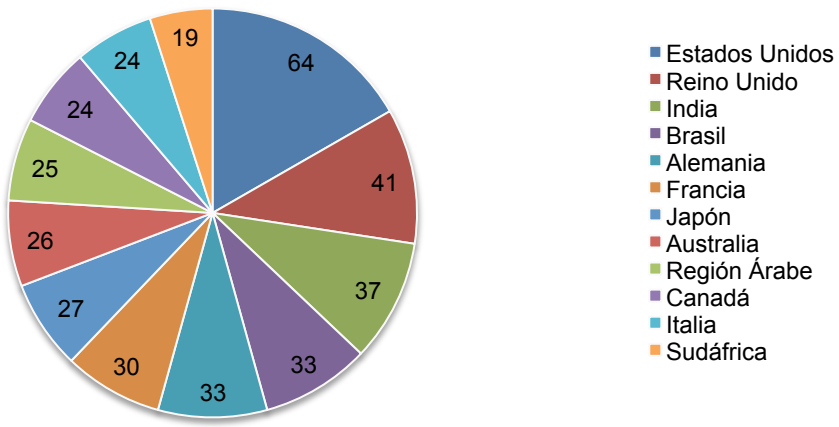
Tabla 1. Estudio global en cifras

Leyenda	Países	Muestra	Pct%	Moneda	Años de estudio
AB	Región Árabe*	25	7%	AED/SAR	3
AU	Australia	26	7%	AU dólar	7
BZ	Brasil	33	9%	Real	4
CA	Canadá	24	6%	CA dólar	2
DE	Alemania	33	9%	Euro	8
FR	Francia	30	8%	Euro	7
ID	India	37	10%	Rupia	5
IT	Italia	24	6%	Euro	5
JP	Japón	27	7%	Yen	5
SA	Sudáfrica	19	5%	ZAR	1
UK	Reino Unido	41	11%	GBP	9
US	Estados Unidos	64	17%	US dólar	11
	Total	383	100%		

*AB es una muestra combinada de empresas ubicadas en Arabia Saudí y los Emiratos Árabes Unidos

El siguiente gráfico muestra la distribución de las 383 organizaciones participantes de 12 países. Como puede observarse, el mayor segmento corresponde a Estados Unidos, con 64 organizaciones y el menor a Sudáfrica, con 19 organizaciones.

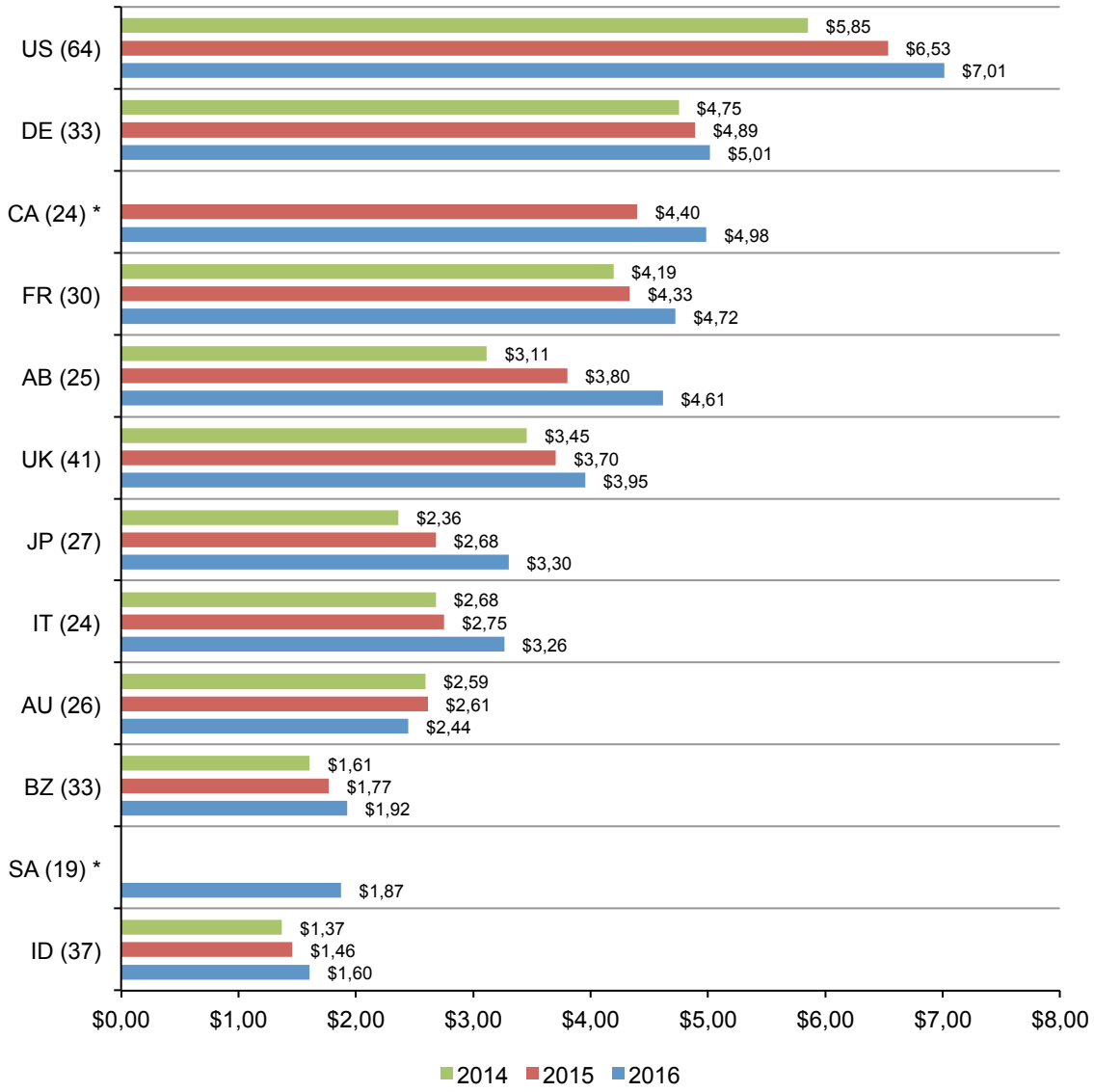
Gráfico circular 1. Frecuencia de muestras de benchmarking por país
(n=383)



Diferencias globales y por sector del coste de las filtraciones de datos

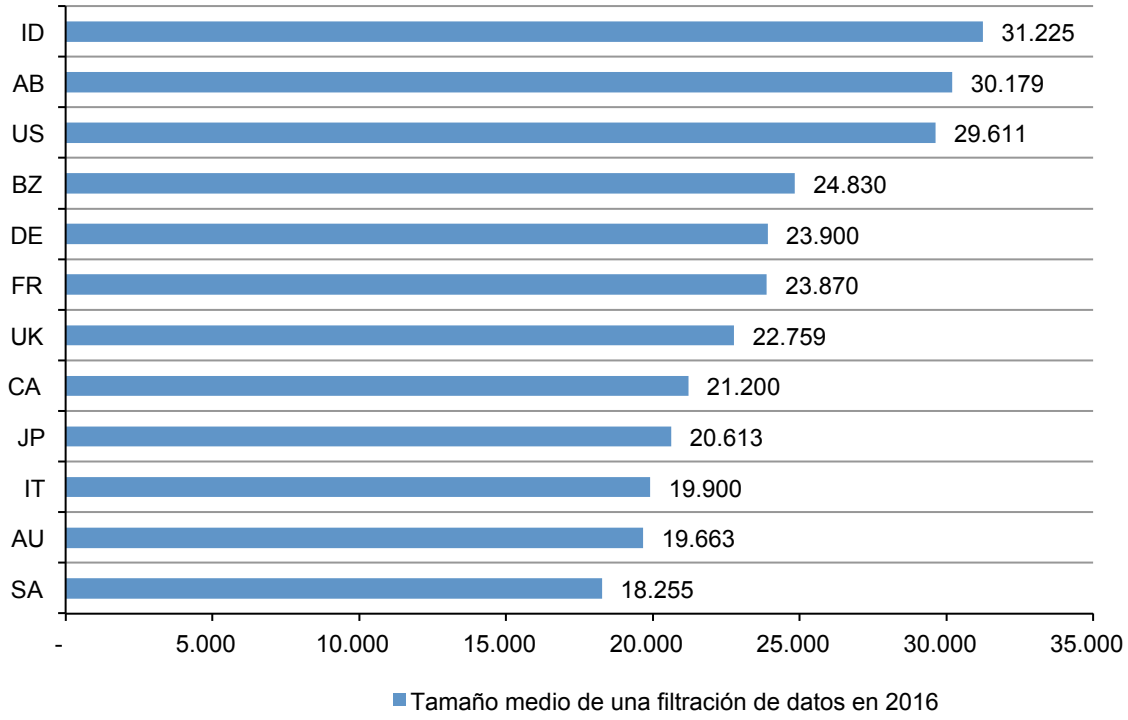
El coste medio de una filtración de datos para una organización varía por país. La Figura 2 representa el coste medio total de una filtración para los 12 países del estudio de este año. Con la excepción de Australia y Sudáfrica, todos los países han experimentado un incremento en el coste medio total con respecto al año anterior. El coste medio total más elevado se registró en Estados Unidos, más de 7,01 millones de dólares, seguido por Alemania con 5,01 millones. Por el contrario, las empresas indias y sudafricanas presentaron el coste medio total más bajo, con 1,60 millones y 1,87 millones, respectivamente.

Figura 2. Coste medio total de una filtración para una organización durante tres años
Promedio general para AF 2016=4,0$, AF 2015=3, 8, $ AF 2014=3,50$
*Datos históricos no disponibles en todos los años
(AF 2016=383, AF 2015=350, AF 2014=315)
Calculado en dólares americanos (millones)



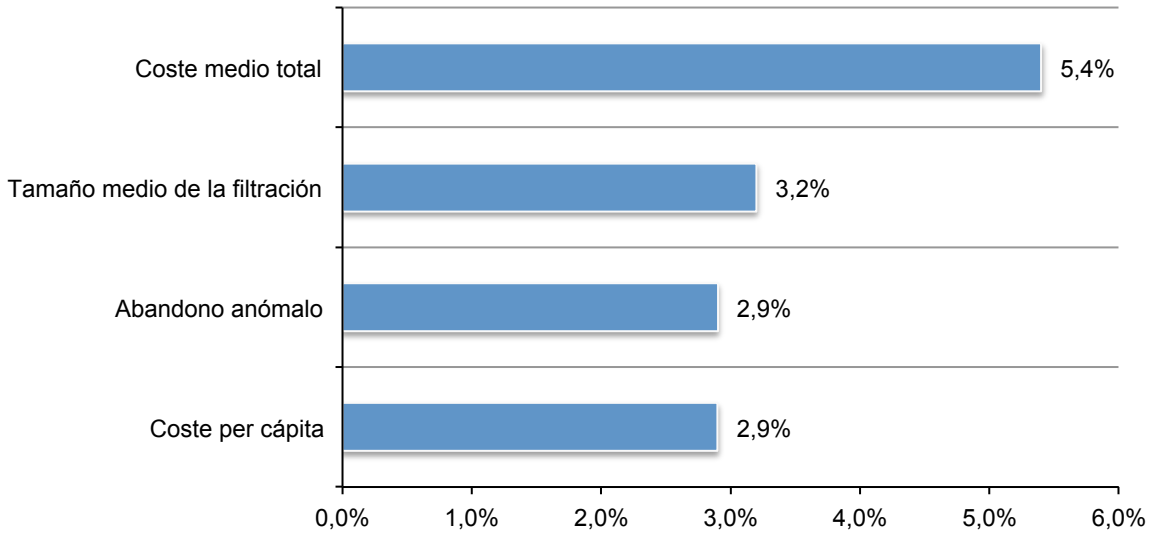
Número de registros expuestos o comprometidos. La Figura 3 representa el tamaño medio de las filtraciones de datos para las organizaciones de los 12 países incluidos en este estudio. Como se muestra, los países con mayor número de registros robados o perdidos son la India, la Región Árabe y Estados Unidos. Sudáfrica obtuvo el número medio más bajo de registros perdidos o robados. En este informe, también revelamos la relación entre el número de registros perdidos o robados y el coste de una filtración de datos.

