



# Situación de la seguridad centrada en los datos

---

## Patrocinado por Informatica

Elaborado de forma independiente por Ponemon Institute LLC

Fecha de publicación: junio de 2014

## Situación de la seguridad centrada en los datos

Ponemon Institute, junio de 2014

### Parte 1. Introducción

Ponemon Institute se complace en presentar los resultados del estudio “*Situación de la seguridad centrada en los datos*”, patrocinado por Informatica. Este estudio se ha llevado a cabo con el objetivo de averiguar qué respuesta dan las organizaciones a las amenazas que se ciernen sobre la seguridad de sus datos estructurados y no estructurados. De acuerdo con nuestros hallazgos, preocupa mucho más la incertidumbre acerca de la ubicación de los datos sensibles y confidenciales que las malas intenciones de los empleados o los piratas.

Hemos encuestado a 1.587 profesionales de la seguridad de TI y de TI global de 16 países.<sup>1</sup> La lista de países participantes figura en el apéndice del informe. Para garantizar que las respuestas fueran prácticas y de calidad, solo se ha permitido la participación de profesionales de TI entre cuyas tareas se incluye la protección de datos estructurados o no estructurados sensibles o confidenciales.

A efectos del presente estudio, la seguridad centrada en los datos asigna a los datos, durante su creación, una política de seguridad, la cual los acompaña allá donde se repliquen, copien o integren, todo ello con independencia de la plataforma tecnológica o de alojamiento y de la ubicación geográfica. La seguridad centrada en los datos incluye tecnologías como el enmascaramiento de datos, el cifrado, la tokenización y la supervisión de la actividad de las bases de datos. En este estudio, sin embargo, se revela que las soluciones automatizadas resultan de utilidad para mejorar la posición de la organización en cuanto al cumplimiento y la protección de los datos se refiere.

### Conclusiones principales del estudio

- **Los datos inescrutables quitan el sueño a los profesionales de TI.** El 57% de los encuestados confirma que su mayor desvelo es ignorar dónde están ubicados los datos sensibles o confidenciales de la organización. En segundo lugar, se halla el 51% al que le preocupa la migración a las nuevas plataformas móviles.
- **A menudo, los datos sensibles o confidenciales pasan inadvertidos a la seguridad de TI.** Solo el 16% de los encuestados cree saber dónde se encuentran todos los datos estructurados sensibles y un pequeño porcentaje (el 7%) sabe dónde residen los datos no estructurados.
- **Las organizaciones confían, sobre todo, en la clasificación de los datos como sensibles para proteger los activos de datos.** Las dos tecnologías más empleadas con los datos estructurados son la clasificación de los datos como sensibles y los controles de acceso a las aplicaciones. Solo el 19% responde que su organización utiliza derechos y gestión de control del acceso centralizados, mientras que el 14% utiliza auditorías del acceso y de los sistemas de archivos.
- **Existe el convencimiento de que las soluciones automatizadas de detección de datos sensibles reducen los riesgos para los datos y aumentan la eficacia de la seguridad.** Pese a la percepción positiva de las soluciones automatizadas, el 60% de los encuestados afirma que no utiliza ninguna para detectar dónde se hallan los datos sensibles o confidenciales. Del 40% de encuestados que sí emplea soluciones automatizadas en su organización, el 64% indica que lo hace para detectar dónde se hallan los datos sensibles o confidenciales en las bases de datos y las aplicaciones empresariales; solo el 22% las utiliza para detectar datos en los archivos y correos electrónicos.

---

<sup>1</sup> El análisis de la muestra mundial se ha dividido en tres regiones: Norteamérica, Europa y Resto del mundo.

- **Determinadas soluciones automatizadas resultan de utilidad para mejorar la posición de la organización en cuanto al cumplimiento y la protección de los datos se refiere.** Las funcionalidades más habituales son el historial automatizado de acceso de los usuarios con supervisión en tiempo real y, a continuación, la automatización del flujo de trabajo de políticas.

## Parte 2. Conclusiones principales

Esta sección presenta el análisis de las conclusiones contrastadas. En el apéndice del informe figuran las conclusiones auditadas completas. El informe está organizado por los temas siguientes:

- Los datos inescrutables quitan el sueño a los profesionales de TI
- Las soluciones de seguridad no suelen mejorar la visibilidad de la ubicación de los datos ni del acceso de los usuarios
- Consiga un sueño reparador una vez implantadas las soluciones apropiadas

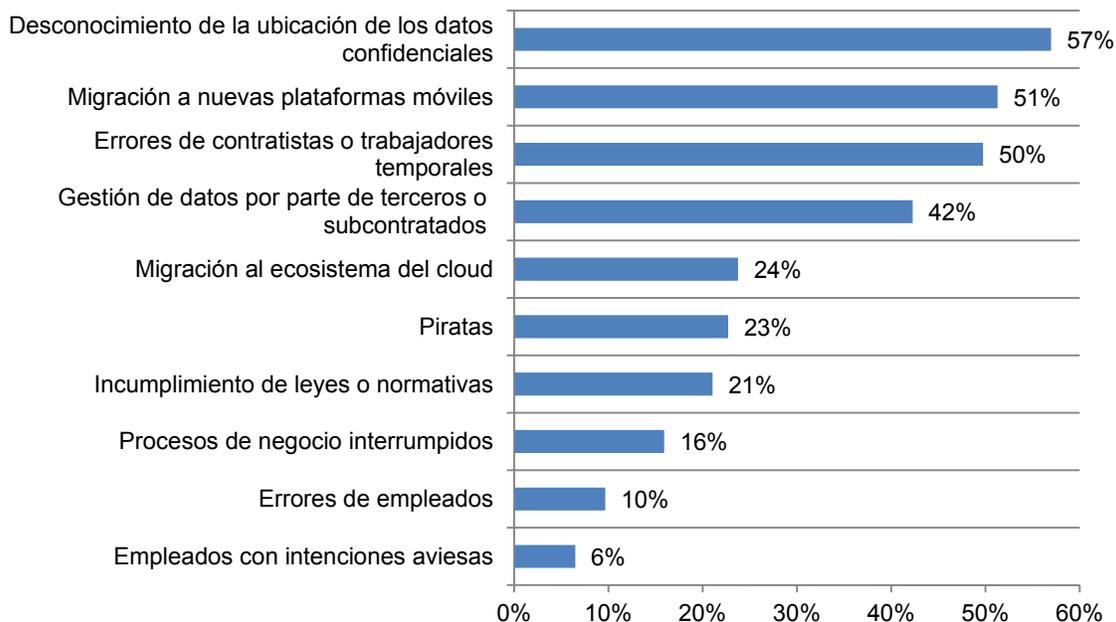
### Los datos inescrutables quitan el sueño a los profesionales de TI

**A la mayoría de los encuestados le quita el sueño ignorar la ubicación de los datos sensibles o confidenciales, ya que representa un elevado riesgo para la seguridad.**

Se mostró a los encuestados una lista con amenazas y riesgos que pueden suponer una pesadilla para los profesionales de la seguridad de TI. Tal y como se muestra en la figura 1, el 57% confirma que su mayor desvelo es ignorar dónde están ubicados los datos sensibles o confidenciales de la organización. En segundo lugar, se halla el 51% al que le preocupa la migración a las nuevas plataformas móviles. Los piratas, el incumplimiento de normativas y los empleados con intenciones aviesas ocupan un lugar mucho más bajo de la lista.

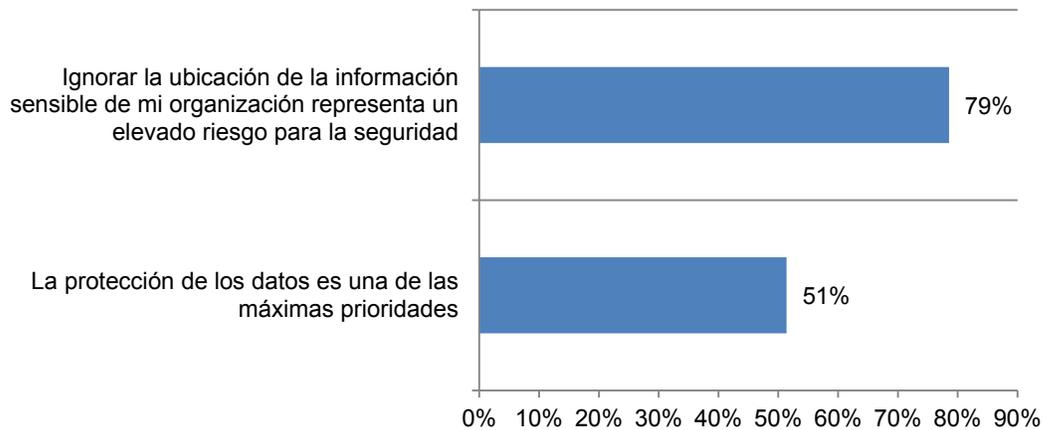
**Figura 1. ¿Qué le quita el sueño?**

Se permiten tres respuestas



**La vulnerabilidad de la seguridad de los datos constituye una amenaza grave pero, con frecuencia, no es una cuestión prioritaria.** La figura 2 revela una desproporción considerable entre el porcentaje de encuestados que se muestra de acuerdo con que ignorar dónde reside la información sensible y confidencial constituye una amenaza grave y el porcentaje de encuestados que confirma que es un tema prioritario en su organización. El 79% de los encuestados cree que supone un riesgo grave para la seguridad al que debe hacer frente su organización. Sin embargo, un porcentaje mucho más reducido (el 51%) cree que la protección de los datos es una de las máximas prioridades de su organización. Esa diferencia indica que quizá existan dificultades al adquirir los recursos necesarios para reducir el riesgo.

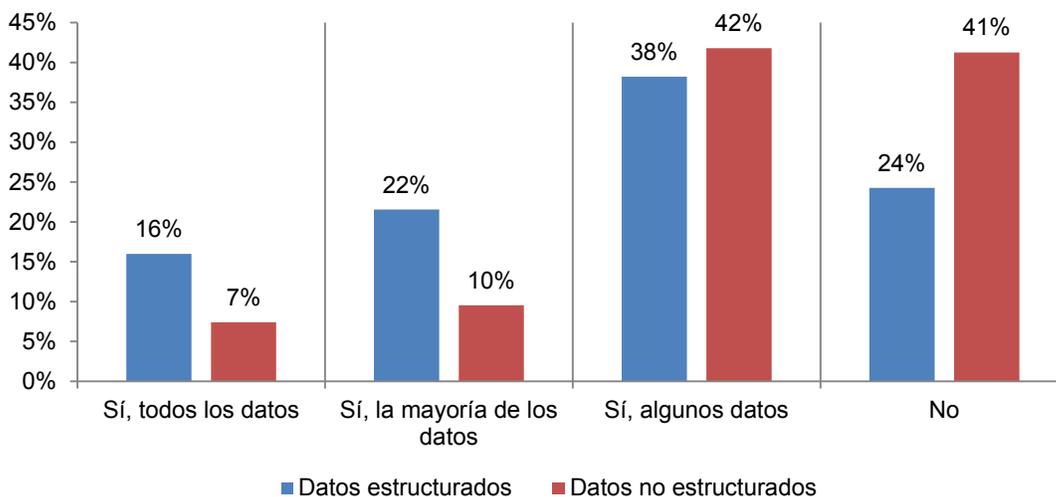
**Figura 2. Características sobre la seguridad de los datos sensibles**  
Están combinadas las respuestas “De acuerdo” y “Totalmente de acuerdo”



**En su mayoría, las organizaciones ignoran dónde están ubicados los datos sensibles o confidenciales.** Según se representa en la figura 3, solo el 16% de los encuestados cree saber dónde se encuentran todos los datos estructurados sensibles y un pequeño porcentaje (el 7%) sabe dónde residen los datos no estructurados.

