Cómo maximizar el valor de sus inversiones en privacidad de datos

Privacidad de datos
Reporte de referencia

CISCO

Resumen

El Reglamento General de Protección de Datos (GDPR) de la UE entró en vigor el 25 de mayo de 2018, y en todo el mundo los códigos y las leyes referentes a la privacidad siguen evolucionando y expandiéndose.

Los clientes ahora hacen más preguntas durante el ciclo de compra sobre cómo se capturan, utilizan, transfieren, comparten, almacenan y destruyen sus datos.

La mayoría de las organizaciones han invertido –y siguen haciéndolo– en las personas, los procesos, la tecnología y las políticas necesarias para cumplir con los requerimientos de privacidad de sus clientes, y para evitar multas y otras penalizaciones cuantiosas. Además, las filtraciones de datos dejan al descubierto la información personal de millones de personas, y a las organizaciones les preocupan los productos que compran, los servicios que utilizan, las personas que emplean, y en general con quiénes se asocian y hacen negocios. Por consecuencia, los clientes ahora hacen más preguntas durante el ciclo de compra sobre cómo se capturan, utilizan, transfieren, comparten, almacenan y destruyen sus datos. En el estudio del año pasado (Estudio Comparativo sobre el Estado de Madurez de la Privacidad 2018 de Cisco), Cisco presentó por primera vez datos e ideas referentes a cómo estas preocupaciones sobre la seguridad afectan de manera negativa los tiempos y el ciclo de compra. La investigación de este año presenta una actualización de esos hallazgos y explora los beneficios de invertir en la privacidad.

El Reporte de Referencia de Privacidad de Datos utiliza los datos del Estudio Comparativo Anual de Ciberseguridad, una encuesta de doble ciego que se aplica a más de 3,200 profesionales de la seguridad de las industrias más importantes y de distintas regiones geográficas en un total de 18 países. Muchas de las preguntas específicas sobre la privacidad se hicieron directamente a los más de 2,900 encuestados que estaban familiarizados con los procesos de privacidad de sus organizaciones. Se preguntó a los participantes sobre el grado de preparación para el GDPR, sobre cualquier retraso en el ciclo de venta debido a las inquietudes de los clientes referentes a la privacidad, sobre pérdidas imputables a filtraciones de datos, y sobre las prácticas actuales para maximizar el valor de sus datos.

Los hallazgos de este estudio proporcionan una evidencia sólida de que las organizaciones reciben beneficios adicionales al cumplimiento por sus inversiones en privacidad. Las organizaciones que ya están listas para el GDPR sufren de menos retrasos en su ciclo de venta debido a preocupaciones de privacidad de datos por parte de sus clientes que las que no están listas para el GDPR. Las organizaciones que ya están listas para el GDPR también han sufrido menos filtraciones de datos y, cuando estas han ocurrido, un menor número de registros se han visto afectados, por lo que se redujo el tiempo de inactividad del sistema. Por lo tanto, el costo total de las filtraciones de datos fue menor que el que enfrentaron las organizaciones que no estaban listas para el GDPR. Aunque las compañías han enfocado sus esfuerzos en cumplir con los requerimientos y las regulaciones de privacidad, casi todas las compañías aseveran que están viendo otros beneficios empresariales debido a estas inversiones, además del cumplimiento. Estos beneficios asociados con la privacidad proporcionan a las organizaciones ventajas competitivas, y este estudio puede servirles como una guía para tomar las decisiones de inversión dirigidas a consolidar sus procesos de privacidad.

> **“La privacidad es un componente esencial para el éxito de la organización, tanto para proteger los datos como para fomentar la innovación”.**
>
> **John N. Stewart, Vicepresidente Senior y Gerente General de Seguridad y Confianza, Cisco**

> **“Esta investigación arroja evidencia sobre algo que los profesionales de la Privacidad han sabido desde hace mucho: que las organizaciones reciben beneficios adicionales al cumplimiento gracias a sus inversiones en privacidad. El estudio de Cisco demuestra que un cumplimiento estricto con respecto a la privacidad acorta la duración del ciclo de venta y aumenta la confianza de los clientes ”.**
>
> **Peter Lefkowitz, Gerente General de Riesgo Digital,**
> **Citrix Systems, y Presidente del Concejo 2018**
> **de la Asociación Internacional de Profesionales de la Privacidad (IAPP)**