Figura 3. Número medio de registros violados por país
Promedio global = 23.834
(n=383)



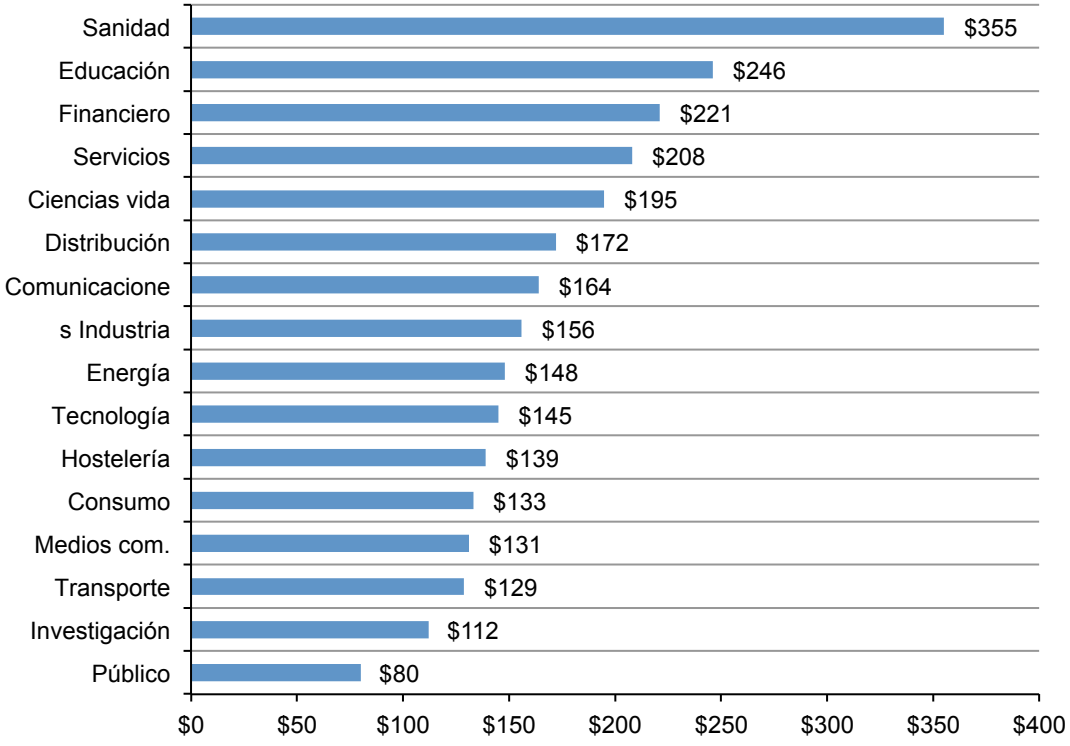
Las medidas revelan por qué se incrementó el coste. La Figura 4 presenta cuatro métricas que explican el incremento en el coste de una filtración de datos. El coste medio de una filtración de datos aumentó un 5,4 % y el coste per cápita o registro aumentó un 2,9 %. El tamaño medio de la filtración de datos (número de registros robados o perdidos) aumentó un 3,2 %. El abandono anómalo creció un 2,9 %. El abandono anómalo se define como una pérdida de clientes mayor de lo esperado en el transcurso normal del negocio.

Figura 4. Medidas que afectan al coste de una filtración de datos
Vista consolidada (n=383)



Determinados países registraron costes superiores por una filtración de datos. La Figura 5 muestra los costes per cápita para la muestra consolidada por clasificación sectorial. Los sectores más regulados, como la sanidad, educación y empresas financieras, tuvieron un coste per cápita por encima de la media general de 158$. El sector público, la investigación y las organizaciones de transporte tuvieron un coste per cápita bastante inferior al valor medio.

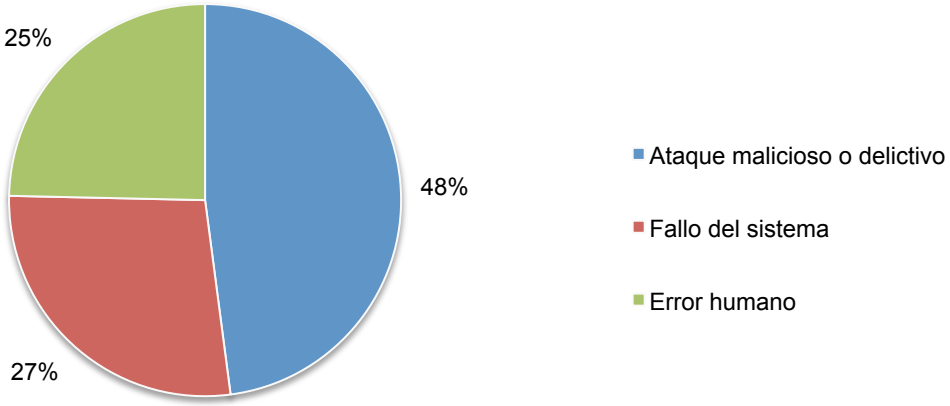
Figura 5. Clasificación del coste per cápita por sector
Vista consolidada (n=383), calculado en dólares americanos



Causas de una filtración de datos

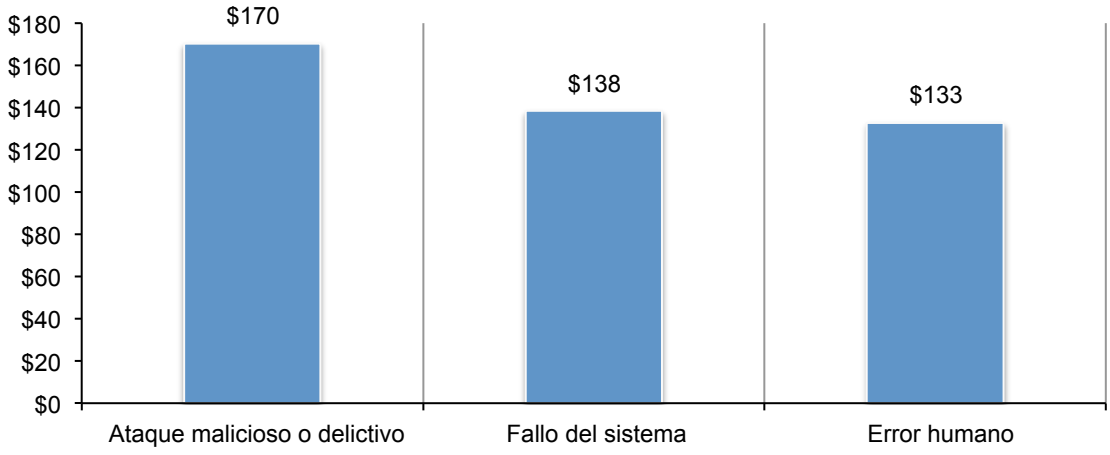
Los ataques maliciosos o delictivos fueron los causantes de la mayoría de las filtraciones[6]. El gráfico circular 2 ofrece un resumen de las principales causas raíz de una filtración de datos sobre una base consolidada para los 12 países representados en el estudio. El 48 % de los incidentes fueron motivados por un ataque malicioso o delictivo, el 25 % por la negligencia de empleados o contratistas (factor humano) y el 27 % implicaron fallos del sistema, que incluye errores en procesos de negocio y TI[6].

Gráfico circular 2. Distribución de la muestra de benchmarking por causa de la filtración
Vista consolidada (n=383)



Los ataques maliciosos tienen un coste superior a nivel global. La Figura 6 representa el coste per cápita de las filtraciones de datos para las tres posibles causas del incidente. En 2016, el coste de las filtraciones debidas a ataques maliciosos o delictivos fue de 170$, valor muy superior al coste per cápita de las filtraciones causadas por fallo del sistema o factores humanos (138$ y 133$, respectivamente).

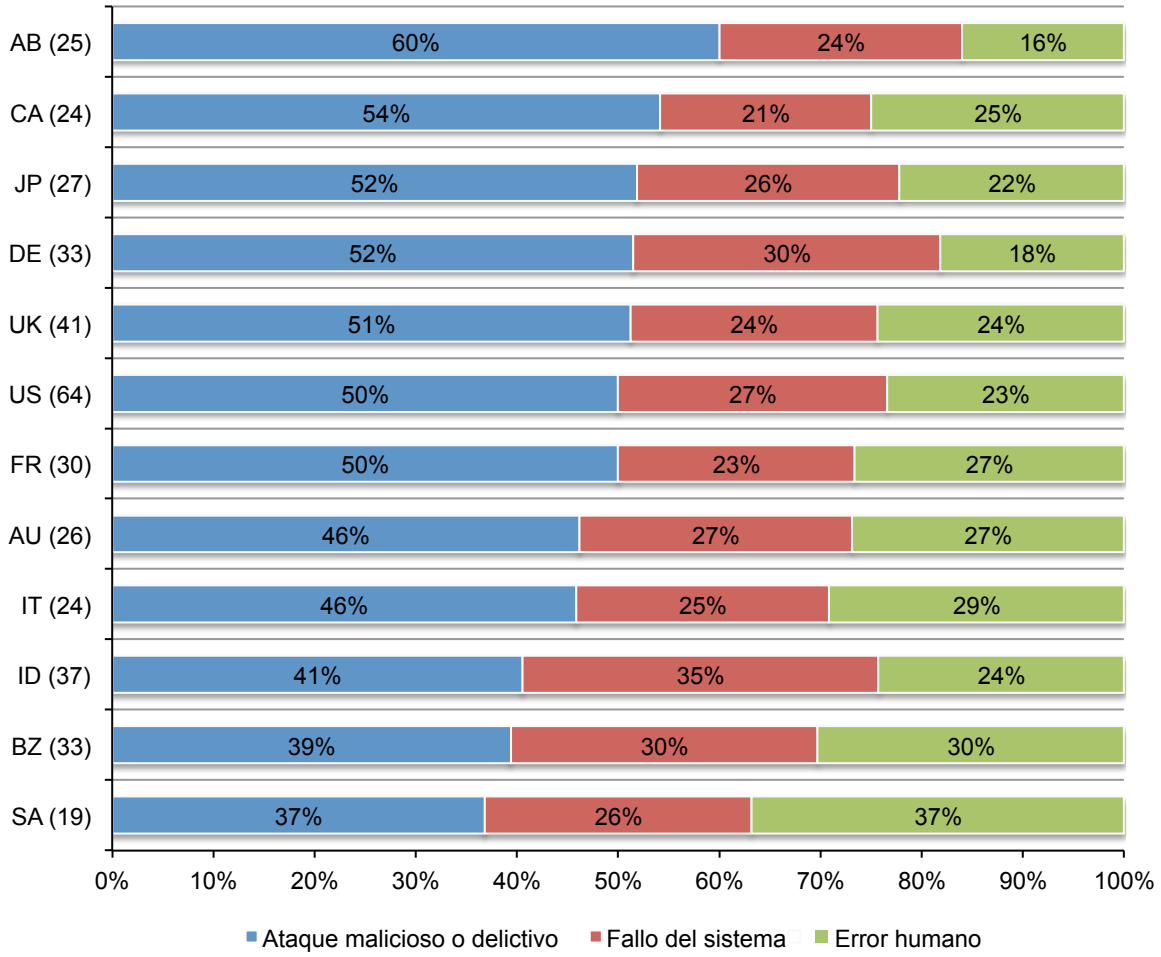
Figura 6. Coste per cápita para las tres posibles causas raíz de la filtración de datos
Vista consolidada (n=383), calculado en dólares americanos



[5]El personal negligente son personas que provocan una filtración por un descuido, de acuerdo con una investigación posterior a la filtración de datos. Los ataques maliciosos pueden ser provocados por hackers o delincuentes internos (empleados, contratistas u otros).
[6]Los tipos de ataques maliciosos o criminales más comunes incluyen infecciones de malware, delincuentes internos, phishing/ingeniería social e inyección SQL.