También se observa una gran diferencia entre datos estructurados y no estructurados. El 24% de los encuestados afirma que no puede determinar dónde se encuentran los datos estructurados, mientras que el 41% no tiene idea alguna con respecto a los datos no estructurados de su organización.

**Figura 3. ¿Sabe dónde están ubicados sus datos sensibles o confidenciales?**

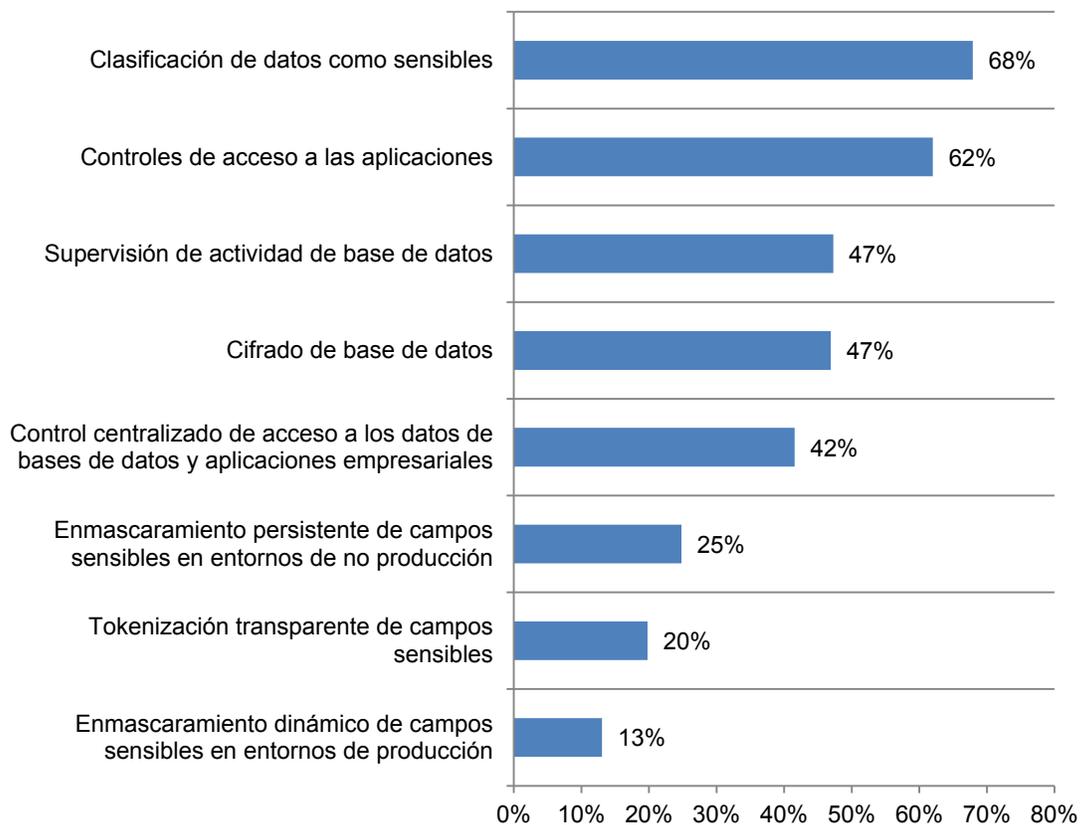


**Las soluciones de seguridad no suelen mejorar la visibilidad de la ubicación de los datos ni el acceso de los usuarios**

**Las organizaciones confían, sobre todo, en la clasificación de los datos como sensibles para proteger los activos de datos estructurados y no estructurados.** Los encuestados calculan que, de media, el 34% de los datos de su organización se puede clasificar como sensible o confidencial, incluidos tanto los datos estructurados como no estructurados. El 53% de los encuestados piensa que el mayor riesgo lo corren los datos de los clientes, seguido por el 38%, que señala la propiedad intelectual.

La figura 4 revela las tecnologías o herramientas que emplean las organizaciones para proteger los activos de datos estructurados. Las dos más empleadas con los datos estructurados son la clasificación de los datos como sensibles y los controles de acceso a las aplicaciones.

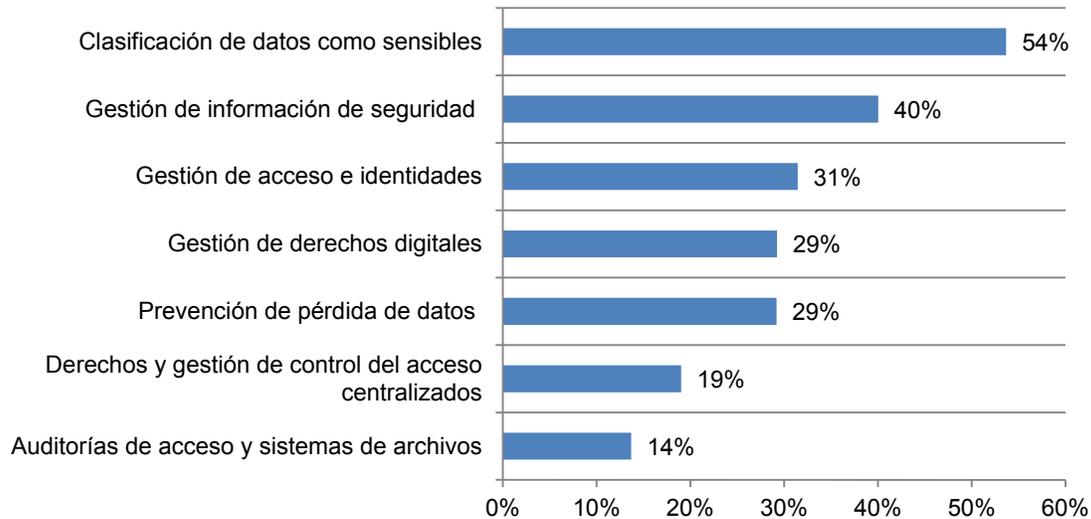
**Figura 4. Tecnologías de protección de los activos de datos estructurados**  
Se permite más de una respuesta



En el caso de los datos no estructurados (figura 5), las organizaciones también emplean la clasificación de los datos como sensibles, seguida de los sistemas de gestión de la información de seguridad.

**Figura 5. Tecnologías de protección de los activos de datos no estructurados**

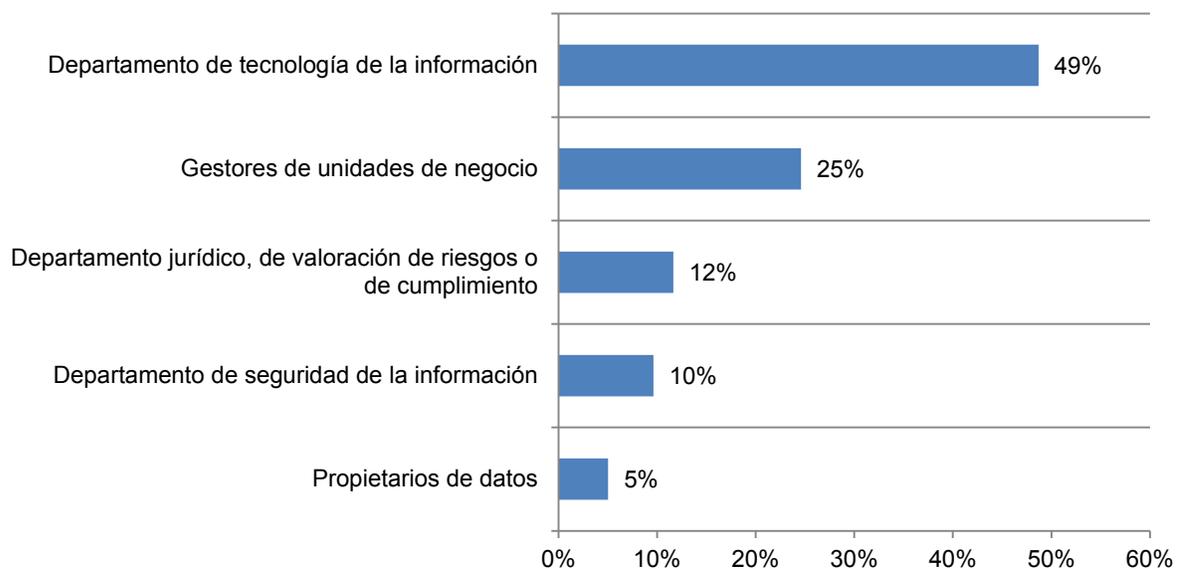
Se permite más de una respuesta



La mayoría de las veces, el departamento de TI es el responsable de conceder a los usuarios acceso a los activos de datos. Tal y como se muestra en la figura 6, el 49% confirma que la función de TI franquea el acceso a los empleados y el 25% atribuye esa responsabilidad a los gestores de las unidades de negocio.

**Figura 6. ¿Quién es el principal responsable de conceder a los usuarios acceso a los activos de datos?**

Se permiten dos respuestas

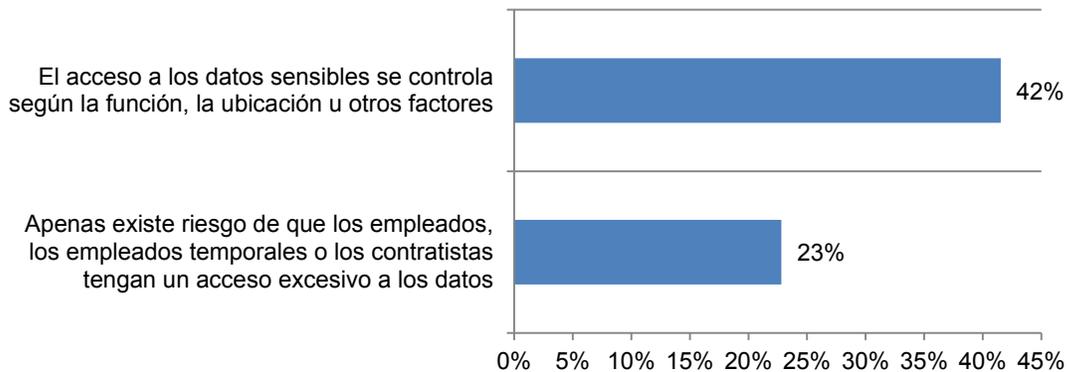


**El control del acceso a la información sensible es fundamental para reducir riesgos.**

El 42% de los encuestados indica que el acceso a los datos sensibles se controla según la función, la ubicación y otros factores, tal y como se revela en la figura 7. No obstante, de los resultados obtenidos, se infiere que los procedimientos de control del acceso de las empresas no funcionan. Solo el 23% cree que los empleados, los empleados temporales o los contratistas disponen del grado de acceso apropiado y que apenas existe riesgo de que esos usuarios tengan un acceso excesivo.

