Leyes de privacidad de datos: Simplificación de los trámites

un informe de Ovum contratado por Intralinks

ovum

INTRA LINKS™

ovum

Contenido

INTRA LINKS

Una transferencia de derechos de privacidad a nivel mundial representa nuevos y considerables riesgos de negocios y económicos

Los gobiernos nacionales están promulgando nuevas y estrictas leyes de privacidad de datos para proteger los datos de los ciudadanos, salvaguardar los intereses de seguridad nacional y proveer potencialmente un impulso para las industrias locales. Este apuro por proteger la información confidencial y personal amenaza las actuales estrategias, prácticas y procesos empresariales que las organizaciones que operan a nivel internacional usan ampliamente.

Para explorar el impacto de la evolución de las reglamentaciones de privacidad de datos y la soberanía de los datos, Ovum fue contratada en el tercer trimestre de 2015 por Intralinks para realizar una encuesta internacional a 366 encargados de tomar decisiones de TI.

Las siguientes son algunas de las conclusiones clave:

Las reglamentaciones de privacidad de datos entran directamente en conflicto con las prácticas de la nube, el software como servicio (SaaS) y la informática móvil dentro de las empresas.

La computación en la nube es una parte establecida del panorama de TI empresarial, y se espera que la adopción siga aumentando durante la siguiente década. Los procesos de negocios con mucho intercambio de información dependen del SaaS, y esto, aunado a un cambio hacia las plataformas de computación móviles, implica que controlar la ubicación de los datos y cumplir con las regulaciones de privacidad es algo extremadamente difícil. Sin embargo, durante los próximos tres años, el 78% de los encuestados planea usar aplicaciones en la nube y basadas en SaaS, incluso para almacenar y compartir datos confidenciales y regulados.

Los líderes de negocios son bastante pesimistas en cuanto a las consecuencias potenciales de las nuevas reglamentaciones de privacidad de datos

Nuestra encuesta muestra que las organizaciones son conscientes de que la privacidad de los datos es un problema, pero se enfrentan a desafíos para decidir cómo responder a ello. Cuando preguntamos sobre el Reglamento general sobre la protección de los datos (GDPR) pendiente en la Unión Europea, el 52% dijo que creen que resultará en multas comerciales para su compañía, y dos tercios piensan que los va a obligar a realizar cambios en su estrategia de negocios en Europa.

El costo del cumplimiento reglamentario será considerable, pero el costo de no cumplir será aún más elevado

Cerca del 70% de los encuestados esperan incrementar los gastos para cumplir con los requerimientos de soberanía de los datos, y cerca del 30% esperan que los presupuestos aumenten más del 10% durante los próximos dos años. De los que planean actualizar las estrategias de privacidad de los datos en los próximos tres años, el 38% planea contratar especialistas y el 27% contratará a un director de privacidad.

Las organizaciones con sede en Estados Unidos son especialmente vulnerables

El efecto Snowden es real. De entre las 20 economías industrializadas, Estados Unidos se clasifica como el país menos confiable y el más probable en obtener acceso no autorizado a la información confidencial; seguido por China en segundo lugar y Rusia en tercer lugar. Las nuevas regulaciones también pondrán a las compañías estadounidenses en una desventaja aún mayor, pues el 63% de los encuestados creen que las reglamentaciones propuestas del GDPR de la UE les dificultarán más competir a las compañías estadounidenses, y el 70% piensa que la nueva legislación favorecerá a las empresas con sede en Europa.

ovum

La mayoría de las organizaciones no utilizan la tecnología de manera efectiva para lidiar con los problemas de privacidad de datos

Lo alarmante es que muchas organizaciones no están aprovechando las tecnologías disponibles que protegen los datos confidenciales. Solo el 44% de los encuestados monitorean las actividades de los usuarios y proporcionan alertas a las violaciones de la política de datos, y solo el 53% definen información como “reservada” para que quede cubierta bajo los controles de acceso. Casi la mitad (47%) no tienen políticas ni controles que gobiernen el acceso al almacenamiento en la nube para el consumidor como Dropbox.