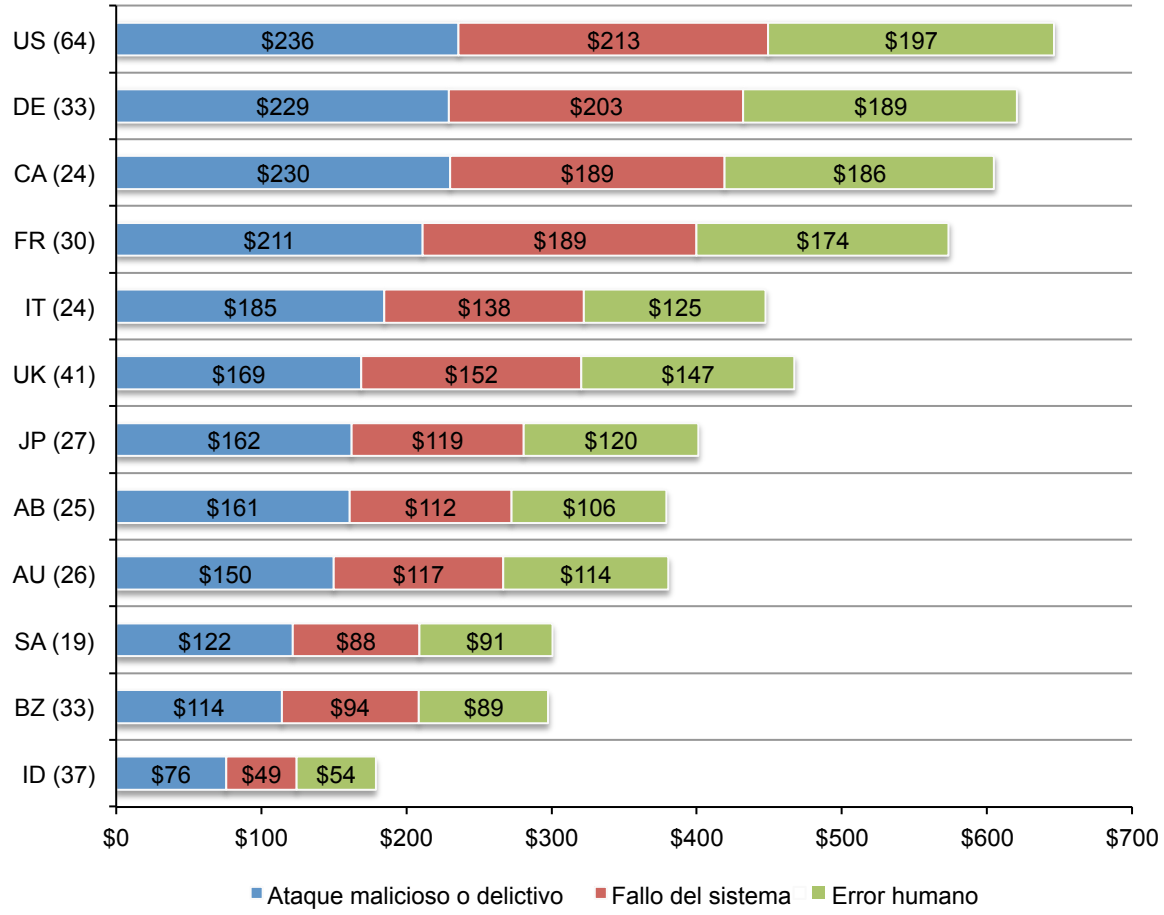
Diferencias por países de las causas raíz de una filtración. La Figura 7 presenta las principales causas raíz de una filtración de datos para los 12 países representados. Con un 60%, las organizaciones árabes tenían más probabilidades de sufrir un ataque malicioso o delictivo. En contraste, las empresas brasileñas y sudafricanas presentaron el porcentaje más bajo. Por el contrario, las empresas sudafricanas presentaron el porcentaje más elevado de filtraciones por error humano y las organizaciones de la India presentaron más probabilidades de sufrir una filtración de datos por un fallo del sistema o del proceso de negocio.

Figura 7. Distribución de la muestra de benchmarking por causa raíz de la filtración
(n=383)



El coste per cápita para las tres causas raíz difiere entre países. La Figura 8 muestra el coste per cápita de las filtraciones por muestra de países para las tres causas raíz. Estos resultados muestran claramente que los costes derivados de ataques maliciosos o delictivos fueron bastante superiores a los costes derivados de fallos del sistema o errores humanos. Este gráfico también revela una amplia variación entre países. El coste en Estados Unidos de un incidente de filtración malicioso o delictivo fue de 236$ por registro comprometido. En la India, este coste fue de 76$.

Figura 8. Coste per cápita para las tres causas raíz
(n=383)

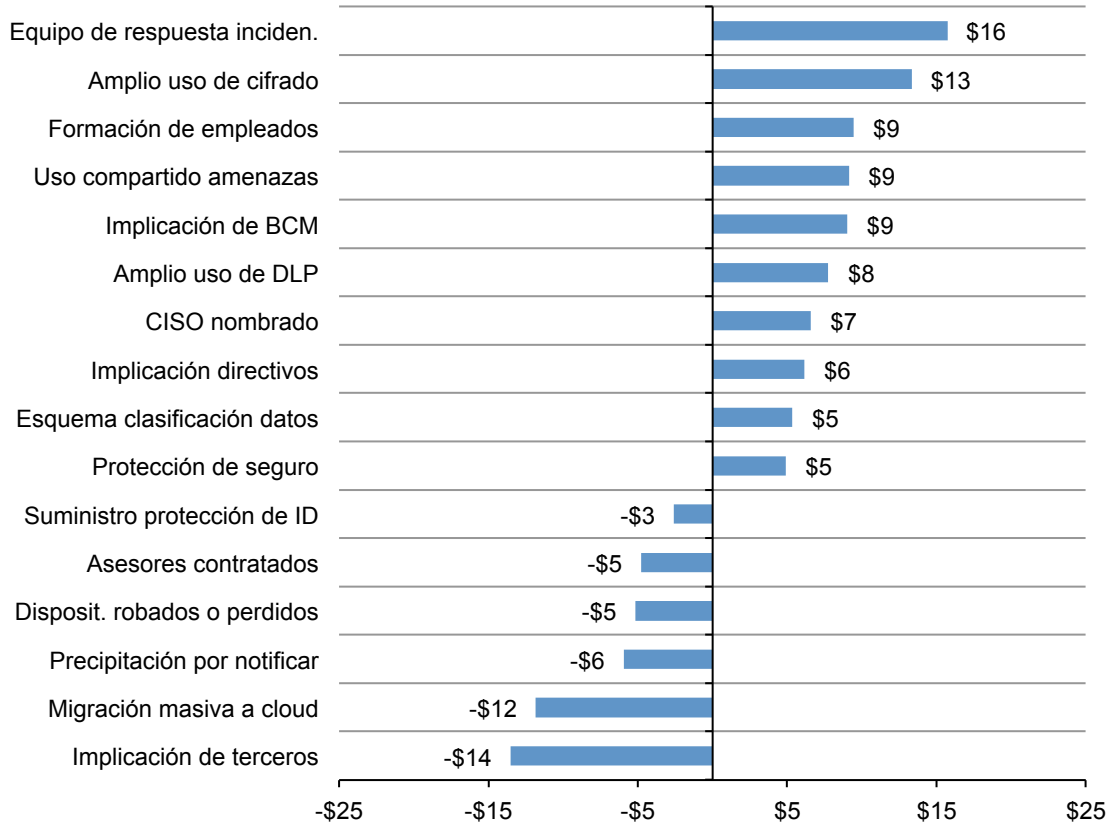


Factores que influyen en el coste de las filtraciones de datos

Determinados factores disminuyen el coste de una filtración. La Figura 9 proporciona una lista de 16 factores que aumentan o disminuyen el coste per cápita de una filtración de datos. Como se muestra, un equipo de respuesta ante incidentes, un amplio uso de cifrado, la formación de los empleados, el uso compartido de amenazas o la gestión de la continuidad del negocio disminuyeron el coste per cápita de las filtraciones de datos.

Las filtraciones de datos causadas por la implicación de terceros, la migración masiva a cloud, la precipitación por notificar o dispositivos perdidos o robados incrementaron el coste per cápita de las filtraciones (representado en números negativos). Por ejemplo, un equipo de respuesta ante incidentes redujo el coste en 16$, de 158$•a 142$. Por el contrario, la implicación de terceros en la causa de la filtración generó un incremento de 14$, de 158$ a 172$.

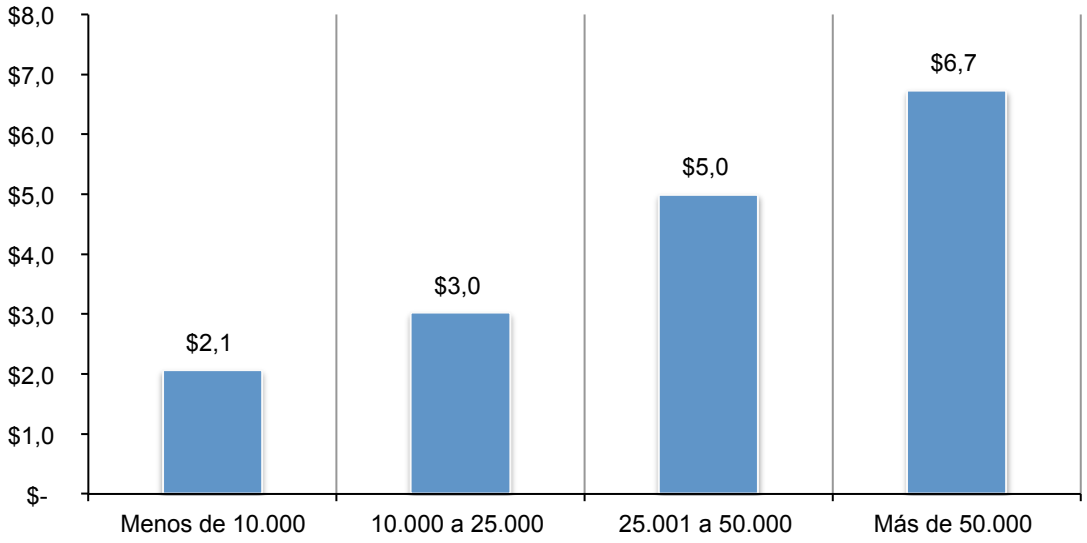
Figura 9. Impacto de 16 factores sobre el coste per cápita de las filtraciones de datos
Vista consolidada (n=383), calculado en dólares americanos