**Figura 7. Características sobre la seguridad de los datos sensibles**

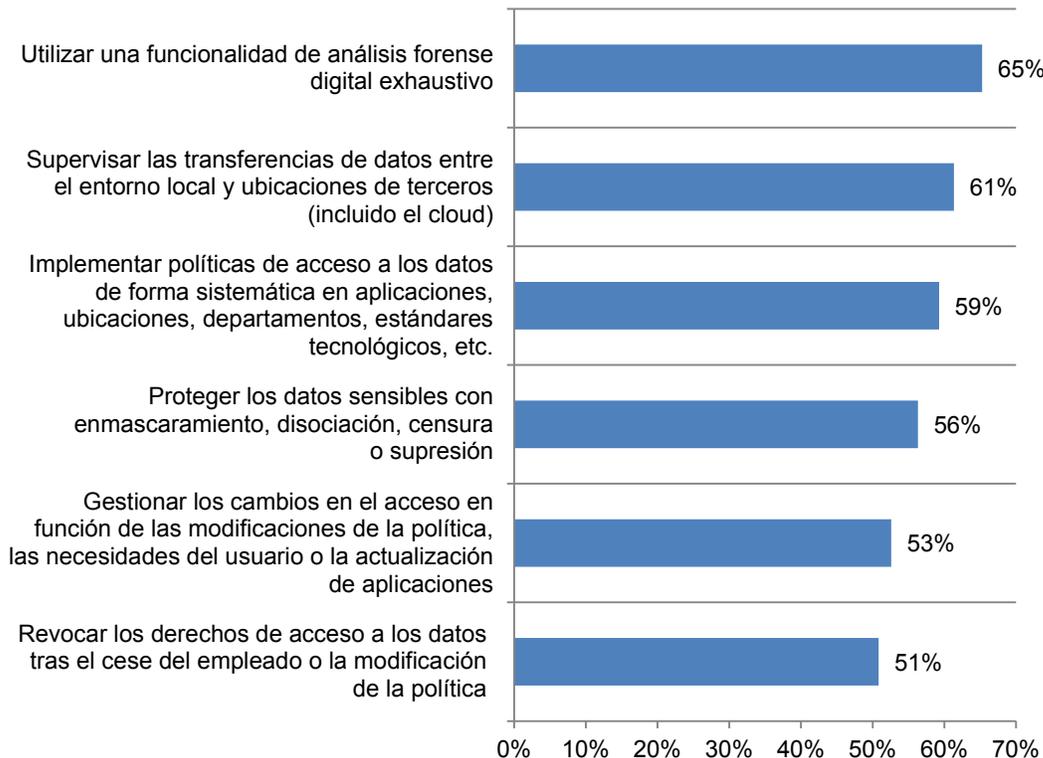
Están combinadas las respuestas “De acuerdo” y “Totalmente de acuerdo”



**Los procedimientos de seguridad de los activos de datos se califican como escasos o incumplidos.** En la figura 8, se relacionan los procedimientos de seguridad que no se siguen en las organizaciones. Tal y como se observa, casi ninguna organización emplea el análisis forense digital exhaustivo, la supervisión de transferencias de datos entre el entorno local y ubicaciones de terceros (incluido el cloud) ni la aplicación sistemática de políticas de acceso a los datos.

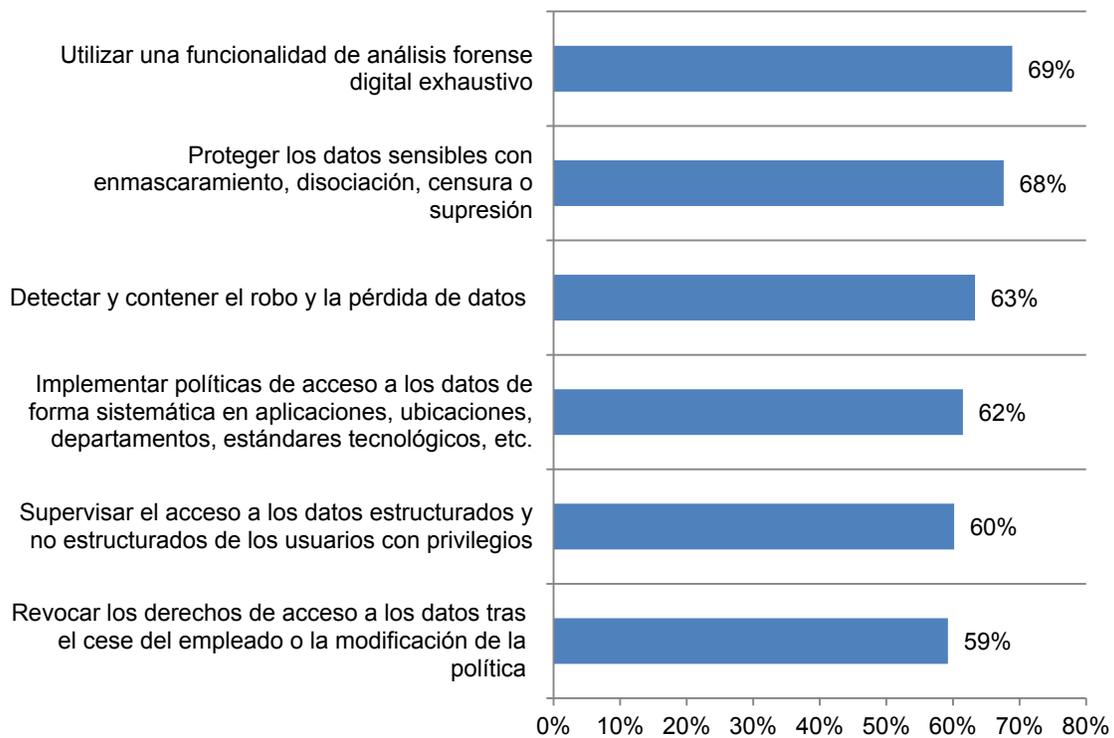
**Figura 8. Procedimientos de seguridad de los activos de datos de las bases de datos**

Están combinados los procedimientos que apenas se cumplen o no se cumplen en absoluto



**No se han implantado muchos de los procedimientos de seguridad relativos a los datos sensibles y confidenciales de los correos electrónicos.** Tal y como se observa en la figura 9, casi ninguna organización emplea el análisis forense digital exhaustivo, la protección de datos sensibles con enmascaramiento, disociación, redacción o supresión ni la aplicación sistemática a aplicaciones, ubicaciones, departamentos y estándares tecnológicos de políticas de acceso a los datos.

**Figura 9. Procedimientos de seguridad de los activos de datos de los correos electrónicos**  
Están combinados los procedimientos que apenas se cumplen o no se cumplen en absoluto



**Los procedimientos de seguridad de los datos de los archivos no suelen supervisar las transferencias de datos entre el entorno local y ubicaciones de terceros (incluido el cloud).** En la figura 10, se muestran los procedimientos de seguridad de los activos de datos de los archivos que, según los encuestados, son escasos o no se cumplen en sus organizaciones. Además de obviar la supervisión de las transferencias de datos, las organizaciones no tienen ninguna funcionalidad de análisis forense digital exhaustivo ni aplican políticas de acceso a los datos de forma sistemática a las aplicaciones o ubicaciones.

**Figura 10. Procedimientos de seguridad de los activos de datos de los archivos**  
Están combinados los procedimientos que apenas se cumplen o no se cumplen en absoluto

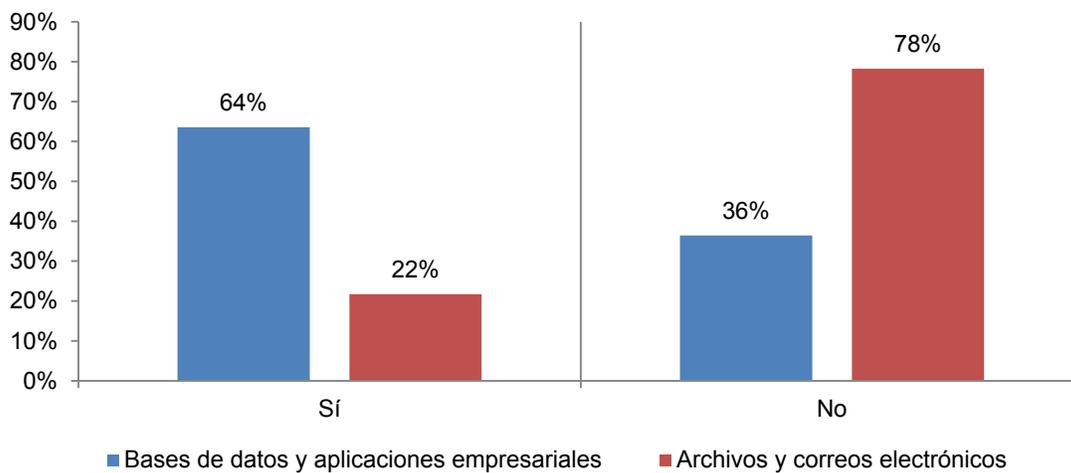


## Consiga un sueño reparador una vez implantadas las soluciones apropiadas

**Existe el convencimiento de que las soluciones de detección de datos sensibles y automatizadas reducen los riesgos para los datos y aumentan la eficacia de la seguridad.** Pese a la percepción positiva de las soluciones automatizadas, el 60% de los encuestados afirma que no utiliza ninguna para detectar dónde se hallan los datos sensibles o confidenciales.

Tal y como se muestra en la figura 11, del 40% de encuestados que sí emplea soluciones automatizadas en su organización, el 64% indica que lo hace para detectar dónde se hallan los datos sensibles o confidenciales en las bases de datos y las aplicaciones empresariales; solo el 22% señala que tiene una solución automatizada de detección para los datos que se hallan en los archivos y los correos electrónicos.

**Figura 11. Soluciones automatizadas empleadas para detectar datos sensibles o confidenciales en bases de datos, aplicaciones empresariales, archivos y correos electrónicos**



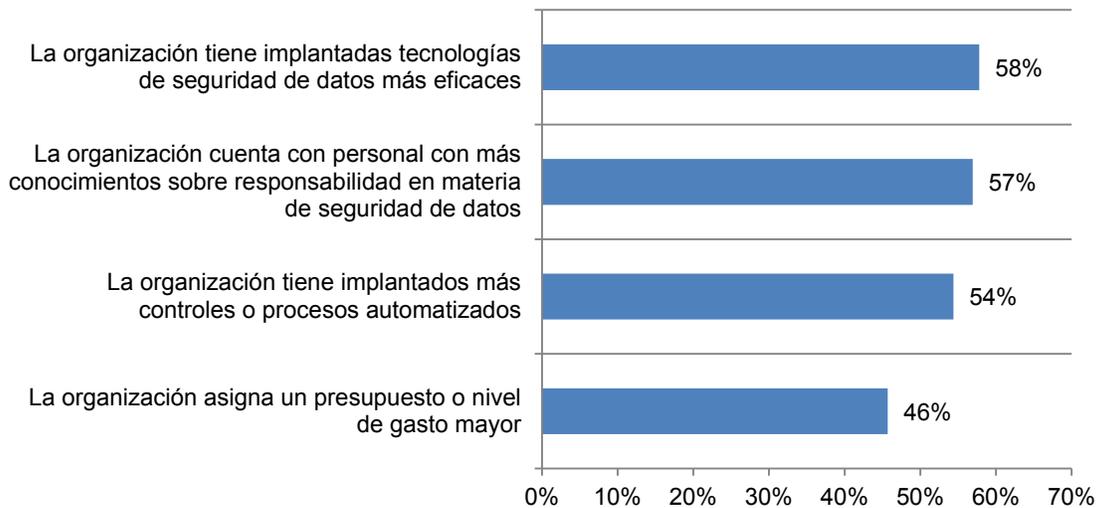
**Es posible reducir las filtraciones de datos.** El 72% de las organizaciones incluidas en el estudio ha sido víctima de alguna filtración de datos en los 12 meses anteriores. En opinión de los encuestados, esos incidentes se podrían haber impedido de haber contado con tecnologías de seguridad de datos eficaces y personal cualificado.