Los resultados

Nivel de preparación para el GDPR

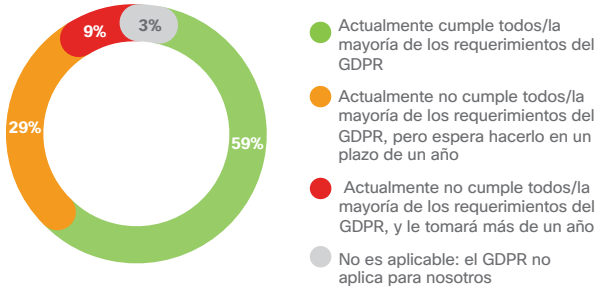
De los encuestados del Reporte de referencia de Privacidad de Datos, el 59% respondió que cumple con todos o casi todos los requerimientos actuales del GDPR (ver Figura 1). El 29% dijo que espera estar completamente preparado para el GDPR en un plazo de un año, y el 9% restante dijo que la preparación le tomaría más de un año. Llama la atención que, aunque el GDPR es aplicable para los negocios ubicados en la UE o para el procesamiento de los datos personales recopilados de personas ubicadas en la UE, solo el 3% de los encuestados de todo el mundo indicó que no creía que el GDPR fuera aplicable para su organización.

El nivel de preparación para el GDPR por país varió del 42% al 76% (ver Figura 2). Los países europeos que participaron en la encuesta (España, Italia, Reino Unido, Francia, Alemania) se encuentran, como era de esperarse, en el rango más alto.

Solo el 3% de los encuestados de todo el mundo indicó que no creía que el GDPR fuera aplicable para su organización.

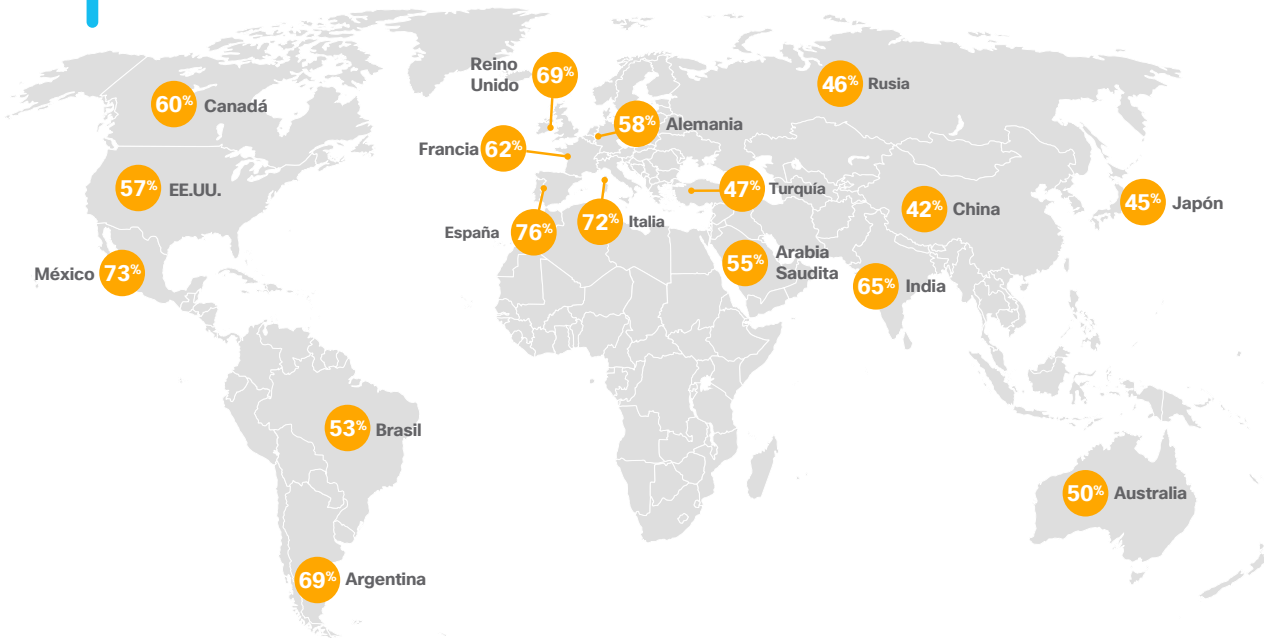
59% de las compañías reportó cumplir con todos o casi todos los requerimientos actuales del GDPR, y otro 29% espera hacer lo mismo en un plazo de un año. Los máximos desafíos identificados para la preparación para el GDPR son: la seguridad de los datos, la capacitación de los empleados, y estar al día con los cambios constantes en los reglamentos.