Tendencias en la frecuencia de los registros comprometidos y la rotación de clientes

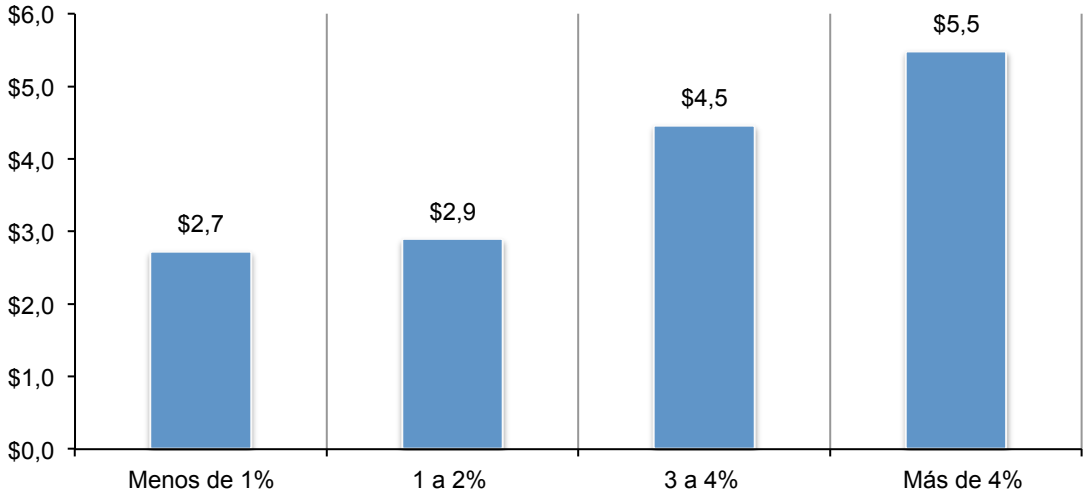
El coste de la filtración de datos es proporcional al número de registros perdidos. La Figura 10 muestra la relación entre el coste total de la filtración y el tamaño del incidente para las 383 organizaciones, en orden ascendente según el tamaño del incidente. En el estudio de este año, el coste osciló entre 2,1 y 6,7 millones de dólares.

Figura 10. Coste total por tamaño de la filtración de datos
Vista consolidada (n=383), calculado en millones de dólares americanos



El coste per cápita de la filtración de datos es proporcional al abandono. La Figura 11 representa la distribución de los costes per cápita de la filtración en orden ascendente del abandono anómalo para las 383 organizaciones. Las empresas con una pérdida de clientes inferior al 1 % tuvieron un coste medio de filtración de 2,7 millones, o si la pérdida de clientes superó el 4 %, el coste medio fue de 5,5 millones de dólares.

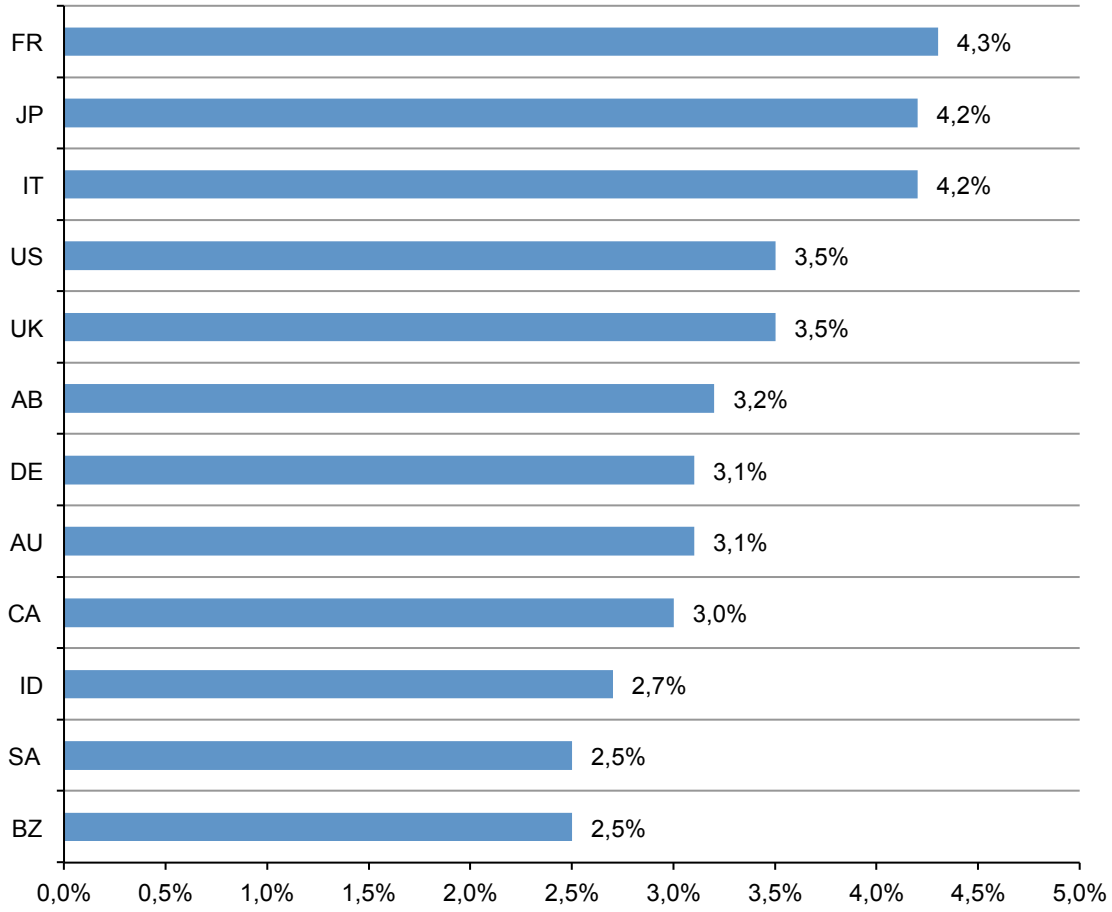
Figura 11. Coste total de la filtración de datos por tasa de abandono anómalo
Vista consolidada (n=383), calculado en millones de dólares americano



Determinados países son más vulnerables al abandono. La Figura 12 muestra las tasas de abandono anómalo para los 12 países representados en este estudio. Los resultados revelan importantes diferencias entre países. Francia mantiene la tasa más elevada de abandono, seguido de Japón. El sector público y minorista experimentaron la menor tasa de abandono.

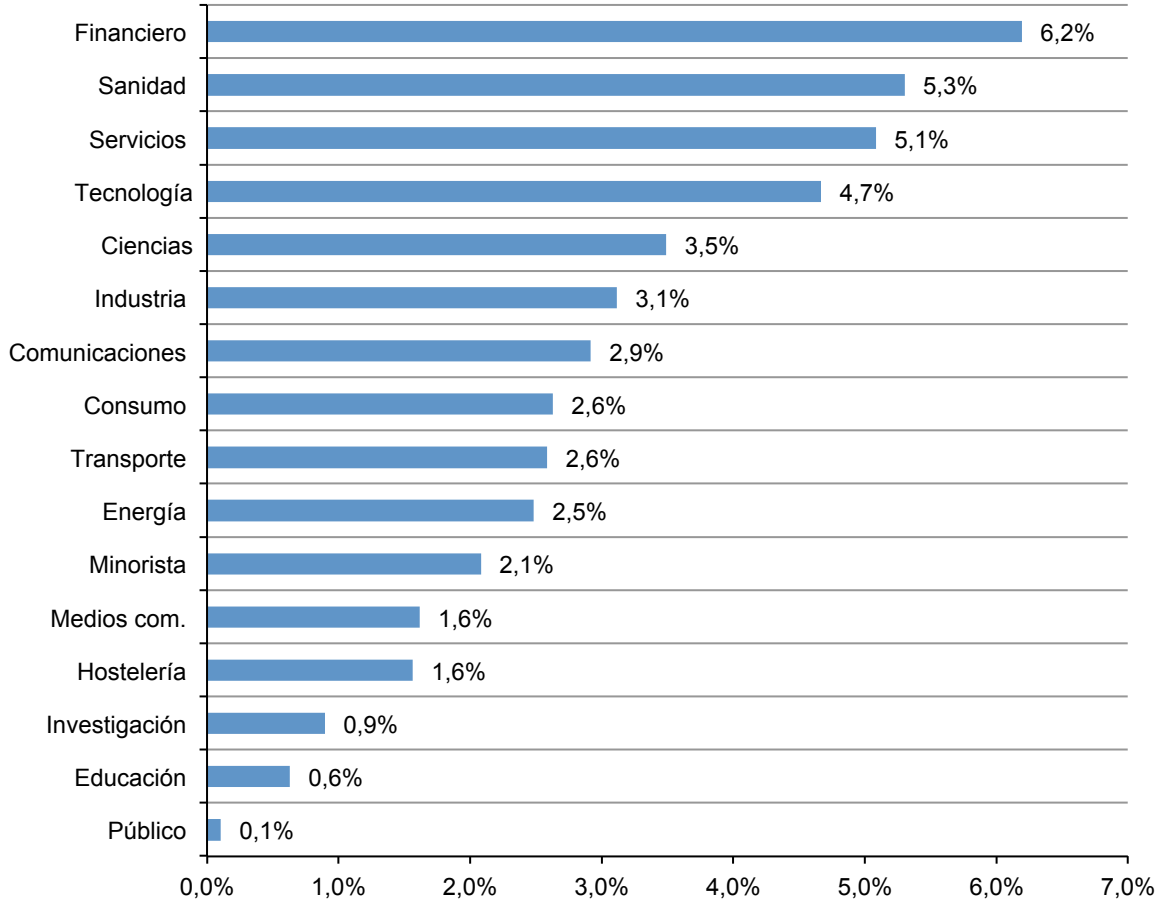
De aquí podemos extraer que las organizaciones en países con tasas de abandono altas podrían reducir los costes de las filtraciones de manera significativa si se centraran en actividades de retención de clientes para conservar la reputación y el valor de la marca.

Figura 12. Tasas de abandono anómalo durante tres años por país
(n = 383)



Determinados sectores son más vulnerables al abandono. La Figura 13 muestra la tasa de abandono anómalo de las organizaciones representadas en este estudio de 2016. Aunque no podemos generalizar el efecto del sector sobre las tasas de abandono de clientes debido al tamaño de la muestra, el sector financiero, la sanidad y las empresas de servicios sufrieron un abandono anómalo relativamente alto, mientras que el sector público y la educación, un abandono anómalo relativamente bajo[7].