En la figura 12, se muestran las medidas tomadas para impedir las filtraciones de datos o reducir su magnitud y frecuencia. Según el 58% de los encuestados, unas tecnologías de seguridad de datos más eficaces reducirían los riesgos y el 57% cree que, si el personal tuviera más conocimientos sobre la responsabilidad en materia de seguridad de datos, habría disminuido la probabilidad de que se produjera la filtración.

El 54% piensa que la filtración se podría evitar con los controles o los procesos automatizados implantados. No parece que el presupuesto sea un factor decisivo a la hora de reducir el riesgo de incidentes. Un porcentaje menor de encuestados (el 46%) cree que la filtración se habría evitado si su organización hubiese asignado un presupuesto o un nivel de gasto mayor.

**Figura 12. Maneras de haber evitado un incidente de filtración de datos**

Están combinadas las respuestas “Probablemente” y “Muy probablemente”

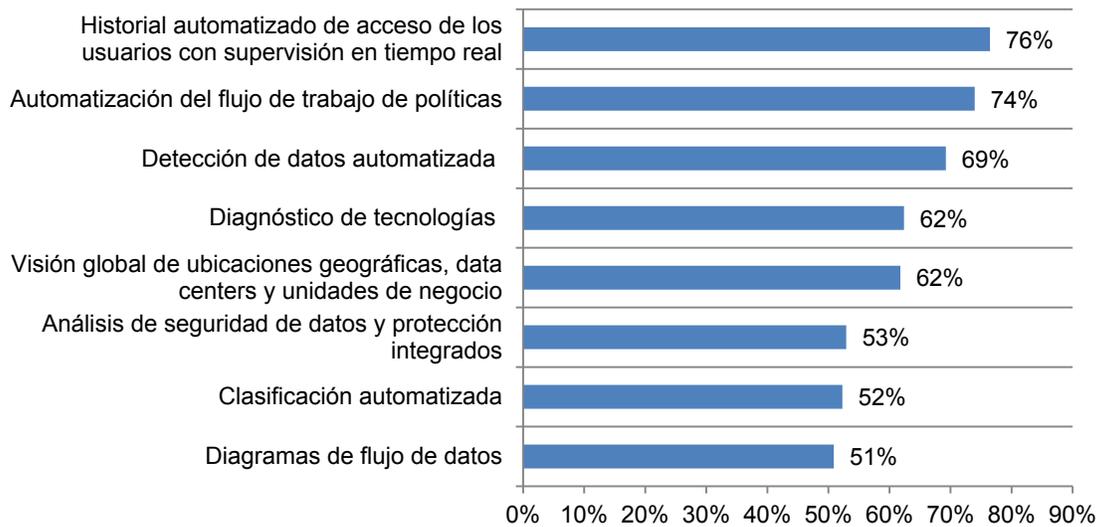


**Determinadas soluciones automatizadas resultan de utilidad para mejorar la posición de la organización en cuanto al cumplimiento y la protección de los datos se refiere.**

En la figura 13, se relacionan las ocho funcionalidades de seguridad centrada en los datos que, en opinión de la mayoría de los encuestados, serían valiosas a la hora de mejorar la posición en cuanto al cumplimiento y la protección de los datos se refiere. Según los encuestados, las funcionalidades más habituales son el historial de acceso de los usuarios automatizado con supervisión en tiempo real, seguido de la automatización del flujo de trabajo de políticas (el 76% y el 74% de los encuestados, respectivamente). Les sigue de cerca el 69% de los encuestados, que piensa que la detección de datos automatizada sería beneficiosa.

**Figura 13. ¿Supondrían alguna mejora del cumplimiento y la protección de los datos las ocho funcionalidades de seguridad centrada en los datos siguientes?**

Están combinadas las respuestas "Mejora considerable" y "Mejora"



### Parte 3. Diferencias entre las regiones mundiales

En esta sección, se ofrece el análisis de las diferencias más significativas entre los países incluidos en el estudio.

**La preocupación por la situación de la seguridad de los datos quita el sueño a los encuestados de todo el mundo.** La figura 14 muestra que la mayoría de los encuestados están preocupados por las amenazas que se ciernen sobre los activos de datos de la organización por ignorar dónde residen los datos sensibles o confidenciales. Los encuestados de Resto del mundo son los que sufren los mayores desvelos. En comparación con los demás países, los encuestados europeos son quienes se inquietan más por el incumplimiento de leyes o normativas.

**Figura 14. ¿Qué le quita el sueño?**

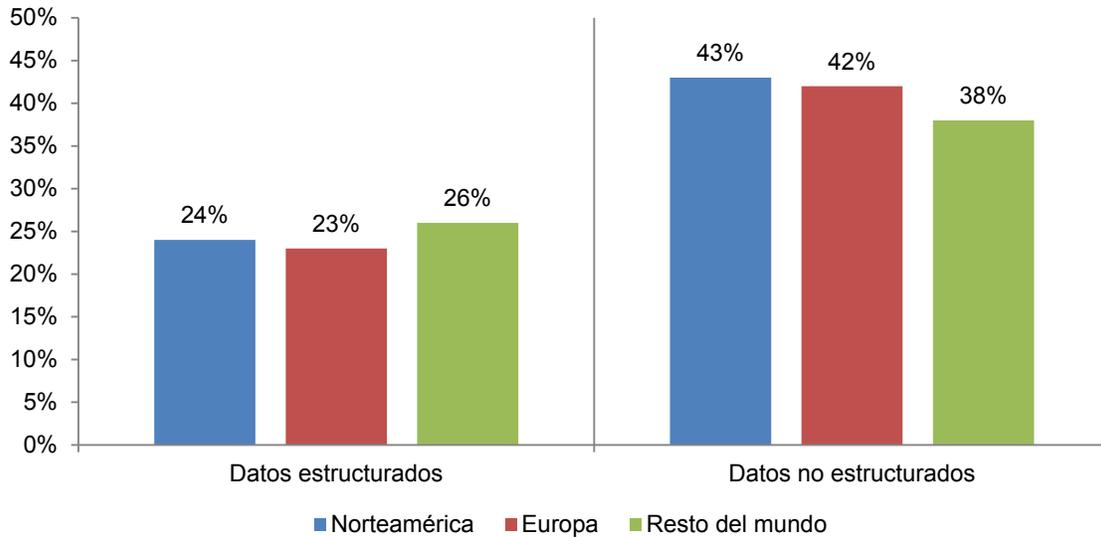
Se permiten tres respuestas



**En su mayoría, las organizaciones ignoran dónde están ubicados los datos sensibles o confidenciales.** Según se representa en la figura 15, apenas la cuarta parte de los encuestados en el estudio de todas las zonas del mundo cree saber dónde se encuentran todos los datos estructurados sensibles. No lo saben, en concreto, el 24% de los encuestados norteamericanos, el 23% de los encuestados europeos y el 26% de los encuestados de otros países. Cuando se trata de conocer la ubicación de los datos no estructurados de la organización, la incertidumbre alcanza un porcentaje mucho más elevado.

**Figura 15. ¿Sabe dónde están sus datos?**

Se muestran los porcentajes de la respuesta "No"

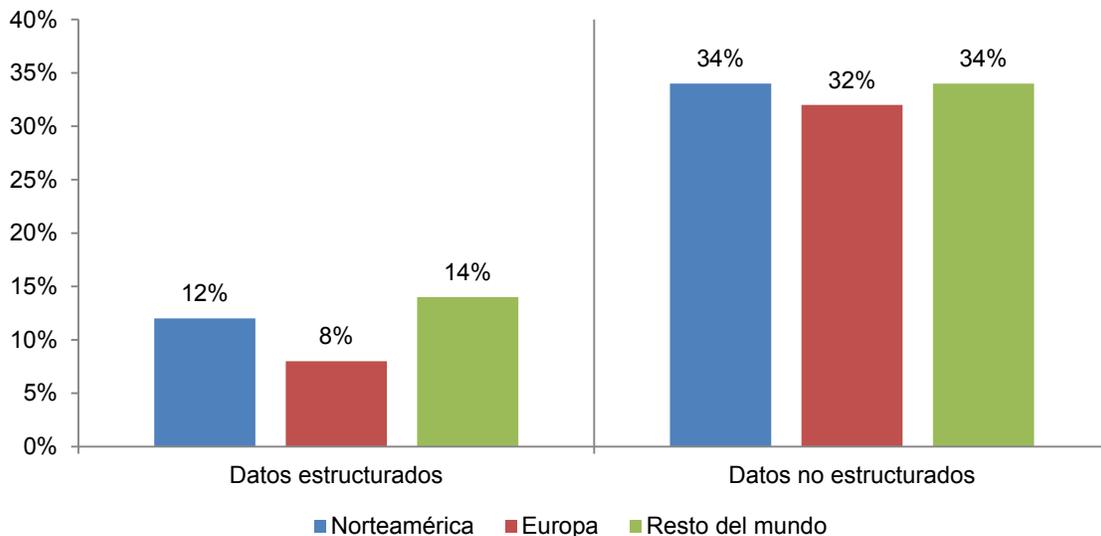


**En todo el mundo, resulta complicado detectar las filtraciones de datos no estructurados.**

En la figura 16, se revela que existe más confianza en detectar una filtración relacionada con los datos estructurados que si el resultado es la pérdida o el robo de datos no estructurados.

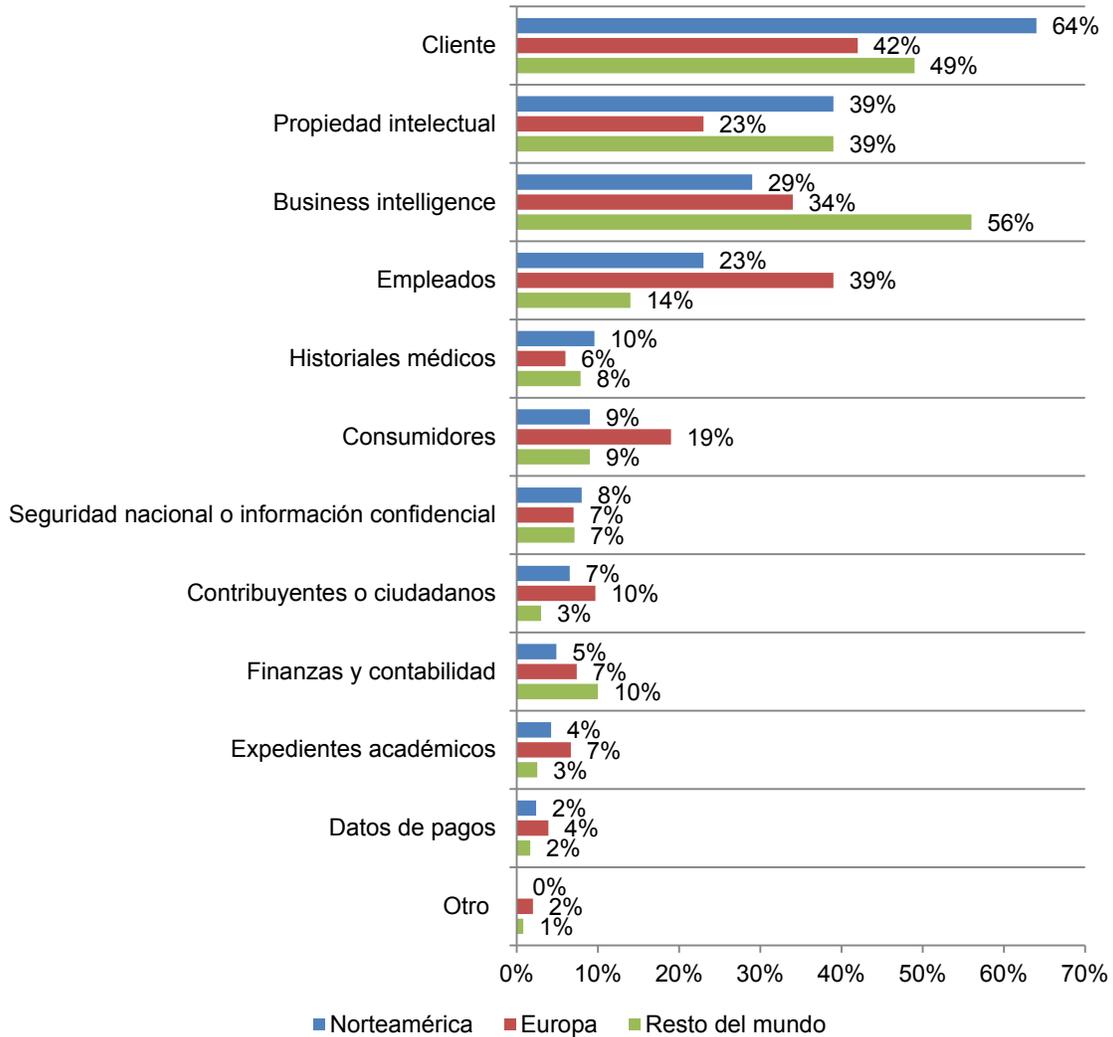
**Figura 16. ¿Sería capaz de detectar una filtración de datos?**