Figura 1 Nivel de preparación para el GDPR
Porcentaje de encuestados, N=3,206



Fuente: Reporte de referencia de Privacidad de Datos 2019 de Cisco, n=3,206

Figura 2 Nivel de preparación para el GDPR por país
Porcentaje de encuestados, N=3,206



Fuente: Reporte de referencia de Privacidad de Datos 2019 de Cisco

Se pidió a los encuestados que identificaran los desafíos más importantes que sus organizaciones enfrentan al prepararse para el GDPR. Las principales respuestas fueron la seguridad de datos, la capacitación interna, los cambios constantes de los reglamentos y los requerimientos de Privacidad por defecto (ver Figura 3).

Figura 3 Desafíos más importantes en la preparación para el GDPR Porcentaje de encuestados, N=3,098

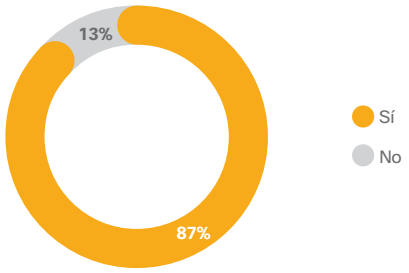
42%	Cumplir con los requerimientos de seguridad de datos
39%	Capacitación interna
35%	Estar al día con los cambios constantes conforme el reglamento avanza
34%	Cumplir con los requerimientos de la Privacidad por defecto
34%	Cumplir con las solicitudes de los titulares para acceder a sus datos
31%	Catalogar e inventariar los datos
30%	Habilitar las solicitudes para borrar datos
29%	Contratar/identificar a los encargados de la protección de datos en cada área geográfica relevante
28%	Manejo de proveedores

Fuente: Reporte de referencia de Privacidad de Datos 2019 de Cisco

Retrasos en ventas debido a cuestiones de privacidad

Se preguntó a los encuestados si sufrían de retrasos en sus ciclos de venta debido a preocupaciones relacionadas con la privacidad de los datos por parte de sus clientes. El 87% de los encuestados respondió que tiene retrasos en ventas, ya sea para sus clientes actuales o para los prospectos (ver Figura 4). Este porcentaje es significativamente mayor al 66% de los encuestados que reportó retrasos en la encuesta del año pasado, y probablemente es consecuencia de una mayor conciencia sobre la importancia de la privacidad de los datos, a que el GDPR entró en vigor, y a que surgieron nuevos requerimientos y leyes de privacidad. La privacidad de los datos se ha convertido en un asunto de máxima prioridad a nivel gerencial para muchas organizaciones, y los clientes se están asegurando de que sus proveedores y asociados tengan respuestas acertadas a sus preocupaciones de seguridad antes de iniciar cualquier negocio con ellos.

Figura 4 Encuestados que sufren de retrasos en sus ciclos de venta debido a preocupaciones sobre la privacidad de los datos por parte de los clientes Porcentaje de encuestados, N=2,064



Fuente: Reporte de referencia de Privacidad de Datos 2019 de Cisco

Con respecto a la duración de los retrasos, las estimaciones variaron ampliamente. El retraso promedio de ventas para los clientes actuales fue de 3.9 semanas, y más del 94% de las organizaciones reportaron retrasos de entre 0 y 10 semanas. Sin embargo, hubo algunas organizaciones que reportaron retrasos de hasta 25 a 50 semanas, o más (ver Figura 5). Es de notar que el retraso promedio de ventas para prospectos fue de 4.7 semanas, quizá a consecuencia del mayor tiempo necesario para abordar de manera adecuada las preocupaciones de privacidad en una posible nueva relación con un cliente.

Los retrasos en ventas debido a preocupaciones sobre la privacidad de los datos por parte de los clientes siguen siendo un problema para la mayoría de las organizaciones.