Figura 13. Clasificación de las tasas de abandono anómalo por sector
(n = 383)

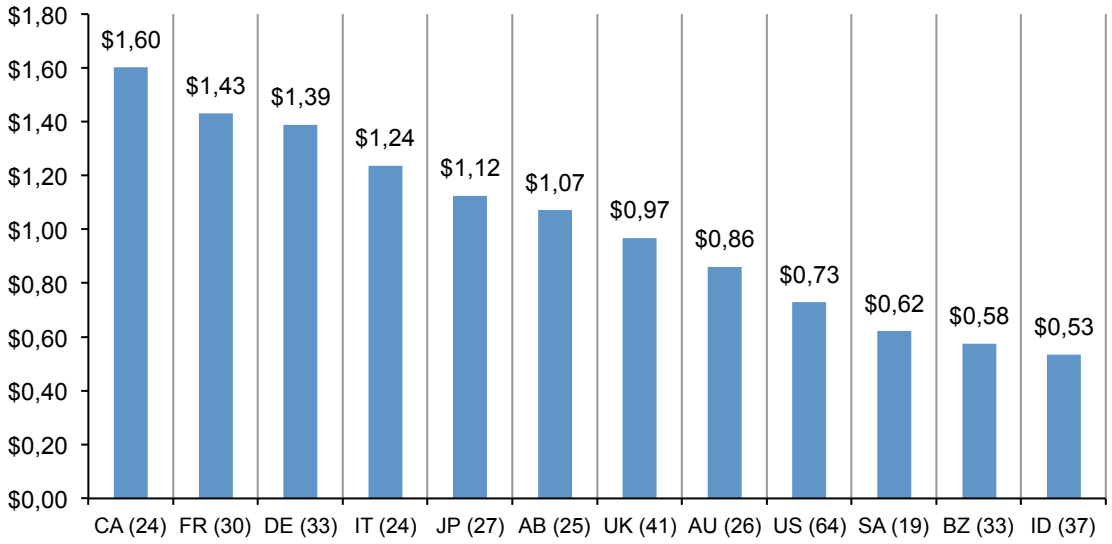


[7]Las empresas del sector público utilizan un esquema de abandono diferente, ya que sus clientes normalmente no tienen ninguna opción alternativa.

Tendencias en los componentes de coste de una filtración de datos

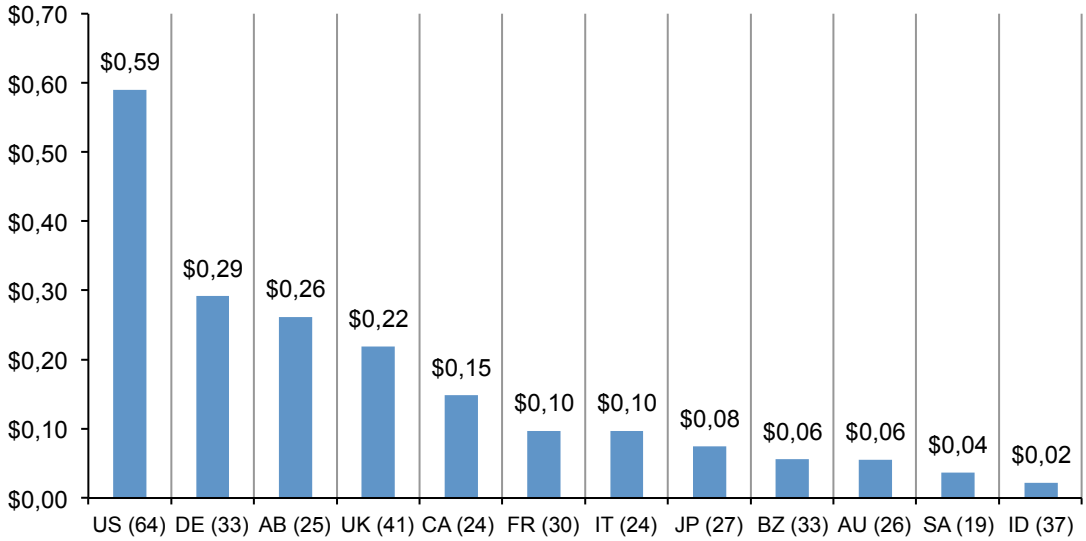
Los costes más elevados de detección y escalado se registraron en Canadá, y los más bajos en la India. Los costes de las filtraciones asociados a la detección y el escalado se refieren a actividades de investigación, evaluación y servicios de auditorías, gestión de equipos de crisis y comunicaciones a los directivos y al consejo de administración. Estos costes medios fueron de 1,60$ en Canadá, en claro contraste con el promedio de 0,53$ de la India.

Figura 14. Costes de detección y escalado
(n = 383), calculado en dólares americanos (millones)



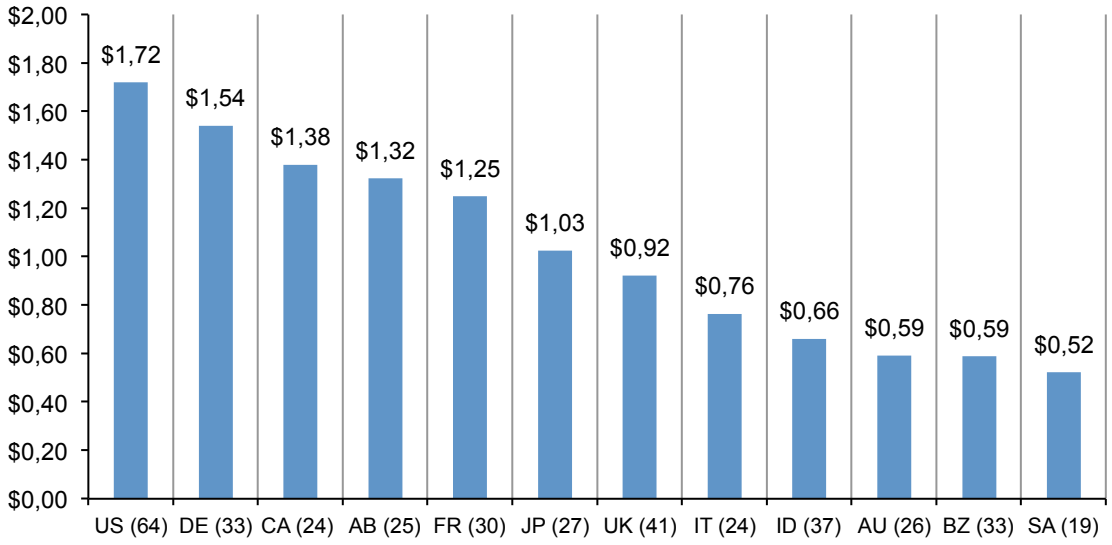
Los costes de notificación más elevados se registraron en Estados Unidos. Estos incluyen actividades de TI asociadas a la creación de bases de datos de contacto, la determinación de todos los requisitos normativos, la contratación de expertos externos, gastos postales, correo electrónico rechazado y configuración de comunicaciones internas. Con diferencia, los costes de notificación de las empresas estadounidenses fueron los más elevados (0,59$) (Figura 15).

Figura 15. Costes de notificación
(n = 383), calculado en dólares americanos (millones)



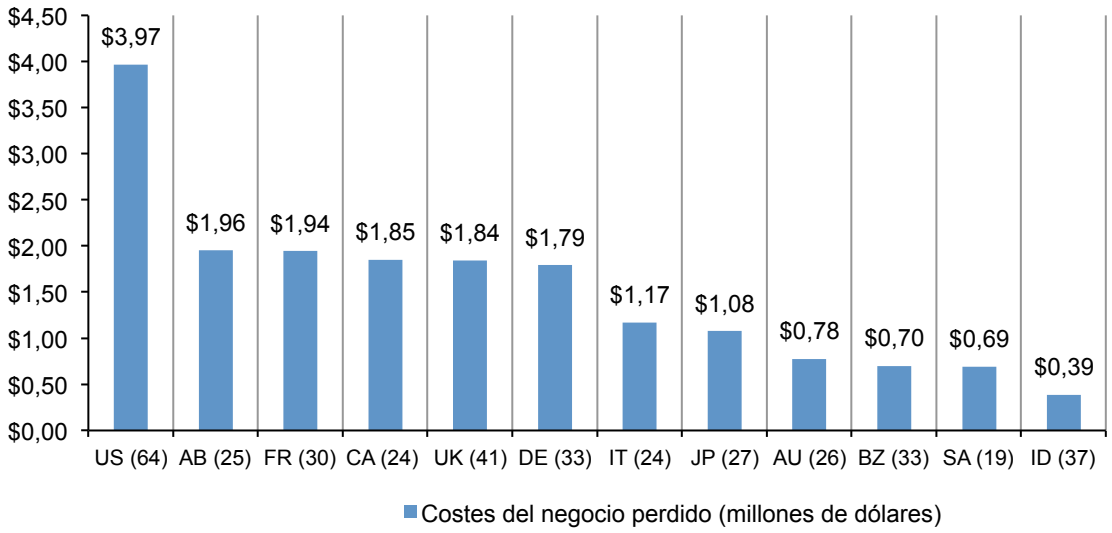
Los costes de respuesta tras la filtración fueron más elevados en Estados Unidos y Alemania. Los costes asociados a la detección y respuesta tras la filtración en Estados Unidos fueron de 1,72$ y 1,54$ en Alemania, como se aprecia en la Figura 16). Estos costes incluyen actividades del servicio técnico, comunicaciones internas, actividades especiales de investigación, remediación, gastos legales, descuentos en productos, servicios de protección de identidad e intervenciones reguladoras.

Figura 16. Costes de respuesta tras la filtración
(n = 383), calculado en dólares americanos (millones)



Estados Unidos pagó el precio más alto por la pérdida de clientes tras una filtración. De acuerdo con la Figura 17, el coste de la pérdida de negocio fue especialmente alto para las empresas estadounidenses (3,97$). Este componente d ecoste incluye la rotación anómala de clientes, el aumento de las actividades de adquisición de clientes, las pérdidas de reputación y una menor buena disposición.

Figura 17. Costes del negocio perdido
(n = 383), calculado en dólares americanos (millones)

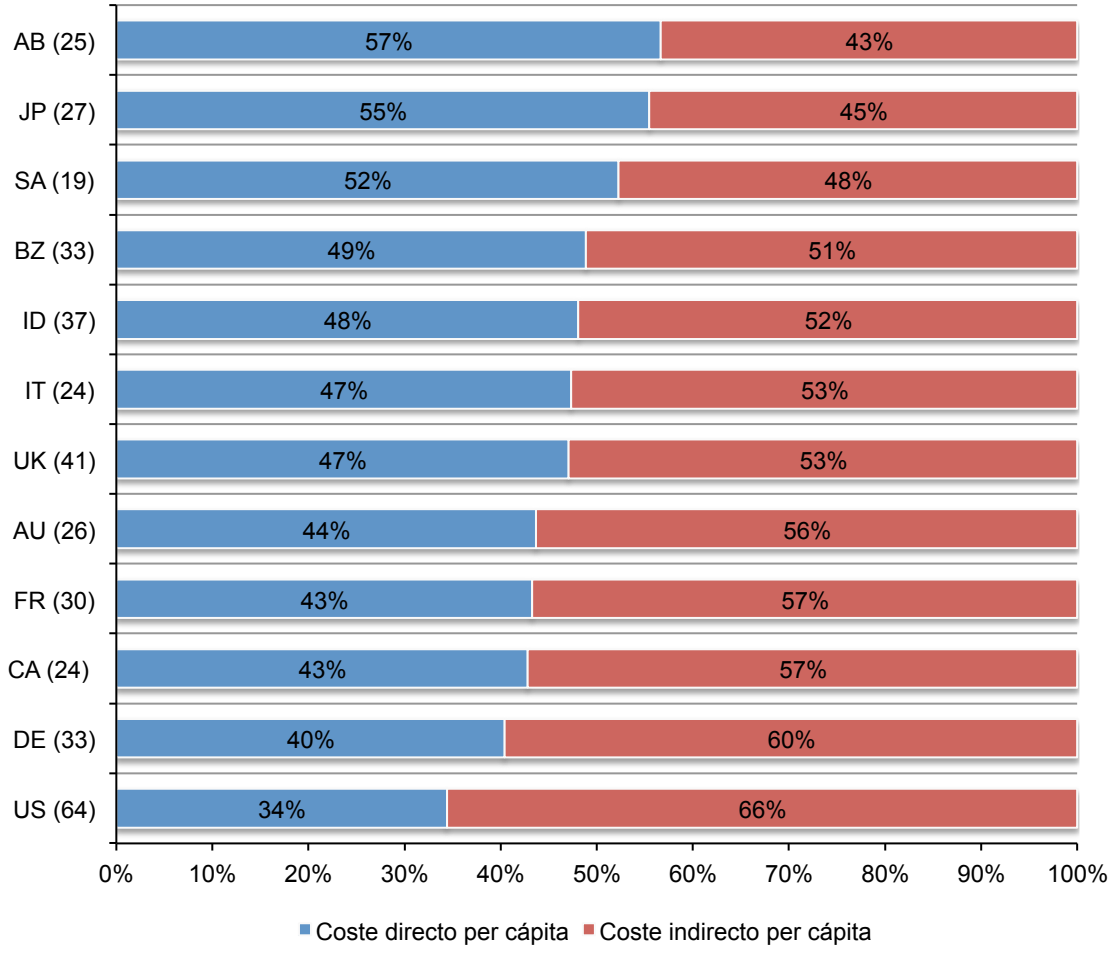


La proporción de costes directos e indirectos de una filtración de datos varía por país

La Región Árabe registró los costes directos más altos y Estados Unidos los costes indirectos más altos. Los costes directos se refieren al desembolso directo para realizar una actividad determinada, como contratar expertos y abogados u ofrecer a las víctimas servicios de protección de identidad. Los costes indirectos engloban el tiempo, el esfuerzo y otros recursos de la organización destinados a la resolución de la filtración. Incluyen la asistencia de los empleados en las notificaciones o en la investigación del incidente, así como la pérdida de la buena disposición y el abandono de clientes.