Se muestran los porcentajes de la respuesta "No"



**En Norteamérica, se considera que el mayor riesgo lo corren los datos de los clientes.** Como se constata en la figura 17, los encuestados de otros países (Resto del mundo) también confirman la vulnerabilidad de los datos de los clientes. Solo el 23% de los encuestados de Europa están inquietos por la propiedad intelectual. Resulta interesante destacar que el 56% de los encuestados de los demás países considera que el business intelligence corre el mayor riesgo.

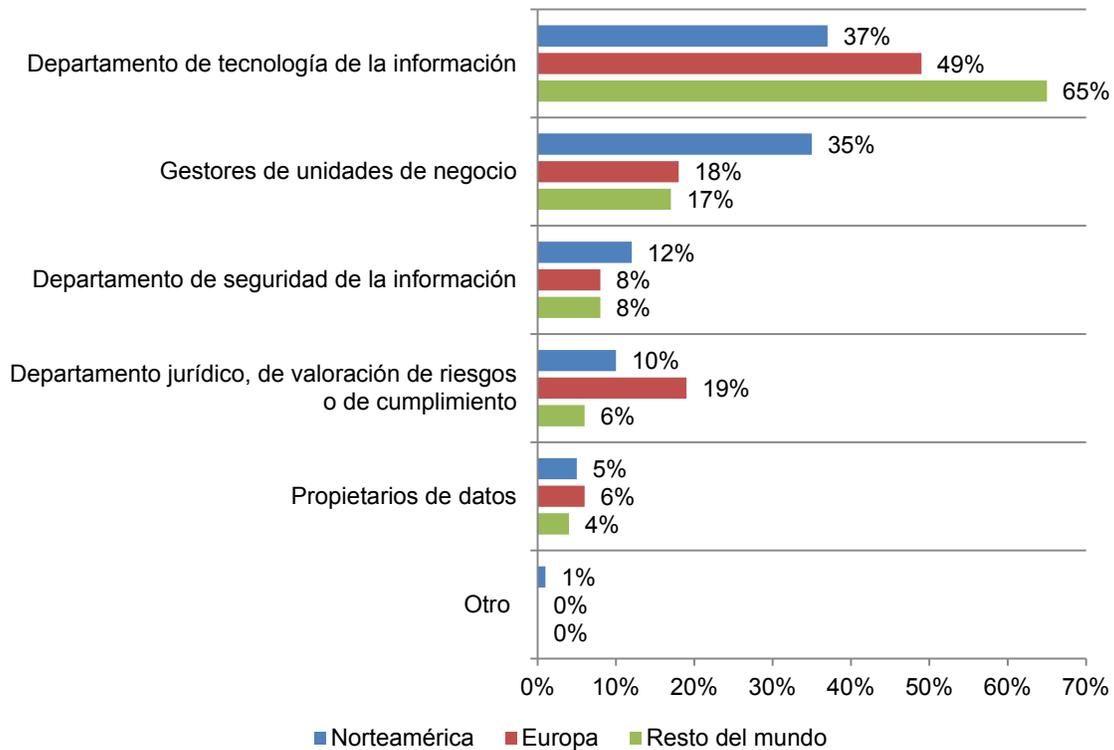
**Figura 17. Datos considerados de mayor riesgo en la organización**  
Se permiten dos respuestas



Salvo en Norteamérica, el departamento de tecnología de la información es el principal responsable de conceder a los usuarios acceso a los activos de datos. Aunque las organizaciones de Norteamérica tienden a repartir la responsabilidad entre el departamento de TI y los gestores de las unidades de negocio, la figura 18 demuestra que estos últimos ejercen menos influencia. A causa de la preocupación por el incumplimiento, son más los encuestados europeos que responden que la responsabilidad principal recae en el departamento jurídico, de valoración de riesgos o de cumplimiento.

**Figura 18. ¿Quién es el principal responsable de conceder a los usuarios acceso a los activos de datos?**

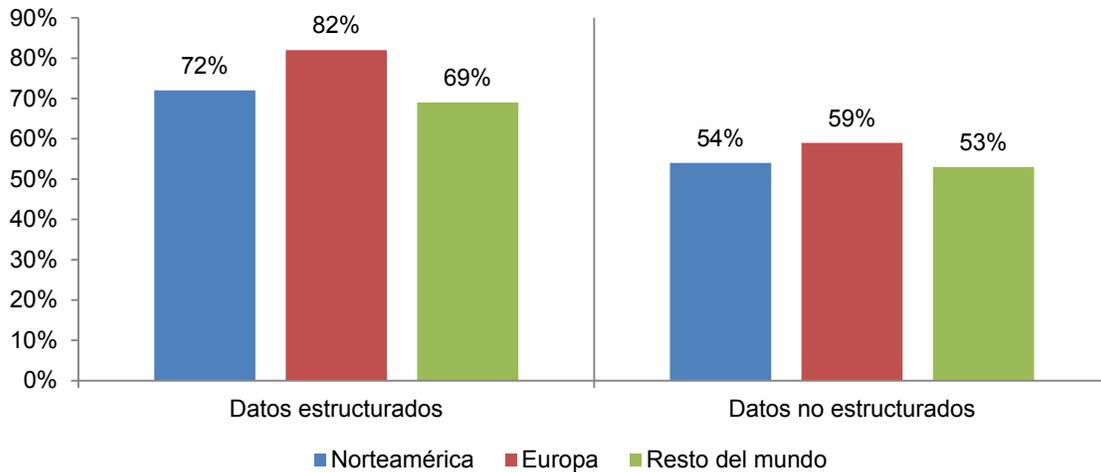
Se permiten dos respuestas



**La confianza en la visibilidad del acceso de los usuarios a la información sensible o confidencial varía según el país.** En la figura 19, se observa que, al parecer, las organizaciones europeas tienen más confianza en su capacidad para enterarse del acceso de los usuarios a los datos estructurados, confianza que se ve reducida en otros países. En ninguno de los países se expresa tanta confianza en la visibilidad del acceso de los usuarios a los datos no estructurados.

**Figura 19. ¿Cuánta confianza tiene en que su organización disponga de visibilidad del acceso de los usuarios a los datos confidenciales?**

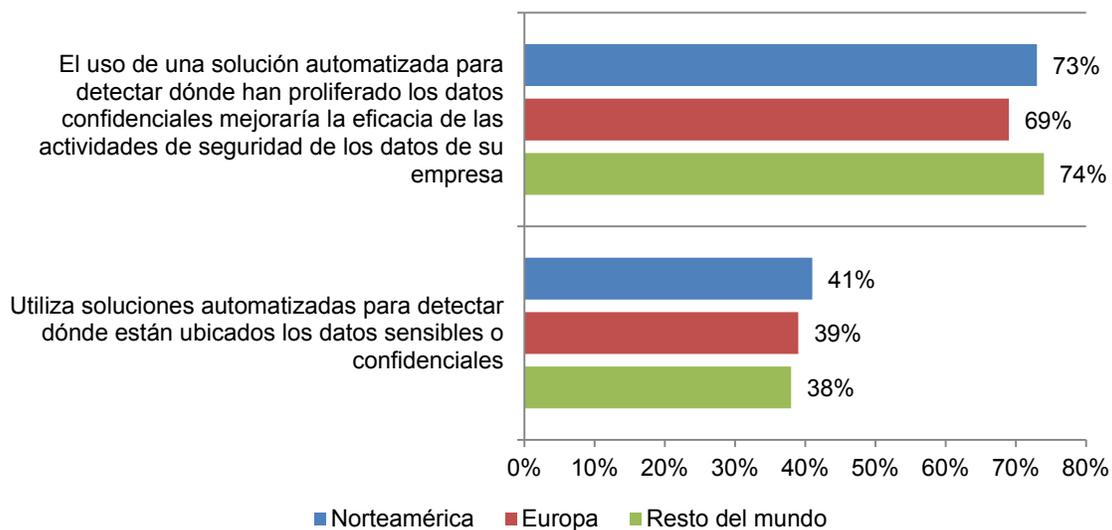
Están combinadas las respuestas “Mucha confianza” y “Confianza normal”



**Los países incluidos en el estudio muestran una actitud positiva hacia el uso de soluciones automatizadas para detectar dónde han proliferado los datos sensibles o confidenciales.** A pesar de que el uso de estas soluciones alcanza unas cotas bajas (el 41% de los encuestados en Norteamérica, el 39% en Europa y el 38% en Resto del mundo), la mayoría de los encuestados está convencida de su utilidad para conocer en qué lugar de la organización han proliferado los datos sensibles o confidenciales. La figura 20 muestra las diferencias entre los distintos países.