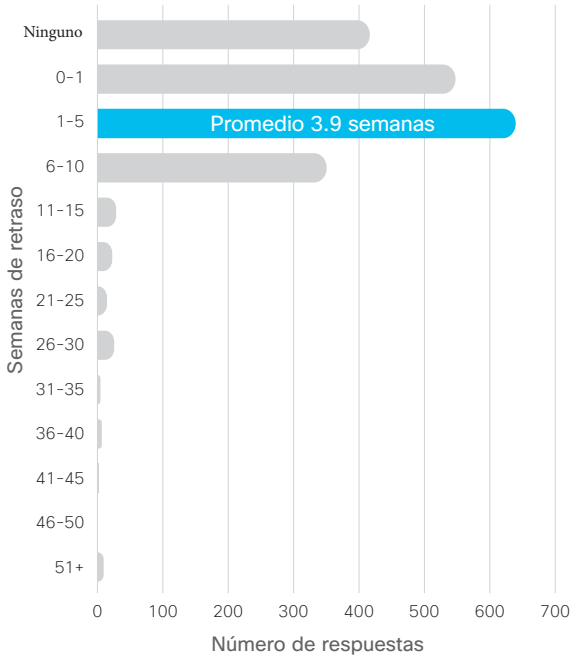
El 87% reportó que tienen retrasos de ventas con clientes actuales o prospectos, lo cual representa un aumento significativo con respecto al año pasado.

Principales causas para los retrasos de ventas relacionados con cuestiones de privacidad:

- *Investigar las solicitudes específicas de los clientes*
- *Traducir la información de privacidad al idioma del cliente*
- *Instruir al cliente sobre los procesos o prácticas de privacidad de la compañía*
- *Tener que rediseñar el producto para que cumpla con los requerimientos de privacidad del cliente*

Estos retrasos promedio tanto para clientes actuales como para prospectos son significativamente menores al promedio de 7.8 semanas reportado en la encuesta del año pasado, quizá debido a que las compañías se han equipado mejor durante este último año para responder a las preocupaciones de privacidad de los clientes.

Figura 5 Retrasos en la respuesta a las preocupaciones sobre la privacidad de los datos por parte de los clientes Porcentaje de encuestados, N=2,081



Fuente: Reporte de referencia de Privacidad de Datos 2019 de Cisco

La duración de los retrasos de ventas para clientes actuales, por país, varió entre 2.2 y 5.5 semanas. Generalmente, los retrasos con mayor duración se relacionan con requerimientos de privacidad más estrictos o en estado de transición, cuando las organizaciones trabajan para adaptarse a las nuevas preocupaciones por parte de sus clientes (ver Figura 6).

Figura 6 Desglose de duración de retraso de ventas por país
Porcentaje de encuestados, N=2,081

País	Retraso promedio (semanas)
Alemania	3.1
Arabia Saudita	4.8
Argentina	3.9
Australia	3.9
Brasil	5.2
Canadá	5.1
China	3.5
España	5.5
Estados Unidos	3.7
Francia	4.2
India	4.9
Italia	2.6
Japón	4.1
México	2.9
Reino Unido	4.9
Rusia	2.5
Turquía	2.2
General	3.9

Fuente: Reporte de referencia de Privacidad de Datos 2019 de Cisco

Los retrasos de ventas, como mínimo, provocan que los ingresos se retrasen durante algún tiempo. Esto puede causar el incumplimiento de metas de ingresos, afectando así las compensaciones, las decisiones de financiamiento y las relaciones con los inversionistas. Además, el retraso en las ventas puede convertirse en ventas perdidas, por ejemplo, cuando los retrasos provocan que un cliente potencial compre el producto de la competencia o se arrepienta de comprar el producto o servicio.

También se pidió a los encuestados que identificaran los motivos de cualquier retraso de ventas relacionado con cuestiones de privacidad en sus organizaciones. Entre las principales respuestas están la necesidad de investigar las solicitudes específicas de los clientes, de traducir la información de privacidad al idioma del cliente, de instruir al cliente sobre los procesos o prácticas de privacidad de la compañía, o de tener que rediseñar el producto para cumplir con los requerimientos de privacidad del cliente (ver Figura 7).