La Figura 18 muestra el porcentaje de los costes per cápita directos e indirectos para los 12 países. La Región Árabe registró el porcentaje más alto (57 %) de costes directos y Estados Unidos el porcentaje más alto (66 %) de costes indirectos.

Figura 18. Porcentaje de costes per cápita directos e indirectos
Vista consolidada (n=383)

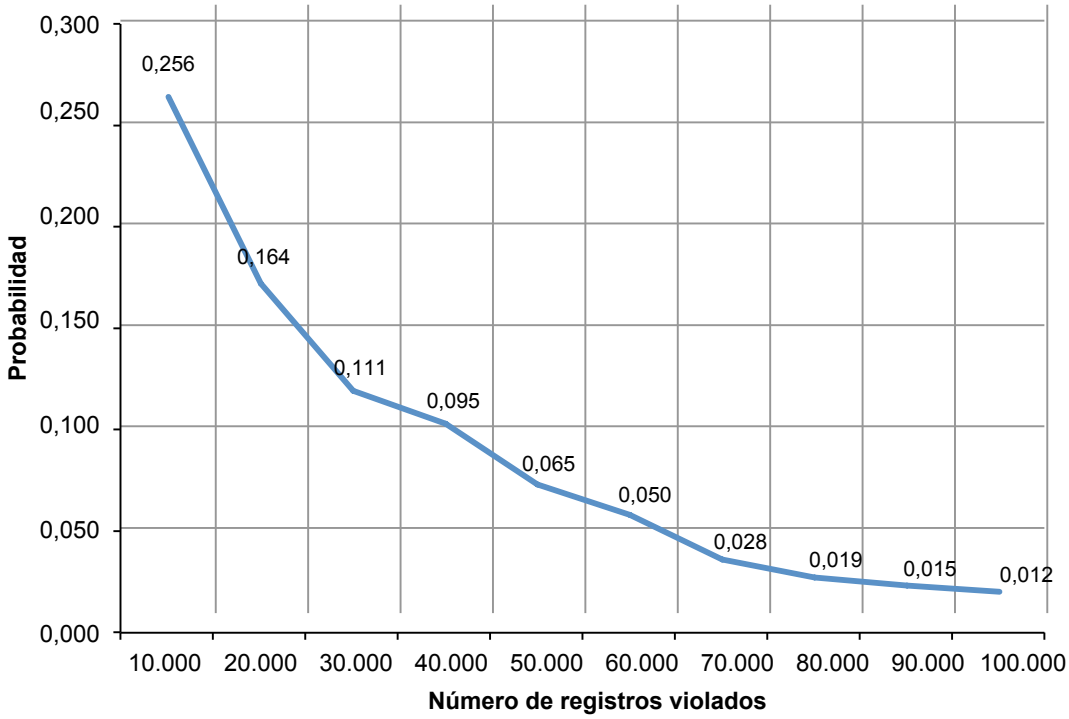


Probabilidad de que una organización sufra una filtración de datos

Nuestro estudio proporciona un análisis de la probabilidad de que se produzca una o más filtraciones de datos en los próximos 24 meses. En base a las experiencias de las organizaciones del estudio, creemos que es posible prever la probabilidad de una filtración en función de dos factores: la cantidad de registros perdidos o robados y el sector de la empresa.

La Figura 19 muestra las probabilidades subjetivas de incidentes de filtración con un mínimo de 10.000 a 100.000 registros comprometidos[8]. Como puede observarse, la probabilidad de filtración disminuye a medida que el tamaño aumenta. Mientras que la probabilidad de filtración con un mínimo de 10.000 registros implicados se estima al 26 % en un periodo de 24 meses, las probabilidades de una filtración con 100.000 registros implicados son inferiores al 1 %.

Figura 19. Probabilidad de una filtración de datos con un mínimo de 10.000 a 100.000 registros implicados Vista consolidada (n=383)

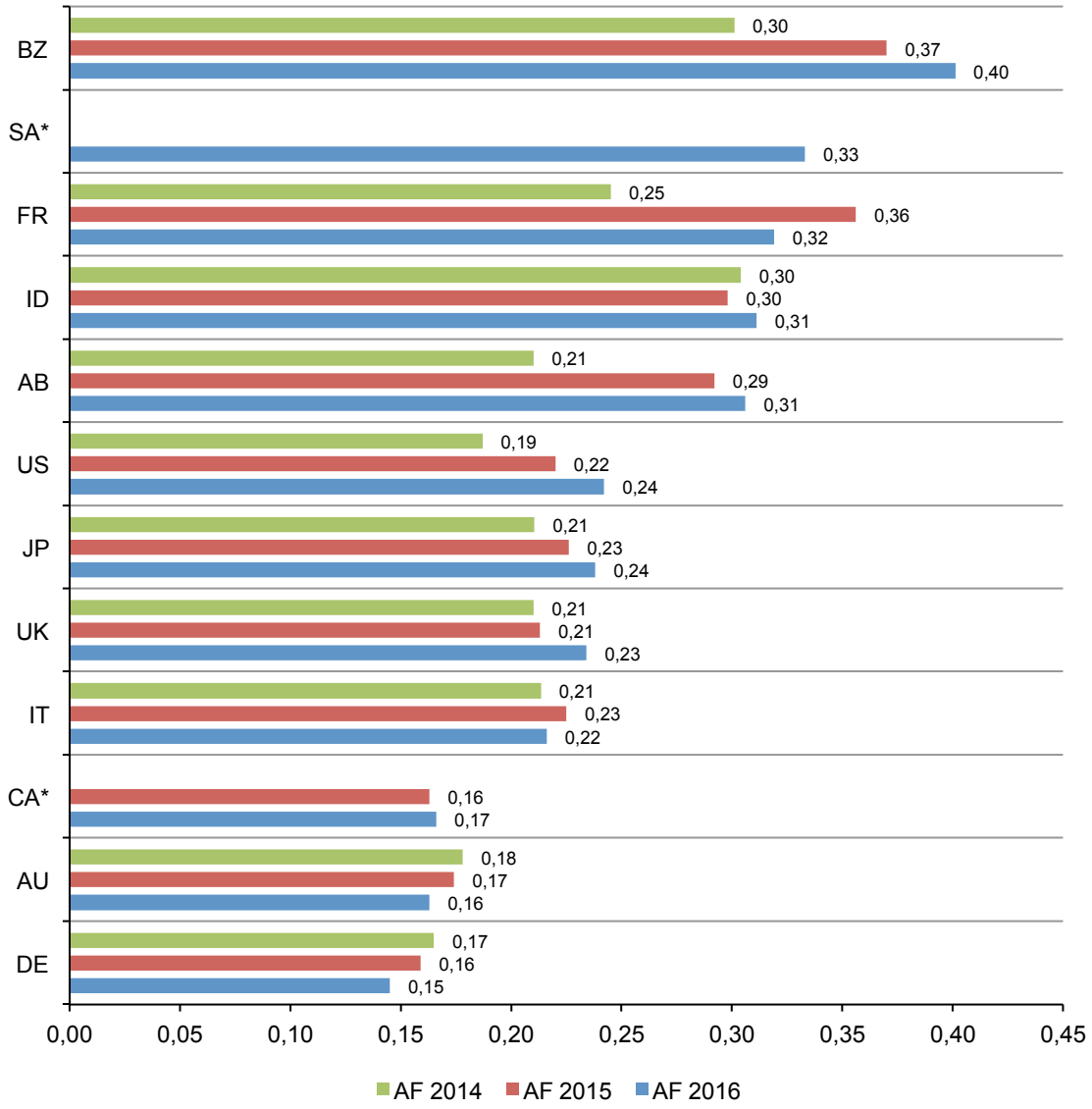


[8]Las probabilidades estimadas se extrajeron de los encuestados mediante una técnica de estimación puntual. Las personas que participaron en las entrevistas de evaluación de costes, como el CISO o el CPO, proporcionaron su estimación de probabilidad de filtración para 10 niveles de incidentes de filtración (rango de 10.000 a 100.000 registros perdidos o robados). La escala de tiempo utilizada fueron los próximos 24 meses. Se extrapoló una distribución de probabilidad agregada para cada una de las 383 empresas participantes.

Las organizaciones de determinados países tienen más probabilidades de sufrir una filtración de datos. La Figura 20 resume la probabilidad de una filtración de datos con un mínimo de 10.000 registros comprometidos para los 12 países. Aunque no podemos generalizar las diferencias por país debido al tamaño de la muestra, la probabilidad estimada de una filtración de datos materiales varía considerablemente entre países.

Brasil y Sudáfrica presentan la mayor probabilidad estimada de sufrir una filtración de datos, mientras que Alemania y Australia la inferior

Figura 20. Probabilidad de una filtración de datos con un mínimo de 10.000 registros comprometidos por país
Promedio general = 25,6%, Mínimo de 10.000 registros comprometidos
*Datos históricos no disponibles en todos los años
Vista consolidada (AF 2016=383, AF 2015=350, AF 2014=315)

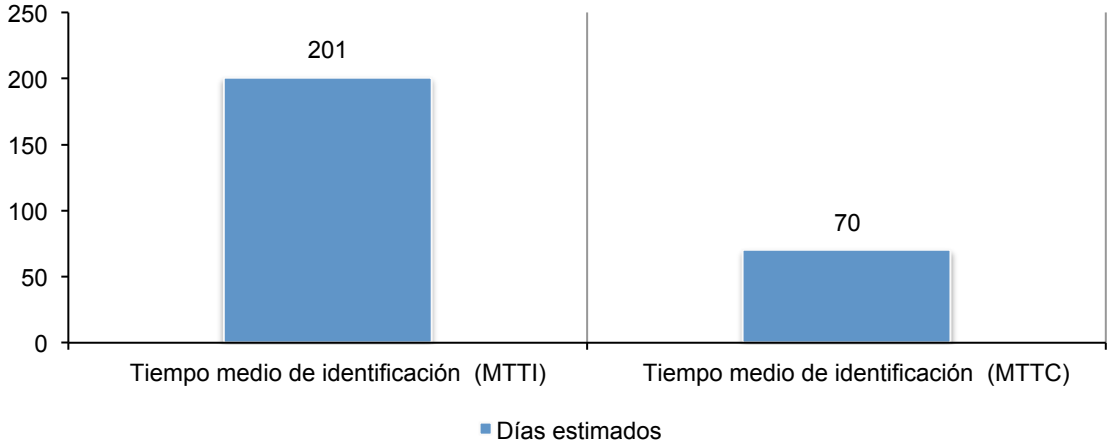


El tiempo dedicado a identificar y contener una filtración afecta al coste

Las métricas Tiempo medio de identificación (MTTI) y Tiempo medio de contención (MTTC) se utilizan para determinar la efectividad de los procesos de respuesta ante incidentes y contención de una organización. La métrica MTTI ayuda a las organizaciones a comprender el tiempo requerido para detectar que se ha producido un incidente y la métrica MTTC calcula el tiempo que se tarda en resolver una situación y, finalmente, restaurar el servicio.