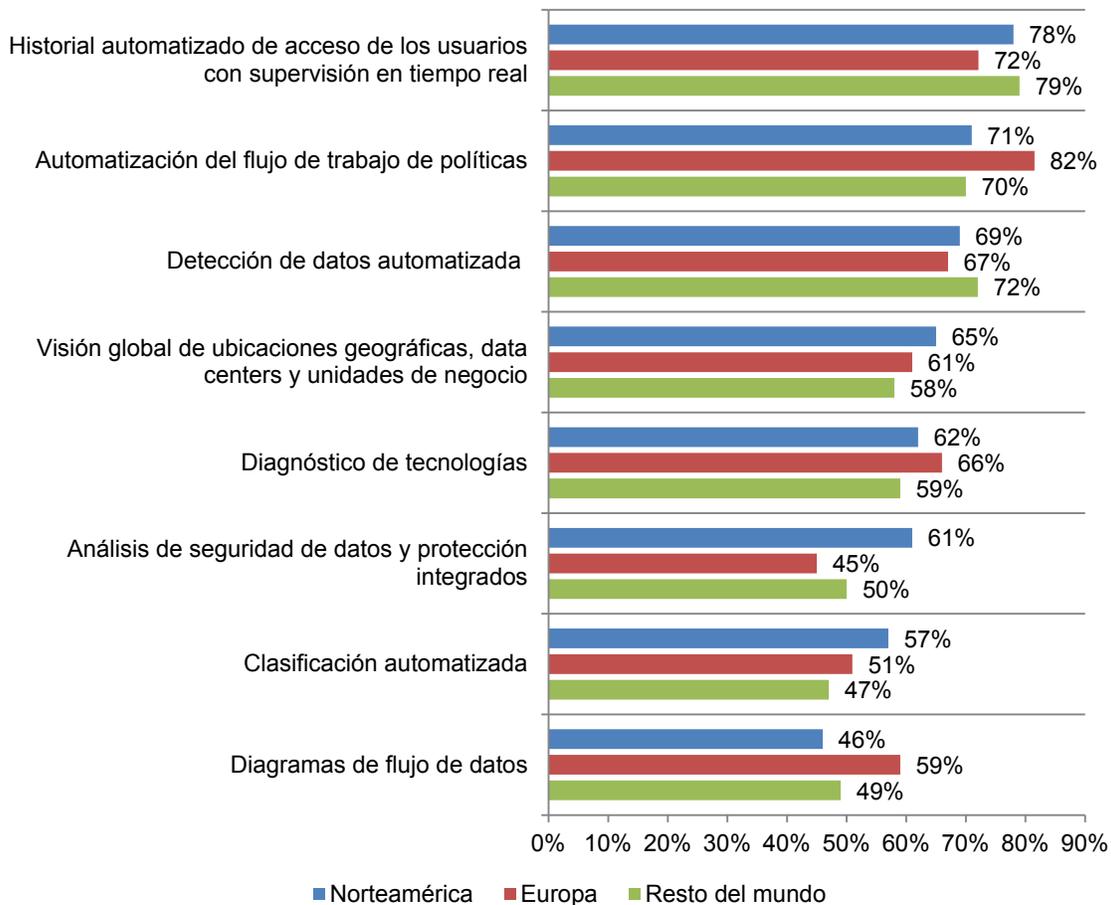
**Figura 20. Uso de soluciones automatizadas**

Se muestran los porcentajes de la respuesta “Sí”



Los países incluidos en el estudio comparten percepciones parecidas acerca de las funcionalidades más eficaces en cuanto a la seguridad centrada en los datos. La figura 21 revela que las tres funcionalidades más apreciadas son el historial de acceso de los usuarios automatizado con supervisión en tiempo real, la automatización del flujo de trabajo de políticas y la detección de datos automatizada.

**Figura 21. ¿Supondrían alguna mejora del cumplimiento y la protección de los datos estas ocho funcionalidades de seguridad centrada en los datos?**  
Están combinadas las respuestas "Mejora considerable" y "Mejora"



#### Parte 4. Métodos y limitaciones

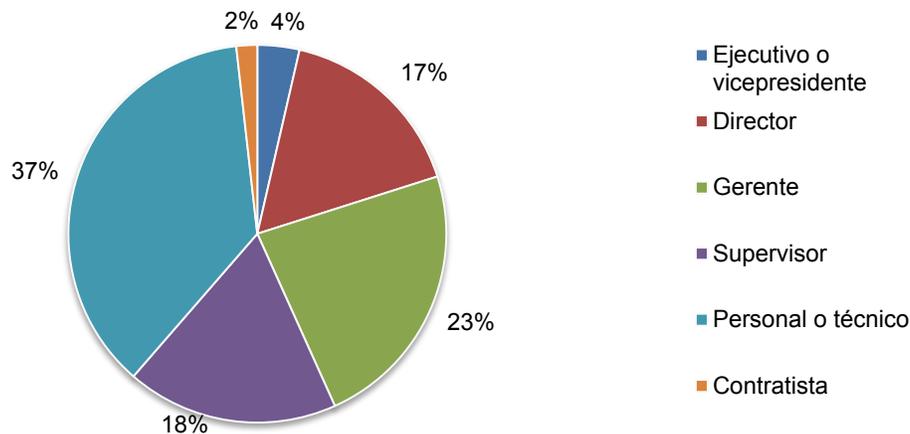
En la tabla 1, consta la respuesta de la muestra contrastada en Norteamérica, Europa y Resto del mundo. Se ha invitado a participar en este estudio mundial a un total de 45.829 profesionales de TI y de la seguridad de TI provenientes de 16 países. Han devuelto sus respuestas un total de 1.743 encuestados. En las pruebas de fiabilidad y filtrado, se han descartado 156 encuestas. La muestra final combinada ha sido de 1.587 encuestas, lo cual arroja un índice de respuesta del 3,5%.

<b>Tabla 1. Respuesta de muestra</b>	Número	Porcentaje
Marco de muestreo	45.829	100%
Total de devoluciones	1.743	3,8%
Encuestas rechazadas y escrutinadas	156	0,3%
Muestra definitiva	1.587	3,5%

En el gráfico de sectores 1, se representa el puesto de los encuestados en la organización participante. Por el propio diseño, el 61% de los encuestados pertenece al grado de supervisor u otro superior.

#### Gráfico de sectores 1. Puesto actual en la organización

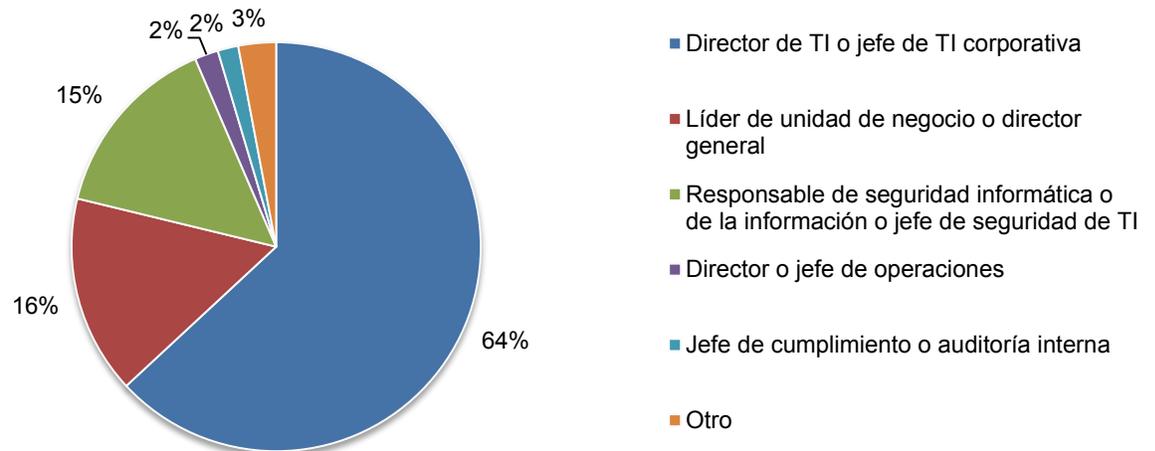
Vista contrastada



En el gráfico de sectores 2, se representa el canal de subordinación directa de los encuestados dentro de la organización. El 64% de los encuestados rinde cuentas directamente al director de TI o al jefe de TI corporativa.

### Gráfico de sectores 2. Canal de subordinación directa

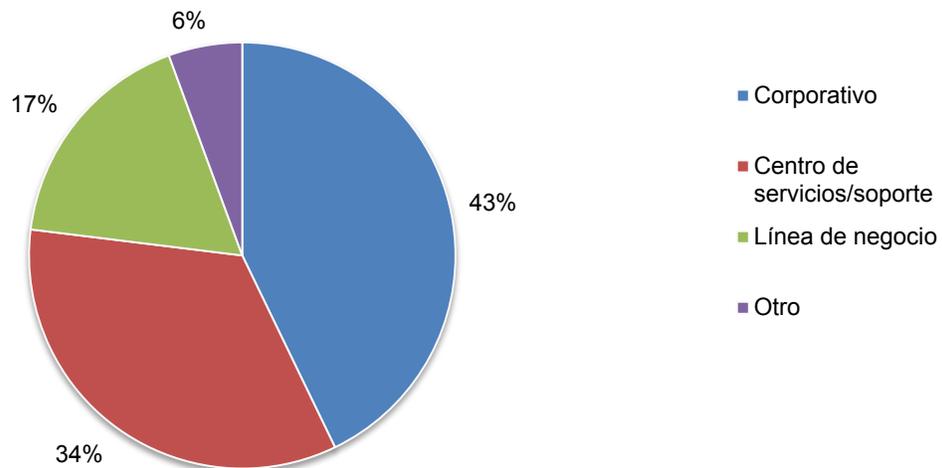
Vista contrastada



Tal y como se observa en el gráfico de sectores 3, el 43% de los encuestados identifica el ámbito de su trabajo o puesto como una función corporativa y el 34%, como una función de centro de servicios/soporte.

### Gráfico de sectores 3. Ámbito del trabajo o del puesto

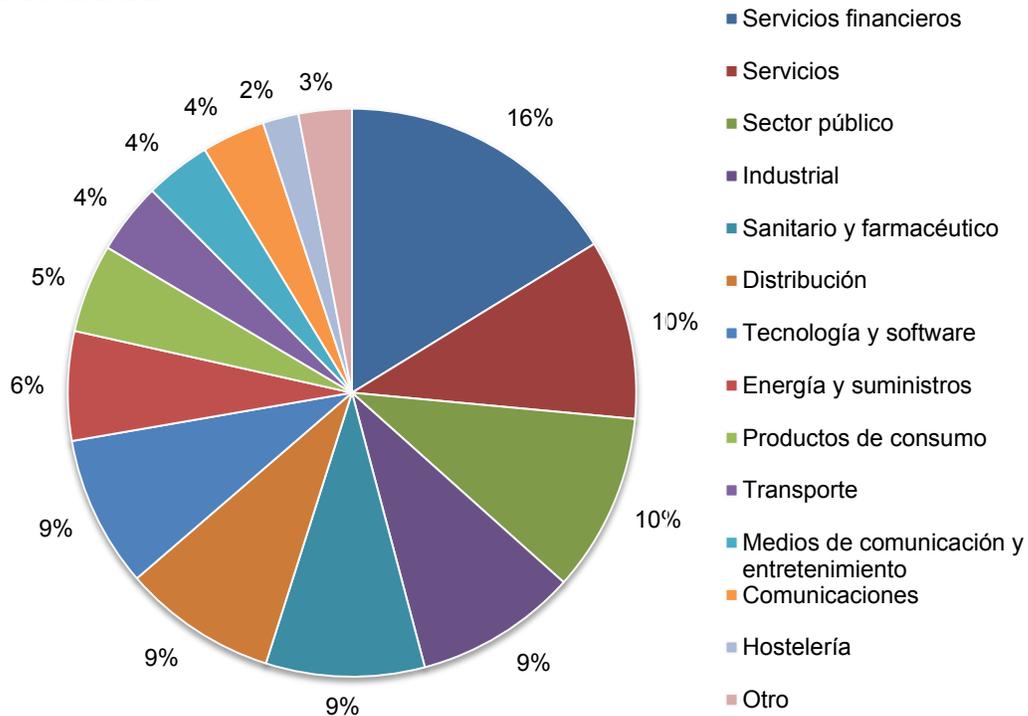
Vista contrastada



En el gráfico de sectores 4, se representa la clasificación de la organización de los encuestados por sectores. Se identifican los servicios financieros (16%) como el segmento más amplio, seguido por los servicios (10%) y el sector público (10%).