Figura 7 Motivos para los retrasos de ventas
Porcentaje de encuestados, N=1,812

49%	Necesitamos investigar requerimientos específicos/ inusuales para el cliente/prospecto antes de que ellos estén satisfechos con nuestras prácticas de privacidad.
42%	Necesitamos traducir la información sobre nuestros procesos/políticas de privacidad al idioma del cliente/prospecto.
39%	El cliente/prospecto necesita aprender más sobre nuestros procesos o prácticas de seguridad.
38%	Es necesario rediseñar nuestro producto o servicio para que cumpla con los requerimientos de privacidad del cliente/prospecto.
33%	No podemos o no estamos dispuestos a cumplir con los requerimientos de privacidad del cliente/prospecto (por ejemplo, políticas de filtración de datos, requerimientos de eliminación de datos).
28%	Toma tiempo encontrar a la persona o al equipo adecuados para responder a las preguntas del cliente/prospecto.
17%	Debemos resolver cuestiones como cuál de las partes es responsable, incluso legalmente, de los datos.
5%	Debemos involucrar a nuestros abogados para que aclaren el panorama con respecto a la ley.

Fuente: Reporte de referencia de Privacidad de Datos 2019 de Cisco

Beneficios empresariales de las inversiones en privacidad

Las organizaciones que han invertido en prepararse para el GDPR se han enfocado principalmente en evitar las multas cuantiosas y otras penalizaciones asociadas con el incumplimiento del reglamento. Sin embargo, como lo indica la investigación, existen otros beneficios empresariales relacionados con estas inversiones en privacidad.

El retraso promedio de ventas a clientes actuales en relación con problemas de privacidad fue de 3.9 semanas. Sin embargo, las organizaciones que reportaron cumplir con todos o casi todos los requerimientos del GDPR tuvieron un retraso de ventas promedio de 3.4 semanas, en comparación con las 4.5 semanas de las organizaciones que no están listas pero esperan estarlo en un plazo de un año, y las 5.4 semanas de las organizaciones a las que aún les tomaría más de un año para estar listas. Por lo tanto, las organizaciones menos preparadas tienen en promedio retrasos casi 60% mayores a los de las que están más preparadas (ver Figura 8).

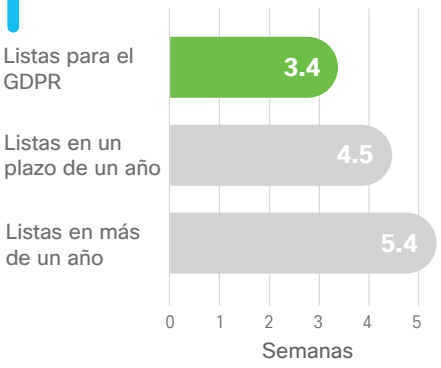
Aunque la mayoría de las compañías reportó haber sufrido alguna filtración de datos en el último año, un menor porcentaje (74%) de las compañías preparadas para el GDPR resultó afectado, en comparación con el 80% de las organizaciones que estarán preparadas para el GDPR en menos de un año, y el 89% de las que todavía tardarán más de un año en estar listas.

Resumen de hallazgos clave

Las compañías preparadas para el GDPR perciben beneficios tangibles adicionales al cumplimiento por sus inversiones en privacidad. Ahora sufren menos retrasos de ventas debido a preocupaciones sobre la privacidad por parte de los clientes (3.4 semanas vs. 5.4 semanas). Además, fueron menos propensos a sufrir filtraciones de datos durante el último año (74% vs. 89%), y, cuando estas ocurrieron, un menor número de registros resultó afectado (79 mil vs. 212 mil registros) y también hubo una reducción en el tiempo de inactividad del sistema (6.4 horas vs. 9.4 horas). Como resultado, los costos totales asociados con estas filtraciones fueron menores; solo el 37% de las compañías listas para el GDPR tuvieron pérdidas por encima de los $500,000 dólares en el último año vs. el 64% de las compañías menos preparadas para el GDPR.

stos resultados evidencian que el nivel de madurez de la privacidad se ha convertido en una ventaja competitiva importante para muchas compañías. Las organizaciones deberían esforzarse en maximizar los beneficios empresariales de invertir en privacidad, que podrían sobrepasar los requerimientos de cualquiera de las regulaciones de privacidad existentes.