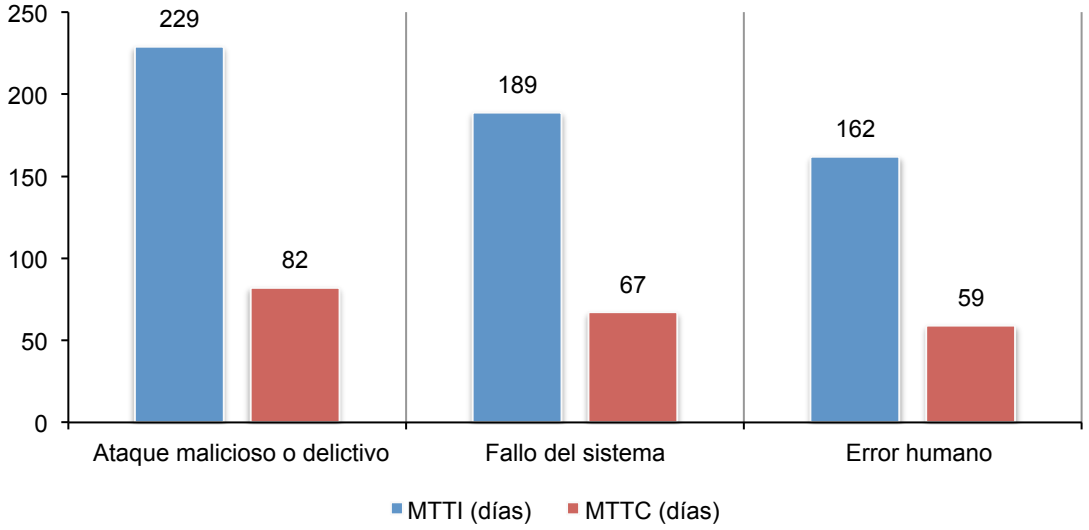
La Figura 21 ofrece datos sobre el tiempo medio de identificación (MTTI) y el tiempo medio de contención (MTTC) de la filtración de datos. Para nuestra muestra consolidada de 383 países, estimamos que el tiempo medio de identificación es de 201 días, con un rango de 20 a 569 días. El tiempo medio de contención fue de 70 días con un rango de 11 a 126 días.

Figura 21. Tiempo medio para identificar y contener incidentes de filtración de datos (en días) Vista consolidada (n = 383)



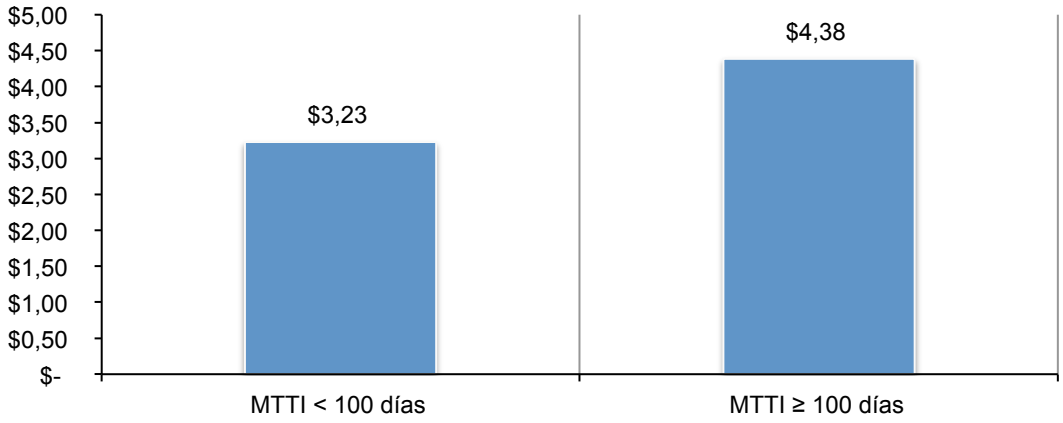
La Figura 22 proporciona el MTTI y MTTC por tres causas raíz del incidente de filtración de datos. Como se muestra, tanto el tiempo de identificación como el de contención fue superior para ataques maliciosos y delictivos (229 y 82 días, respectivamente) y muy inferior para filtraciones de datos causadas por error humano (162 y 59 días, respectivamente).

Figura 22. Tiempo medio para identificar y contener incidentes de filtraciones de datos por causa raíz (en días) Vista consolidada (n = 383)



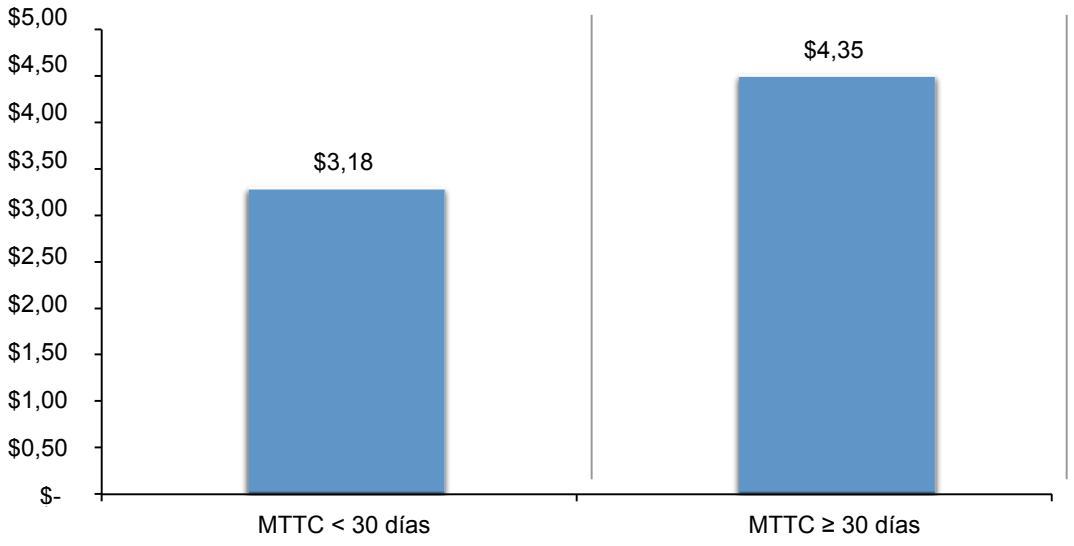
La Figura 23 muestra una relación lineal ascendente entre el coste total de filtración y el tiempo medio para las 383 empresas de los 12 países. Esta relación indica que si no se identifica rápidamente la filtración, los costes serán mayores y pone de manifiesto la importancia de contar con un plan de respuesta ante incidentes. Si el MTTI fue inferior a 100 días, el coste medio para identificar la filtración de datos fue de 3,23 millones de dólares. Si se tardó más de 100 días, el coste fue de 4,38 millones.

Figura 23. Relación entre el tiempo medio de identificación y el coste medio total
Vista consolidada (n=383), calculado en dólares americanos (millones)



La Figura 24 también muestra una regresión lineal ascendente entre el coste total de la filtración y el MTTC. De modo similar al anterior, esta relación indica que si no se contiene rápidamente la filtración, los costes serán mayores. Si el tiempo para contener la filtración fue inferior a 100 días, el coste de contención fue de 3,18 millones de dólares, pero si se necesitaron más de 100 días, el coste ascendió a 4,35 millones.

Figura 24. Relación entre el tiempo medio de contención y el coste medio total
Vista consolidada (n=383), calculado en dólares americanos (millones)



Parte 3. Cómo se calcula el coste de las filtraciones de datos

Para calcular el coste de las filtraciones de datos, utilizamos una metodología de costes denominada Cálculo de costes por actividad (ABC). Esta metodología identifica actividades y asigna un coste de acuerdo con el uso real. Se solicitó a las empresas participantes en el estudio que estimaran el coste para todas las actividades que realizan para resolver la filtración.

Las actividades más comunes para descubrir y responder de inmediato a la filtración de datos incluyen:

- Realizar investigaciones para determinar la causa raíz de la filtración de datos
- Determinar las posibles víctimas de la filtración de datos
- Organizar el equipo de respuesta ante incidentes
- Dirigir las comunicaciones y las relaciones públicas
- Preparar documentos de aviso y otras divulgaciones necesarias para las víctimas y los reguladores de la filtración
- Implementar procedimientos de atención telefónica y formación especializada

Las siguientes son las actividades realizadas normalmente tras descubrir la filtración de datos:

- Servicios de auditoría y consultoría
- Servicios legales para la defensa
- Servicios legales para el cumplimiento normativo
- Servicios gratuitos o con descuento para las víctimas de la filtración
- Servicios de protección de identidades
- Negocio perdido con clientes en base al cálculo de la tasa de abandono o rotación de clientes
- Costes de programas de fidelidad y adquisición de clientes

Cuando la empresa estima un rango de costes para estas actividades, categorizamos los costes como directos, indirectos y de oportunidad, como se define a continuación:

- *Coste directo*: el gasto directo destinado a realizar una actividad determinada.
- *Coste indirecto*: la cantidad de tiempo, esfuerzos y otros recursos organizativos gastados, pero no como desembolso de efectivo directo.
- *Coste de oportunidad*: el coste derivado de las oportunidades de negocio perdidas como consecuencia de la reputación negativa tras notificar a las víctimas la filtración (y revelada públicamente a los medios de comunicación).

Nuestro estudio también analiza las actividades relacionadas con los procesos principales que generan una serie de gastos asociados a la detección de la filtración, la respuesta, la contención y la remediación por parte de una organización. Los costes para cada actividad se exponen en el apartado Conclusiones principales (Parte 2). Los cuatro centros de costes son:

- Detección o descubrimiento: Actividades que permiten a una empresa detectar la filtración de datos personales en riesgo (en almacenamiento) o en movimiento.
- Escalado: Actividades necesarias para reportar la filtración de información protegida al personal adecuado en un periodo de tiempo especificado
- Notificación: Actividades que permiten a la empresa realizar las notificaciones con una carta, llamada, email o aviso general de que la información personal ha sido robada o perdida.
- Tras la filtración de datos: Actividades que facilitan a las víctimas comunicarse con la empresa para realizar preguntas adicionales u obtener recomendaciones a fin de minimizar los posibles daños. Estas actividades también incluyen el control de informes de crédito o la emisión de una nueva cuenta (o tarjeta de crédito).

Además de las actividades anteriores relacionadas con los procesos, la mayoría de las empresas registran costes de oportunidad relacionados con el incidente de filtración, como consecuencia de la pérdida de confianza de los clientes actuales y futuros. En consecuencia, nuestro estudio revela que la publicidad negativa asociada a una filtración de datos afecta a la reputación, pudiendo incrementar las tasas de rotación o abandono anómalo, así como un menor índice de adquisición de nuevos clientes.