#### Gráfico de sectores 4. Clasificación por sector principal

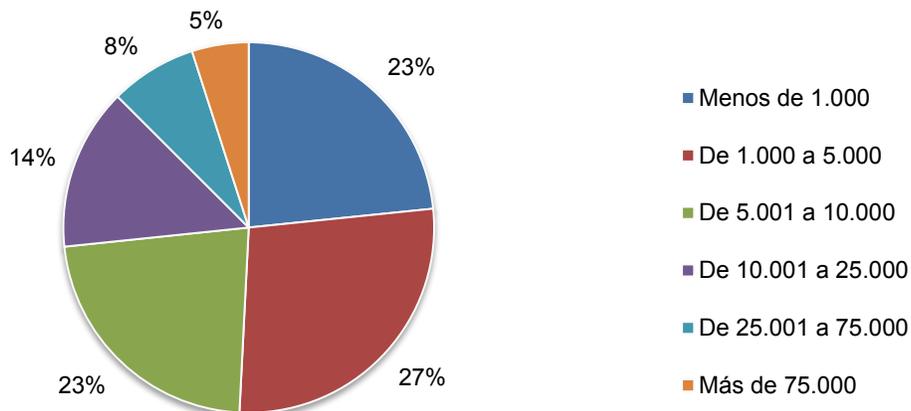
Vista contrastada



Tal y como se observa en el gráfico de sectores 5, el 50% de los encuestados procede de organizaciones con un cómputo global de 5.000 empleados o más.

#### Gráfico de sectores 5. Número de empleados a tiempo completo de toda la organización

Vista contrastada



## Parte 5. Avisos sobre el estudio

En toda encuesta, existen limitaciones inherentes que se deben someter a una escrupulosa consideración antes de inferir ninguna conclusión de los resultados obtenidos. Los elementos siguientes corresponden a limitaciones específicas y pertinentes a la mayoría de las encuestas realizadas por Internet.

- Margen de error de la ausencia de respuesta: las conclusiones proporcionadas se basan en una muestra de las encuestas devueltas. Hemos enviado el cuestionario a una muestra representativa de usuarios y el resultado ha sido un elevado número de respuestas devueltas útiles. Dada la falta de respuestas, siempre cabe la posibilidad de que las opiniones de quienes no hayan participado en la encuesta sean sustancialmente distintas de las de quienes sí lo han hecho.
- Margen de error del marco de muestreo: la precisión se basa en los datos de contacto y en la medida en que la lista es representativa de usuarios que son profesionales de TI o de la seguridad de TI. Además, reconocemos que puede haber cierta parcialidad en los resultados debido a eventos externos como la cobertura mediática. Por último, dado que la vía de recopilación ha sido Internet, es posible que se hubiesen obtenido resultados o patrones distintos si las respuestas se hubiesen proporcionado por otro medio como el teléfono o el correo postal.
- Resultados conforme a las opiniones manifestadas: la calidad del estudio se basa en la integridad de las respuestas confidenciales recibidas de los encuestados. Aunque se incorporen determinadas comprobaciones y compensaciones en el proceso, siempre cabe la posibilidad de que algún encuestado facilite respuestas carentes de precisión.

### Apéndice: resultados detallados de la encuesta

En las tablas siguientes, se indica el número o el porcentaje contrastado de respuestas a todas las preguntas del cuestionario incluido en el presente estudio. Todas las respuestas se han recibido en el mes de abril del año 2014.

Respuesta al cuestionario	Contrastadas
Marco de muestreo	45.829
Total de devoluciones	1.743
Encuestas rechazadas y escrutinadas	156
Muestra definitiva	1.587
Índice de respuesta	3,5%

#### Parte 1: sondeo

S1. ¿Se incluye, entre sus tareas, la protección de información de negocio sensible o confidencial?	Contrastadas
Sí	100%
No (no continúe)	0%
Total	100%

S2. ¿Qué definición se ajusta más a la función que desempeña?	Contrastadas
Tengo la responsabilidad de garantizar la protección de los datos en mi organización	18%
Tengo encomendadas todas las actividades de protección de los datos de mi organización	24%
Tengo encomendadas algunas de las actividades de protección de los datos de mi organización	32%
Participo en las actividades de protección de los datos de mi organización	26%
No tengo encomendada ninguna actividad ni participo en ninguna (no continúe)	0%
Total	100%

S3a. ¿Qué porcentaje de la función que desempeña guarda relación con la protección de los datos <b>estructurados</b> (por ejemplo, los datos que contienen las bases de datos)?	Contrastadas
0% (no continúe)	0%
Menos del 5%	6%
Del 5% al 10%	23%
Del 11% al 25%	33%
Del 26% al 50%	19%
Del 51% al 75%	14%
Del 76% al 100%	4%
Total	100%

S3b. ¿Qué porcentaje de la función que desempeña guarda relación con la protección de los datos <b>no estructurados</b> (por ejemplo, los datos de los archivos y los correos electrónicos)?	Contrastadas
0% (no continúe)	0%
Menos del 5%	9%
Del 5% al 10%	36%
Del 11% al 25%	31%
Del 26% al 50%	12%
Del 51% al 75%	6%
Del 76% al 100%	6%
Total	100%

**Parte 2: problemas**

P1. En lo que respecta a la situación de la seguridad de los datos en su organización, ¿qué le quita el sueño? Elija las tres opciones más apropiadas.	Contrastadas
Desconocimiento de la ubicación de los datos sensibles o confidenciales	57%
Piratas	23%
Empleados con intenciones aviesas	6%
Procesos de negocio interrumpidos	16%
Errores de empleados	10%
Errores de contratistas o trabajadores temporales	50%
Gestión de datos por parte de terceros o subcontratados (incluido el cloud)	42%
Incumplimiento de leyes o normativas	21%
Migración al ecosistema del cloud	24%
Migración a nuevas plataformas móviles	51%
Total	300%

P2a. ¿Sabe dónde están ubicados los <b>datos estructurados</b> sensibles o confidenciales de su organización (por ejemplo, los datos que contienen las bases de datos)? Tenga en cuenta los entornos de producción, prueba y soporte, y los data warehouses.	Contrastadas
Sí, todos los datos	16%
Sí, la mayoría de los datos	22%
Sí, algunos datos	38%
No	24%
Total	100%

P2b. Si su respuesta es no, ¿de qué porcentaje de los <b>datos estructurados</b> sensibles o confidenciales de su organización <b>no conoce</b> la ubicación? Ofrezca una respuesta aproximada.	Contrastadas
0%	0%
Menos del 5%	6%
Del 5% al 10%	24%
Del 11% al 25%	28%
Del 26% al 50%	29%
Del 51% al 75%	10%
Del 76% al 100%	3%
Total	100%

P3a. ¿Sabe dónde están ubicados los <b>datos no estructurados</b> sensibles o confidenciales de su organización (por ejemplo, los datos que contienen los archivos y los correos electrónicos)?	Contrastadas
Sí, todos los datos	7%
Sí, la mayoría de los datos	10%
Sí, algunos datos	42%
No	41%
Total	100%

P3b. Si su respuesta es no, ¿de qué porcentaje de los <b>datos no estructurados</b> sensibles o confidenciales de su organización <b>no conoce</b> la ubicación? Ofrezca una respuesta aproximada.	Contrastadas
0%	0%
Menos del 5%	3%
Del 5% al 10%	8%
Del 11% al 25%	16%
Del 26% al 50%	25%
Del 51% al 75%	27%
Del 76% al 100%	21%
Total	100%

P4a. Si se produjera una filtración de <b>datos estructurados</b> en su organización, ¿sería capaz de detectarla?	Contrastadas
Sí, siempre	26%
Sí, casi siempre	34%
Sí, algunas veces	29%
No	11%
Total	100%

P4b. Si se produjera una filtración de <b>datos no estructurados</b> en su organización, ¿sería capaz de detectarla?	Contrastadas
Sí, siempre	12%
Sí, casi siempre	22%
Sí, algunas veces	33%
No	33%
Total	100%

<b>Afirmaciones:</b> indique su opinión con respecto a cada elemento usando la escala facilitada debajo de cada afirmación sobre los datos sensibles o confidenciales. Están combinadas las respuestas “De acuerdo” y “Totalmente de acuerdo”.	Contrastadas
P5a. Ignorar la ubicación de la información sensible o confidencial de mi organización representa un elevado riesgo para la seguridad.	79%
P5b. En mi organización, la protección de los datos es una de las máximas prioridades.	51%
P5c. En mi organización, apenas existe riesgo de que los empleados, los empleados temporales o los contratistas tengan un acceso <b>excesivo</b> a los datos.	23%
P5d. En mi organización, el acceso a los datos sensibles se controla según la función, la ubicación u otros factores.	42%

P6. En cuanto a robo o pérdida de datos se refiere, ¿qué tipos de datos considera que corren mayor riesgo en su organización? Elija las dos opciones más apropiadas.	Contrastadas
Cliente	53%
Propiedad intelectual	34%
Business intelligence	38%
Empleados	25%
Historiales médicos	8%
Consumidores	12%
Seguridad nacional o información confidencial	7%
Contribuyentes o ciudadanos	6%
Finanzas y contabilidad	7%
Expedientes académicos	4%
Datos de pagos (por ejemplo, número de tarjeta)	3%
Otro (especifique)	1%
Total	200%

P7. ¿Qué porcentaje de datos de su organización se considera sensible o confidencial (incluidas todas las fuentes, estructuradas y no estructuradas)?	Contrastadas
Menos del 5%	3%
Del 5% al 10%	21%
Del 11% al 25%	36%
Del 26% al 50%	13%
Del 51% al 75%	10%
Del 76% al 100%	17%
Total	100%

P8. ¿Quién es el principal responsable de conceder a los usuarios acceso a los activos de datos? Marque solo dos respuestas.	Contrastadas
Departamento de tecnología de la información	49%
Departamento de seguridad de la información	10%
Departamento jurídico, de valoración de riesgos o de cumplimiento	12%
Gestores de unidades de negocio	25%
Propietarios de datos	5%
Otro (especifique)	0%
Total	100%

P9a. ¿Qué tecnologías o “herramientas” tiene implantadas su organización para el uso seguro de activos de <b>datos estructurados</b> sensibles o confidenciales?	Contrastadas
Supervisión de actividad de base de datos	47%
Clasificación de datos como sensibles	68%
Cifrado de base de datos	47%
Tokenización transparente de campos sensibles	20%
Enmascaramiento persistente de campos sensibles en entornos de no producción	25%
Enmascaramiento dinámico de campos sensibles en entornos de producción	13%
Controles de acceso a las aplicaciones	62%
Control centralizado de acceso a los datos de bases de datos y aplicaciones empresariales	42%

P9b. ¿Qué tecnologías o herramientas tiene implantadas su organización para el uso seguro de activos de <b>datos no estructurados</b> sensibles o confidenciales? Marque todas las opciones aplicables.	Contrastadas
Prevención de pérdida de datos	29%
Clasificación de datos como sensibles	54%
Gestión de acceso e identidades	31%
Gestión de derechos digitales	29%
Derechos y gestión de control del acceso centralizados	19%
Auditorías de acceso y sistemas de archivos	14%
Gestión de información de seguridad	40%

P10a. ¿Cuánta confianza tiene en que su organización disponga de visibilidad del acceso de los usuarios a los <b>datos estructurados</b> sensibles o confidenciales?	Contrastadas
Mucha confianza	34%
Confianza normal	40%
Poca confianza	26%
Total	100%

P10b. ¿Cuánta confianza tiene en que su organización disponga de visibilidad del acceso de los usuarios a los <b>datos no estructurados</b> sensibles o confidenciales?	Contrastadas
Mucha confianza	21%
Confianza normal	34%
Poca confianza	45%
Total	100%