Figura 8 Promedio de semanas de retraso (actuales)
Porcentaje de encuestados, N=2,081



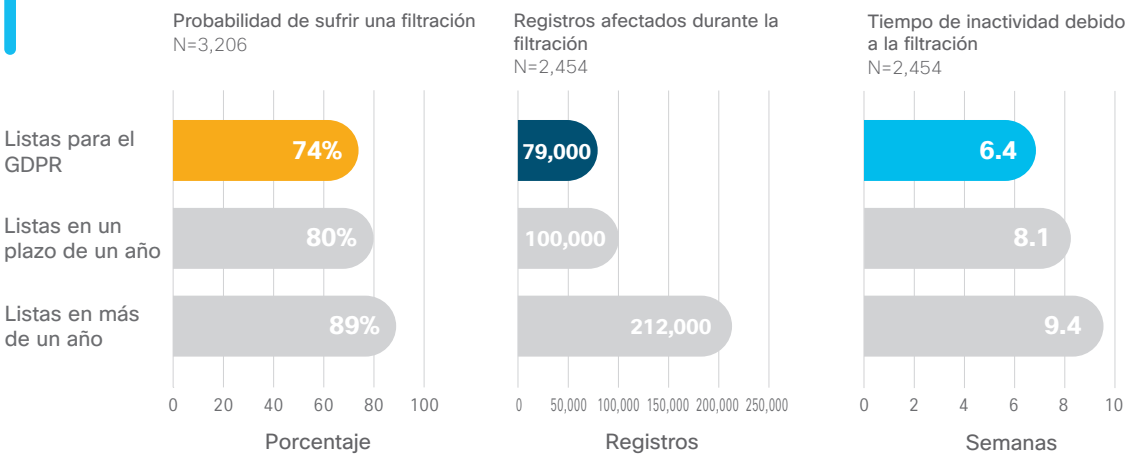
Fuente: Reporte de referencia de Privacidad de Datos 2019 de Cisco

> **"Las organizaciones aún tienen un largo camino por recorrer para maximizar el valor de sus inversiones en privacidad. Nuestra investigación señala que el mercado está listo para aquellos que estén dispuestos a invertir en activos de datos, y la privacidad es el camino correcto para alcanzar este punto".**
>
> **Michelle Dennedy, Gerente General de Privacidad, Cisco**

Otro beneficio tangible de estar listo para el GDPR es que parece reducir la frecuencia y el impacto de las filtraciones de datos. El GDPR exige que las organizaciones sepan dónde se encuentra la información de identificación personal (PII por sus siglas en inglés) y que esta información esté protegida adecuadamente. Estos esfuerzos pudieran haber ayudado a las organizaciones a entender mejor sus datos, los riesgos asociados a estos, y a implementar o reforzar sus medidas de protección.

Mientras que la mayoría de las compañías reportó haber sufrido alguna filtración de datos en el último año, un menor porcentaje (74%) de las compañías preparadas para el GDPR resultó afectado, en comparación con el 80% de las compañías que estarán preparadas para el GDPR en menos de un año, y el 89% de aquellas que tardarán más de un año en estar listas (ver Figura 9).

Figura 9 Beneficios empresariales de invertir en privacidad



Fuente: Reporte de referencia de Privacidad de Datos 2019 de Cisco

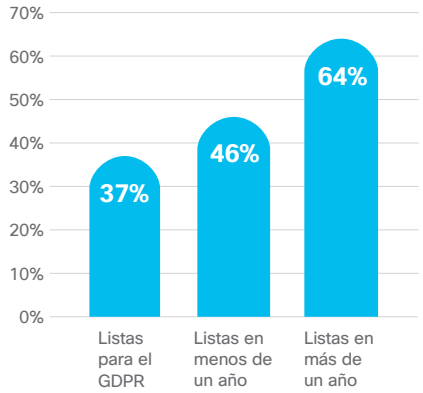
Más aún, al presentarse una filtración, las compañías preparadas para el GDPR experimentaron daños menores. El promedio de registros afectados fue de 79,000 para estas compañías, en comparación con los 212,000 registros para las compañías menos preparadas para el GDPR (ver Figura 9).

Casi todas las compañías (97%) reportan percibir beneficios adicionales hoy en día como resultado de sus inversiones en privacidad, incluyendo agilidad e innovación, ventaja competitiva, eficiencia operacional, reducción de pérdidas por filtraciones, disminución de retrasos de ventas, y un creciente atractivo para los inversionistas.

Las organizaciones que ya están listas para el GDPR también experimentaron tiempos más cortos de inactividad del sistema relacionados con dichas filtraciones, quizá debido a un mejor manejo de los activos de datos. Las compañías listas para el GDPR experimentaron en promedio un periodo de inactividad de 6.4 horas en comparación con las 9.4 horas de las organizaciones menos preparadas para el GDPR (ver Figura 9).