Las organizaciones mundiales necesitan una metodología orquestada para la soberanía de los datos que cubra a las personas, los procesos y la tecnología.

Los líderes de negocios reconocen la necesidad de adoptar un enfoque equilibrado para abordar la soberanía y la privacidad de los datos. Cuando se les preguntó sobre las estrategias de inversión, el 55% dijo que están planeando nueva capacitación para empleados, el 51% enmendará y adaptará las políticas, y el 53% se prepararán adoptando nuevas tecnologías.

Las organizaciones se enfrentan a una amalgama de reglamentaciones sobre la privacidad a nivel mundial contradictorias y conflictivas, y necesitan opciones de tecnología para lidiar con todas las eventualidades

La revolución de la soberanía de los datos amenaza con la creación de un panorama de tecnología “balcanizada”, en donde distintas jurisdicciones imponen mandatos inconsistentes y a menudo incompatibles en cuanto a la forma de almacenar, procesar y compartir los datos personales. Esto ya está creando confusión e incertidumbre y deja las preguntas fundamentales sin responder, como la forma

INTRA LINKS

Introducción

de interpretar los requisitos sobre la ubicación de los datos. Las organizaciones necesitan opciones de tecnología que les permitan reaccionar a un entorno reglamentario en rápido cambio.
Incluso antes de que las revelaciones de Edward Snowden mostraran todo el alcance de la vigilancia electrónica de la Agencia de Seguridad Nacional (NSA) de Estados Unidos, la privacidad de los datos se estaba convirtiendo en un problema mundial. La intromisión del gobierno, combinada con las fugas de datos masivas durante los últimos años, obligó a los gobiernos nacionales a reconocer que las leyes de privacidad actuales sobrevivieron a la era basada en papel y necesitan ser adaptadas a las realidades de la economía digital. El resultado ha sido una ola sin precedentes de nueva legislación diseñada para gobernar la forma en que se pueden recopilar, almacenar, procesar y compartir ciertos datos confidenciales.

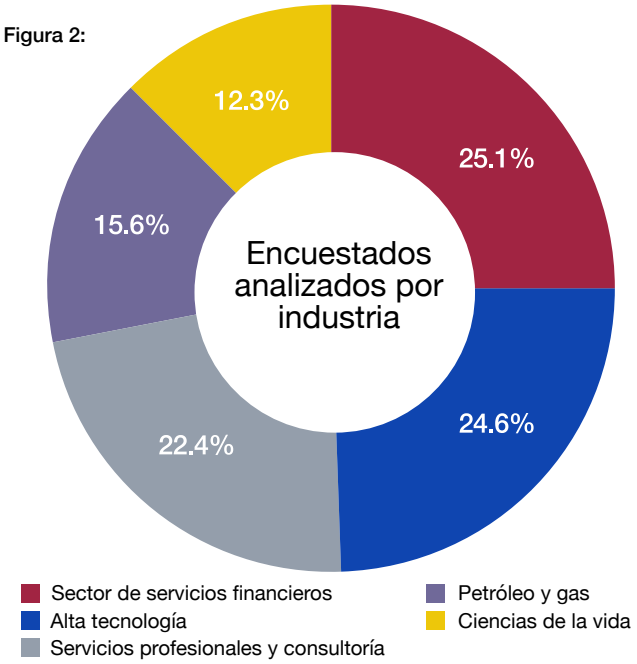
Países tan diversos como Brasil, Singapur y Rusia están haciendo sus reglamentaciones más estrictas. La Unión Europea se acerca al final de un proceso extenso de revisión de la legislación en este campo, lo que afectará a toda organización que opere en sus países miembros. Estas restricciones se imponen debido a que las organizaciones ya no están delimitadas por fronteras y los empleados son más móviles, lo que junto con una migración a los sistemas de TI basados en la nube puede provocar un conflicto con estas nuevas leyes. Las obligaciones de cumplimiento que surgen de la legislación se están volviendo más complejas, en particular para las organizaciones que operan a través de distintas jurisdicciones, y en especial en el contexto de cómo se aplica la legislación a los datos almacenados por los servicios basados en la nube.