P11. ¿Cuánta eficacia tiene la gobernanza de su organización en lo que respecta a los usos aceptables de los activos de datos basándose en los procedimientos relacionados a continuación? Califíquela en una escala del 1 al 5 de “Es excelente” a “No se cumple”.	
<b>Procedimientos de seguridad de los datos [BASES DE DATOS]</b>	Contrastadas
Saber dónde están ubicados los datos sensibles o confidenciales y realizar su seguimiento	45%
Construir la arquitectura de datos (incluidos mapas, linaje, flujos e inventarios)	50%
Gestionar la clasificación de los datos mediante la priorización	40%
Supervisar los derechos de acceso según el trabajo, la función o la necesidad	48%
Gestionar los cambios en el acceso en función de las modificaciones de la política, las necesidades del usuario o la actualización de aplicaciones	53%
Revocar los derechos de acceso a los datos tras el cese del empleado o la modificación de la política	51%
Implementar políticas de acceso a los datos de forma sistemática a aplicaciones, ubicaciones, departamentos, estándares tecnológicos, etc.	59%
Supervisar el acceso a los datos estructurados y no estructurados de los usuarios con privilegios	49%
Supervisar la separación de tareas	27%
Proporcionar pruebas del cumplimiento de las políticas y las normativas	35%
Crear políticas de uso aceptables	30%
Supervisar las transferencias de datos entre el entorno local y ubicaciones de terceros (incluido el cloud)	61%
Formar a los usuarios finales sobre el acceso a los datos y las políticas de control	47%
Detectar y contener el robo y la pérdida de datos (filtraciones de datos)	45%
Implementar una solución de prevención de pérdida de datos	45%
Proteger los datos sensibles mediante el cifrado o la tokenización	42%
Proteger los datos sensibles con enmascaramiento, disociación, censura o supresión	56%
Utilizar una funcionalidad de análisis forense digital exhaustivo	65%

<b>Procedimientos de seguridad de los datos [CORREOS ELECTRÓNICOS]</b>	Contrastadas
Saber dónde están ubicados los datos sensibles o confidenciales y realizar su seguimiento	56%
Construir la arquitectura de datos (incluidos mapas, linaje, flujos e inventarios)	56%
Gestionar la clasificación de los datos mediante la priorización	44%
Supervisar los derechos de acceso según el trabajo, la función o la necesidad	59%
Gestionar los cambios en el acceso en función de las modificaciones de la política, las necesidades del usuario o la actualización de aplicaciones	57%
Revocar los derechos de acceso a los datos tras el cese del empleado o la modificación de la política	59%
Implementar políticas de acceso a los datos de forma sistemática a aplicaciones, ubicaciones, departamentos, estándares tecnológicos, etc.	62%
Supervisar el acceso a los datos estructurados y no estructurados de los usuarios con privilegios	60%
Supervisar la separación de tareas	40%
Proporcionar pruebas del cumplimiento de las políticas y las normativas	44%
Crear políticas de uso aceptables	33%
Supervisar las transferencias de datos entre el entorno local y ubicaciones de terceros (incluido el cloud)	38%
Formar a los usuarios finales sobre el acceso a los datos y las políticas de control	55%
Detectar y contener el robo y la pérdida de datos (filtraciones de datos)	63%
Implementar una solución de prevención de pérdida de datos	45%
Proteger los datos sensibles mediante el cifrado o la tokenización	49%
Proteger los datos sensibles con enmascaramiento, disociación, censura o supresión	68%
Utilizar una funcionalidad de análisis forense digital exhaustivo	69%

<b>Procedimientos de seguridad de los datos [ARCHIVO]</b>	<b>Contrastadas</b>
Saber dónde están ubicados los datos sensibles o confidenciales y realizar su seguimiento	51%
Construir la arquitectura de datos (incluidos mapas, linaje, flujos e inventarios)	58%
Gestionar la clasificación de los datos mediante la priorización	49%
Supervisar los derechos de acceso según el trabajo, la función o la necesidad	63%
Gestionar los cambios en el acceso en función de las modificaciones de la política, las necesidades del usuario o la actualización de aplicaciones	63%
Revocar los derechos de acceso a los datos tras el cese del empleado o la modificación de la política	64%
Implementar políticas de acceso a los datos de forma sistemática a aplicaciones, ubicaciones, departamentos, estándares tecnológicos, etc.	67%
Supervisar el acceso a los datos estructurados y no estructurados de los usuarios con privilegios	63%
Supervisar la separación de tareas	42%
Proporcionar pruebas del cumplimiento de las políticas y las normativas	43%
Crear políticas de uso aceptables	40%
Supervisar las transferencias de datos entre el entorno local y ubicaciones de terceros (incluido el cloud)	72%
Formar a los usuarios finales sobre el acceso a los datos y las políticas de control	58%
Detectar y contener el robo y la pérdida de datos (filtraciones de datos)	56%
Implementar una solución de prevención de pérdida de datos	62%
Proteger los datos sensibles mediante el cifrado o la tokenización	48%
Proteger los datos sensibles con enmascaramiento, disociación, censura o supresión	64%
Utilizar una funcionalidad de análisis forense digital exhaustivo	68%

<b>P12a. En la actualidad, ¿usa su organización alguna solución automatizada para detectar dónde están ubicados los datos sensibles o confidenciales?</b>	<b>Contrastadas</b>
Sí	40%
No	60%
Total	100%

<b>P12b. En caso afirmativo, ¿dispone de alguna solución automatizada para detectar dónde se hallan los datos sensibles o confidenciales en las bases de datos y las aplicaciones empresariales?</b>	<b>Contrastadas</b>
Sí	64%
No	36%
Total	100%

<b>P12c. En caso afirmativo, ¿dispone de alguna solución automatizada para detectar dónde se hallan los datos sensibles o confidenciales en los archivos y los correos electrónicos?</b>	<b>Contrastadas</b>
Sí	22%
No	78%
Total	100%

<b>P12d. Si no lo hace, ¿cree que el uso de una solución automatizada para detectar la ubicación de los datos sensibles o confidenciales mejoraría la eficacia de las actividades de seguridad de los datos?</b>	<b>Contrastadas</b>
Sí	78%
No	22%
Total	100%

P12e. ¿Cree que el uso de una solución automatizada para detectar dónde han proliferado los datos sensibles o confidenciales mejoraría la eficacia de las actividades de seguridad de los datos de su empresa?	Contrastadas
Sí	72%
No	28%
Total	100%

P13a. ¿Ha sido víctima su organización de alguna filtración de datos en los 12 últimos meses?	Contrastadas
Sí, solo un incidente	27%
Sí, entre dos y cinco incidentes	18%
Sí, más de cinco incidentes	4%
No (pase a P14)	51%
Total	100%

P13b. Están combinadas las respuestas “Probablemente” y “Muy probablemente”	Contrastadas
P13b-1. Si su respuesta ha sido afirmativa, ¿cree que se habría evitado el incidente si su organización hubiese tenido implantadas <b>tecnologías de seguridad de datos</b> más eficaces?	58%
P13b-2. Si su respuesta ha sido afirmativa, ¿cree que se habría evitado el incidente si su organización hubiese asignado un <b>presupuesto</b> o un nivel de <b>gasto</b> mayor?	46%
P13b-3. Si su respuesta ha sido afirmativa, ¿cree que se habría evitado el incidente si su organización hubiese contado con <b>personal</b> con más conocimientos sobre responsabilidad en materia de seguridad de datos?	57%
P13b-4. Si su respuesta ha sido afirmativa, ¿cree que se habría evitado el incidente si su organización hubiese tenido implantados más controles o <b>procesos automatizados</b> ?	54%

P14. Si dispusiera de las funcionalidades siguientes, ¿cree que mejoraría la posición de la organización en cuanto al cumplimiento y la protección de los datos se refiere? Ofrezca una respuesta para cada funcionalidad empleando la escala que aparece debajo de cada una. Están combinadas las respuestas “Mejora considerable” y “Mejora”.	Contrastadas
P14a. Detección de datos automatizada	69%
P14b. Clasificación automatizada	52%
P14c. Historial automatizado de acceso de los usuarios con supervisión en tiempo real	76%
P14d. Visión global de ubicaciones geográficas, data centers y unidades de negocio	62%
P14e. Diagramas de flujo de datos	51%
P14f. Diagnóstico de tecnologías (incluidas herramientas de evaluación de la vulnerabilidad)	62%
P14g. Análisis de seguridad de datos y protección integrados	53%
P14h. Automatización del flujo de trabajo de políticas	74%

<b>Parte 3. Características de la muestra</b>	
D1. ¿Qué descripción se ajusta más a su puesto en la organización?	Contrastadas
Ejecutivo o vicepresidente	4%
Director	17%
Gerente	23%
Supervisor	18%
Personal o técnico	37%
Contratista	2%
Otro (especifique)	0%
Total	100%

D2. ¿Qué descripción se ajusta más a su canal de subordinación directa?	Contrastadas
Director ejecutivo o comité ejecutivo	1%
Director o jefe de operaciones	2%
Director de finanzas, interventor o jefe financiero	1%
Director de TI o jefe de TI corporativa	64%
Líder de unidad de negocio o director general	16%
Jefe de cumplimiento o auditoría interna	2%
Responsable de seguridad informática o de la información o jefe de seguridad de TI	15%
Director de privacidad o jefe de privacidad corporativa	1%
Otro (especifique)	0%
Total	100%

D3. ¿Qué descripción se ajusta más al alcance geográfico de su trabajo o su puesto?	Contrastadas
Global	48%
Regional	38%
Local	14%
Total	100%

D4. ¿Qué descripción se ajusta más al ámbito de su trabajo o su puesto?	Contrastadas
Corporativo	43%
Línea de negocio	17%
Soporte o asistencia al cliente	34%
Otro (especifique)	6%
Total	100%

D6. ¿Qué descripción se ajusta más a la clasificación de la organización según el sector?	Contrastadas
Agricultura y servicios alimentarios	1%
Comunicaciones	4%
Productos de consumo	5%
Defensa y aeroespacial	0%
Educación e investigación	1%
Energía y suministros	6%
Medios de comunicación y entretenimiento	4%
Servicios financieros	16%
Sanitario y farmacéutico	9%
Hostelería	2%
Industrial	9%
Sector público	10%
Distribución	9%
Servicios	10%
Tecnología y software	9%
Transporte	4%
Otro (especifique)	1%
Total	100%

D5. ¿Qué intervalo se ajusta más al número de empleados a tiempo completo de toda la organización?	Contrastadas
Menos de 1.000	23%
De 1.000 a 5.000	27%
De 5.001 a 10.000	23%
De 10.001 a 25.000	14%
De 25.001 a 75.000	8%
Más de 75.000	5%
Total	100%

Países

D6. ¿Dónde se encuentra (lista de países)?	Contrastadas
Argentina	67
Australia	89
Brasil	54
Canadá	142
Francia	45
Alemania	165
Hong Kong	39
Italia	55
Japón	82
México	55
Países Bajos	71
Singapur	26
Corea del Sur	41
España	46
Reino Unido	109
Estados Unidos	501
Total	1.587

### Ponemon Institute

*Anticipamos la gestión responsable de la información*

Ponemon Institute se dedica a llevar a cabo estudios independientes e impartir formación que anticipa las prácticas de gestión responsable de la información y la privacidad en las empresas y en los organismos oficiales. Nuestra misión consiste en elaborar estudios empíricos de máxima calidad acerca de cuestiones fundamentales que afectan a la gestión y la seguridad de la información sensible sobre personas físicas y jurídicas.

Como miembros de **Council of American Survey Research Organizations (CASRO)**, mantenemos la confidencialidad de los datos, la privacidad y los estándares éticos de investigación más estrictos. No recopilamos ningún dato que permita identificar a ninguna persona (ni a ninguna empresa en el caso de los estudios comerciales). Es más, tenemos estrictos estándares de calidad para garantizar que no se formulen preguntas superfluas, improcedentes ni inapropiadas.