Con un menor número de registros afectados y menores tiempos de inactividad, era de esperarse que las compañías listas para el GDPR hayan tenido que pagar costos totales menores cuando sufren filtraciones de datos. Solo el 37% de estas compañías sufrieron pérdidas totales de al menos $500,000 dólares, en comparación con el 64% de las organizaciones menos preparadas para el GDPR (ver Figura 10).

Figura 10 Probabilidad de pérdidas de $500,000 dólares como resultado de una filtración de datos
Porcentaje de encuestados, N=3,206



Fuente: Reporte de referencia de Privacidad de Datos 2019 de Cisco

Con un menor número de registros afectados y menores tiempos de inactividad, era de esperarse que las compañías listas para el GDPR hayan tenido que pagar costos totales menores cuando sufren filtraciones de datos.

Las organizaciones reconocen los beneficios de invertir en privacidad

Las dos secciones previas de este estudio subrayan la relación entre las inversiones en privacidad y los beneficios empresariales, tales como la reducción de retrasos de ventas y filtraciones de datos menos costosas. Es de notar que la mayoría de los encuestados están empezando a reconocer muchos de estos beneficios. Cuando se les preguntó si sus inversiones en privacidad estaban rindiendo beneficios (tales como mayor agilidad e innovación, incremento en la ventaja competitiva, cumplimiento de la eficiencia operacional, etc.), el 75% de los encuestados identificó dos o más de estos beneficios y casi todas las compañías (97%) identificaron al menos un beneficio (ver Figura 11).

Figura 11 Beneficios de invertir en privacidad
Porcentaje de encuestados, N=3,259

42%	Propiciar una mayor agilidad/innovación como resultado de implementar controles de datos apropiados.
41%	Construir una ventaja competitiva mayor en comparación con otras organizaciones.
41%	Lograr una eficiencia operacional como resultado de organizar y catalogar los datos.
39%	Mitigar las pérdidas ocasionadas por las filtraciones de datos.
37%	Reducir los retrasos de ventas debido a preocupaciones de privacidad de datos por parte de clientes y prospectos.
36%	Incrementar el atractivo para los inversionistas.
3%	Ninguno de los anteriores.

Fuente: Reporte de referencia de Privacidad de Datos 2019 de Cisco

Las organizaciones que reportaron cumplir con todos o casi todos los requerimientos del GDPR tuvieron un retraso de ventas promedio de 3.4 semanas.

Maximizar el valor de los datos

La privacidad de datos es un aspecto crítico de los esfuerzos totales de una organización para maximizar el valor de sus activos de datos a lo largo del ciclo de vida de estos. Como con cualquier otro activo, los datos deben adquirirse, capturarse, protegerse, utilizarse y almacenarse/destruirse de manera eficiente. Las organizaciones que maximizan el valor de sus datos de manera adecuada pueden beneficiarse enormemente al consolidar la confianza de sus clientes y utilizar datos bien protegidos y catalogados para mejorar la experiencia del cliente y generar un mayor valor para todos los interesados.

Se les preguntó a los encuestados de este estudio sobre los comportamientos en entornos que presentan un buen nivel de madurez de datos, tales como tener un catálogo completo de datos, conectar los datos con otros activos, contratar a una gerente general de datos y monetizar los datos externamente (ver Figura 12). Menos de la mitad de los encuestados mostraron una de estas características, por lo que esta será un área para futuras investigaciones para entender mejor cómo las organizaciones están maximizando el valor de sus activos de datos.

Implicaciones

Estos resultados resaltan el hecho de que invertir en privacidad ha creado un valor empresarial adicional al cumplimiento, y que esto se ha convertido en una ventaja competitiva para muchas compañías. Por lo tanto, las compañías deben esforzarse para entender las implicaciones de sus inversiones en privacidad, incluyendo la reducción de retrasos en su ciclo de venta y el hecho de minimizar el riesgo y los costos asociados con las filtraciones de datos, así como otros beneficios potenciales como agilidad e innovación, ventajas competitivas y eficiencia operacional.

El análisis y las observaciones resultantes de este estudio pueden servir como marco y punto de partida para que cada organización maximice el valor de sus inversiones en privacidad.