Para extrapolar estos costes de oportunidad, aplicamos un método de estimación de costes que se basa en el "valor de tiempo de vida de un cliente" de un cliente medio, tal y como se defina para cada organización participante.

- Rotación de clientes existentes: El número estimado de clientes con mayor probabilidad de finalizar su relación con la empresa debido al incidente de filtración. La pérdida incremental es rotación anómala atribuible al incidente de filtración. Este número es un porcentaje anual que se basa en estimaciones proporcionadas por la gestión durante el proceso de entrevistas de benchmarking[9].

- Menor adquisición de clientes: El número estimado de clientes potenciales que no se relacionarán con la organización debido a la filtración. Este número se proporciona como porcentaje anual.

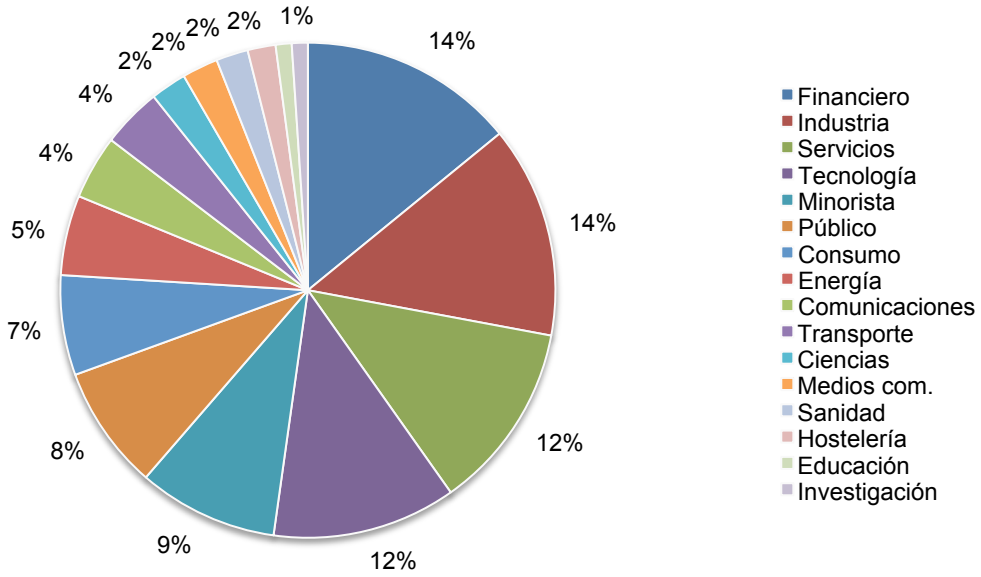
Reconocemos que la pérdida de datos que no son de clientes, como registros de empleados, no incidirá sobre el abandono o rotación en la organización[10]. En estos casos, esperaríamos que la categoría de costes de negocio fuera inferior si las filtraciones de datos no implican datos de clientes (incluyendo información de transacciones de pago).

[9]En varias instancias, la rotación es parcial: las víctimas mantuvieron la relación con la organización, pero disminuyó el volumen de actividad del cliente. Esta disminución parcial es especialmente notable en determinados sectores – como servicios financieros o entidades del sector público, donde la terminación resulta costosa o inviable económicamente.
[10]En este estudio, consideramos la información de ciudadanos, pacientes y estudiantes como datos de clientes.

Parte 4. Características de la organización y métodos de benchmarking

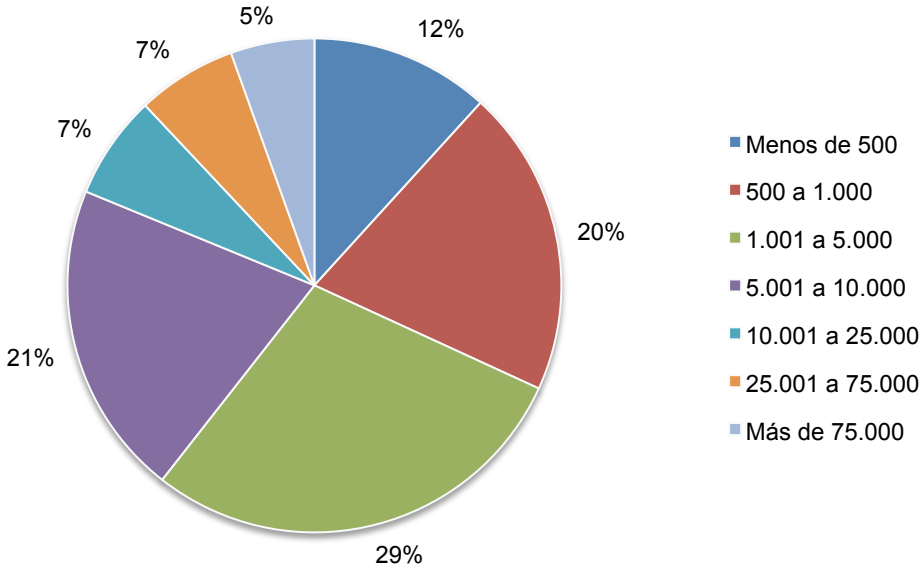
El gráfico circular 3 muestra la distribución de las organizaciones del benchmark clasificadas por su sector principal. En el estudio de este año se representan 16 sectores. El sector con mayor representación es el de servicios financieros, que incluye bancos, aseguradoras, gestión de inversiones y procesadores de pago.

Gráfico circular 3. Distribución de la muestra por segmentos de sector
Vista consolidada (n=383)



El gráfico circular 4 muestra la distribución de las organizaciones del benchmark por plantilla total. Los segmentos de mayor tamaño incluyen empresas con más de 1.000 empleados.

Gráfico circular 4. Plantilla global de las empresas participantes
Vista consolidada (n=383)



Los métodos de recopilación de datos no incluyeron la información contable real, sino que se basaron en estimaciones numéricas de acuerdo con los conocimientos y la experiencia de cada participante. Dentro de cada categoría, la estimación de costes se dividió en dos etapas. Primero, el instrumento de benchmark solicitaba a los participantes que realizaran estimaciones de costes directos para cada categoría de costes marcando un rango variable definido en el siguiente formato de línea numérica.

Cómo utilizar la línea numérica: La línea numérica proporcionada en cada categoría de costes por filtración de datos es un modo de obtener su mejor estimación para la suma de gastos incurridos en desembolsos de efectivo, mano de obra y sobrecarga. Marque un único punto en algún lugar entre los límites inferiores y superiores establecidos arriba. Puede restablecer los límites inferiores y superiores de la línea numérica en cualquier momento durante el proceso de la entrevista.

Exponga aquí su estimación de costes directos para [categoría de coste presentada]

LL	_____|_____	UL

El valor numérico obtenido a partir de la línea numérica, en lugar de una estimación de punto para cada categoría de coste presentada, ha permitido preservar la confidencialidad y garantizar una tasa de respuesta superior. El instrumento de benchmark también solicitaba a los profesionales que proporcionaran una segunda estimación para costes indirectos y de oportunidad, por separado.

Para mantener el proceso de benchmarking a un tamaño gestionable, limitamos prudentemente los elementos a solo aquellos centros de actividad de coste que consideramos cruciales para el cálculo del coste de la filtración de datos. Tras varios debates con expertos, el conjunto final de elementos incluyó un conjunto fijo de actividades de costes. Una vez recopilada la información del benchmark, se volvió a examinar detenidamente cada instrumento para garantizar la coherencia e integridad.

A fin de mantener la máxima confidencialidad, el instrumento de benchmark no capturó información específica de la compañía. Los materiales no contenían códigos de seguimiento ni otros métodos que pudieran vincular respuestas a empresas participantes.

El ámbito de los elementos de coste de filtración de datos de nuestro instrumento de benchmark se limitó a categorías de costes conocidas, que se aplican a un amplio conjunto de operaciones de negocio que tratan información personal. Consideramos que un estudio centrado en el proceso de negocio, y no en actividades de cumplimiento de privacidad o protección de datos, generaría resultados de mayor calidad.

Parte 5. Limitaciones

Nuestro estudio utiliza un método de benchmarking de propiedad confidencial, que se ha desplegado con éxito en investigaciones anteriores. Sin embargo, existen limitaciones inherentes a esta investigación de benchmark que deben considerarse detenidamente antes de extraer conclusiones.

- Resultados no estadísticos: Nuestro estudio se basa en una muestra representativa, no estadística, de entidades globales que durante los pasados 12 meses han sufrido una filtración en la que se han perdido o robado registros de clientes. Las inferencias estadísticas, los márgenes de error y los intervalos confianza no se pueden aplicar a estos datos dado que nuestros métodos de muestreo no son científicos.

- Falta de respuesta: Las conclusiones actuales se basan en una pequeña muestra representativa de benchmarks. En este estudio global, 383 empresas realizaron el proceso de benchmark. El sesgo de falta de respuesta no se probó, por lo que es posible que empresas que no participaron sean sustancialmente diferentes en términos de costes de filtración de datos subyacentes.

- Sesgo de marco de muestreo: Como nuestro marco de muestreo es parcial, la calidad de los resultados se ve influida en la medida en que el marco es representativo de la población de las empresas del estudio. Creemos que el marco de muestreo actual se inclina hacia empresas con programas de seguridad de la información o privacidad más desarrollados.

- Información específica de la empresa: La información del benchmark es sensible y confidencial. Por lo tanto, el instrumento actual no captura información que identifique a la empresa. Además, permite utilizar variables de respuesta categóricas para revelar información demográfica sobre la empresa y la categoría del sector.

- Factores no medidos: Para mantener la coherencia del guión de la entrevista, decidimos omitir otras variables importantes en nuestros análisis, como las principales tendencias y las características de la organización. No se puede determinar en qué medida las variables omitidas podrían explicar los resultados del benchmark.

- Resultados de costes extrapolados: La calidad de la investigación del benchmark se basa en la integridad de las respuestas confidenciales proporcionadas por los encuestados de las empresas participantes. A pesar de que se pueden incorporar algunas comprobaciones y balances al proceso de benchmarking, siempre existe la posibilidad de que los encuestados no proporcionaran respuestas precisas o verdaderas. Además, el uso de métodos de extrapolación de costes, en lugar de datos reales de costes, podría introducir sesgos e imprecisiones de forma involuntaria.

Si tiene alguna duda o comentario acerca de este informe de investigación, o bien le gustaría obtener copias adicionales del documento (incluyendo el permiso para citar o reutilizar este informe), póngase en contacto por correo postal, 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

Encontrará copias completas de los informes de cada país en **www.ibm.com/security/data-breach**

Ponemon Institute LLC

Advancing Responsible Information Management

Ponemon Institute se dedica a la investigación y a la educación independientes, que proporcionan prácticas avanzadas de gestión de la privacidad y la información responsable a empresas y organismos gubernamentales. Nuestra misión consiste en realizar estudios empíricos de calidad sobre cuestiones importantes que afectan a la gestión y a la seguridad de la información sensible, tanto personal como empresarial.

Como miembro del **Consejo de Organizaciones de Investigación y Encuestas de Estados Unidos** (CASRO), seguimos estrictos estándares de confidencialidad de datos, privacidad e investigación ética. No recopilamos información identificable personalmente de personas (o empresas en nuestros estudios de negocio). Además, cumplimos estrictos estándares de calidad para garantizar que a los encuestados se les realicen preguntas pertintentes y adecuadas.