Figura 12 Comportamientos presentes en ambientes con un buen nivel de madurez en manejo de datos
Porcentaje de encuestados, N=3,259

42%	Entendemos el valor de todos/la mayoría de nuestros activos de datos.
42%	Sabemos dónde se encuentra toda/la mayoría de la información de identificación personal y cómo se utiliza.
40%	Conectamos nuestros activos de datos de manera eficiente para generar un mayor valor para nuestros clientes y para nosotros.
37%	Tenemos un catálogo relativamente completo de nuestros activos de datos.
32%	Tenemos un gerente general de datos.
32%	Nos consideramos una compañía centrada en la información.
30%	Somos capaces de monetizar activos de datos seleccionados al venderlos (o intercambiarlos) externamente.
2%	Ninguna de las anteriores.

Fuente: Reporte de referencia de Privacidad de Datos 2019 de Cisco

Las organizaciones que maximizan el valor de sus datos de manera adecuada pueden beneficiarse enormemente al consolidar la confianza de sus clientes y utilizar datos bien protegidos y catalogados para mejorar la experiencia del cliente y generar un mayor valor para todos los interesados.

> **“Una buena política de privacidad corporativa puede proteger a las firmas de cualquier daño financiero debido a filtraciones de datos, al ofrecerle a los clientes total transparencia y control sobre su información personal, mientras que, por otro lado, una política defectiva puede exacerbar los problemas causados por una filtración”.**
>
> **Harvard Business Review, “A Strong Privacy Policy Can Save Your Company Millions”, Feb. 15, 2018**

Conclusión

Invertir en privacidad ha generado un valor comercial adicional al cumplimiento y se ha convertido en una importante ventaja competitiva para muchas compañías.

Este estudio ha cuantificado una serie de beneficios comerciales relacionados con el nivel de madurez de la privacidad. Muchos de los beneficios identificados inicialmente en el reporte del año anterior se han confirmado y explorado de manera más completa, incluyendo la reducción en los retrasos en ventas relacionadas con la privacidad, y en la frecuencia y el impacto de las filtraciones de datos. En futuras investigaciones, exploraremos cómo estos beneficios están cambiando con el tiempo, especialmente a medida que las regulaciones de privacidad y las expectativas de los clientes continúan evolucionando en diferentes industrias y diferentes áreas geográficas. Cisco continuará trabajando con nuestros clientes y otros líderes en el campo de la privacidad para proporcionar la información necesaria para tomar mejores decisiones de inversión y mejorar la confianza con nuestros clientes.

Para más información, visite:
Data Privacy: A Business Perspective

Acerca de Cisco Cybersecurity Series

Durante la última década, Cisco ha publicado un rico acervo de información definitiva sobre seguridad e inteligencia de amenazas para profesionales de seguridad interesados en conocer el estado de la ciberseguridad global. Estos reportes exhaustivos proporcionan informes detallados sobre el estado de las amenazas y sus consecuencias organizacionales, así como las mejores prácticas para protegerse de las consecuencias adversas de las filtraciones de datos.

En un esfuerzo por consolidar nuestro liderazgo de ideas, Cisco Security publica una serie de artículos basados en investigaciones y apoyados por datos, en la sección Serie de Ciberseguridad de Cisco.
Hemos aumentado el número de títulos para incluir varios reportes para profesionales de la seguridad con distintos intereses. Acudiendo a la experiencia de los innovadores e investigadores de las amenazas dentro de la industria de la seguridad, la recopilación de reportes de la serie de 2019 incluye el Reporte de referencia de Privacidad de Datos, el Reporte de Amenazas, y el Análisis de mercado para CISOs, a los cuales se añadirán nuevos reportes durante el transcurso del año.

Para obtener más información, visite: https://www.cisco.com/mx/securityreports.

Oficinas Centrales en América
Cisco Systems, Inc. San Jose, CA

Oficinas Centrales en Asia Pacífico
Cisco Systems (USA), Pte. Ltd. Singapore

Oficinas Centrales en Europa
Cisco Systems International BV Amsterdam,

Cisco cuenta con más de 200 oficinas en todo el mundo. Las direcciones, los números de teléfono y fax están listados en el sitio de Cisco en la siguiente dirección web: www.cisco.com/go/offices. Publicado en Enero de 2019

PRIV_01_0119_r1