En el tercer trimestre de 2015 Intralinks, proveedor líder de soluciones de colaboración de contenido en la nube a nivel empresarial, contrató a Ovum para entender cómo afectarán las reglamentaciones de privacidad de datos a los negocios a nivel mundial. Se realizó una encuesta para explorar las siguientes preguntas:

- ¿Cómo se están preparando las organizaciones para abordar la soberanía de los datos?
- ¿Cuál será el impacto de las nuevas reglamentaciones sobre la privacidad de datos?
- ¿Cómo adaptarán las organizaciones sus negocios para cumplir con las nuevas obligaciones de privacidad?
- ¿Cuáles son las diferencias de opinión en los distintos países y en diferentes jurisdicciones?
- ¿Qué decisiones de tecnología respaldarán las obligaciones de privacidad de los datos?
- ¿Cuáles son las mejores prácticas para adaptarse a los regímenes reglamentarios?

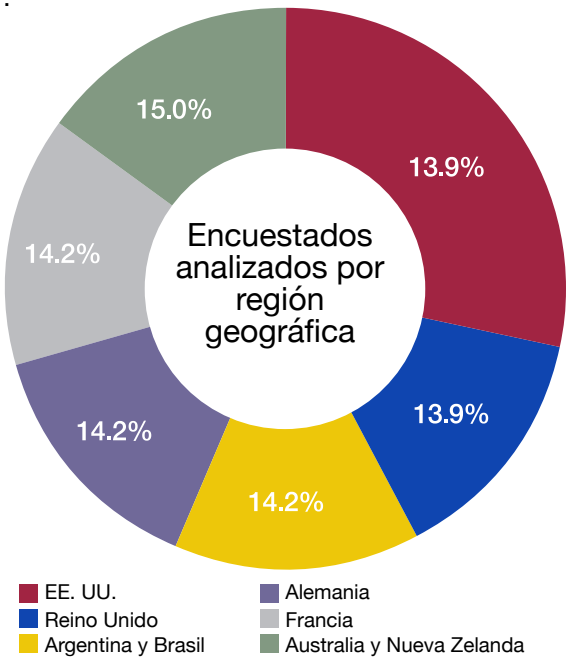
La encuesta de Ovum incluye los comentarios de 366 encuestados de todo el mundo, dentro de organizaciones de distintos tamaños, en diversas industrias (vea las figuras 1, 2 y 3). La demografía se eligió de manera deliberada para incluir una variedad de tipos de organizaciones y países que se ven afectados por las reglamentaciones sobre la privacidad de los datos y las obligaciones de soberanía de los datos.

Figura 2:



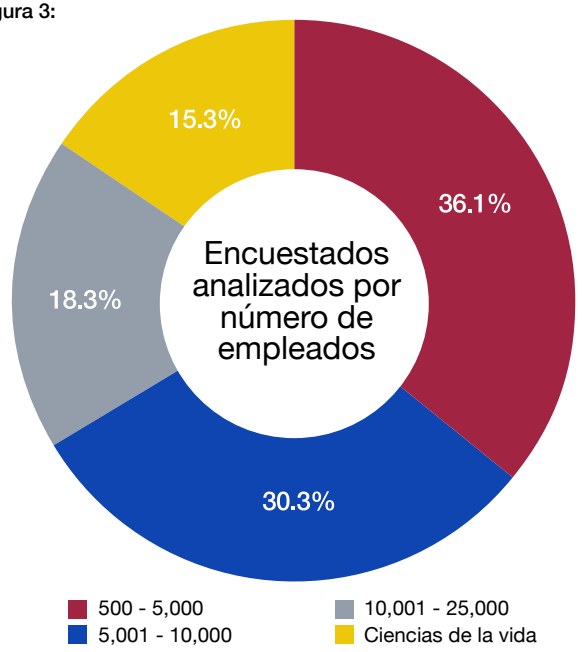
Fuente: Ovum

Figura 1:



Fuente: Ovum

Figura 3:



Fuente: Ovum

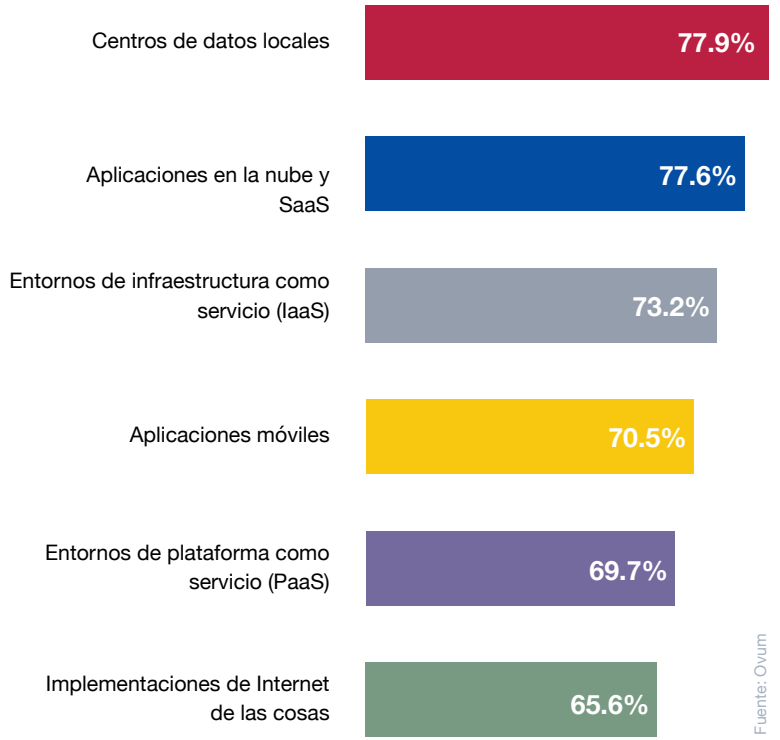
Las empresas se enfrentan a importantes desafíos en cuanto al cumplimiento

Es inevitable continuar el uso de la nube

La computación en la nube impulsa la productividad en los negocios modernos. Conecta toda la fuerza laboral, vincula facilitando las relaciones entre organizaciones, socios de negocios y clientes, y nos conecta a todos en el sentido social. Ha transformado la forma en que nos comunicamos y usamos la información, cambiando de manera radical a las compañías más establecidas del mundo y la forma en que se administran los presupuestos de TI. Por ejemplo, la investigación reciente de Ovum descubrió que, en general, una sexta parte de los presupuestos de TI de las organizaciones ya se destina típicamente a SaaS, y se espera que ese gasto en las soluciones basadas en la nube crezca. Alrededor de cuatro quintas partes de las empresas usan ahora o planean usar la computación en la nube en los modelos de implementación (privada, pública e híbrida) y servicio (IaaS, PaaS y SaaS), en comparación con dos terceras partes a principios de 2014. El mercado se está expandiendo a medida que nuevas generaciones de adoptadores salen a la luz. La segunda ola de adopción ya ha alcanzado su punto cúlmine y una tercera ola, de rezagados, ha comenzado también a crecer en 2015.

La encuesta de soberanía de los datos proporciona nueva evidencia en cuanto a la forma en que se espera que la nube aloje los datos regulados y confidenciales. Lo que es un evidente contraste con lo de hace algunos años, cuando las conversaciones giraban alrededor de si se debía confiar en la nube o no. Ahora, se confía en ella para proteger los activos más confidenciales (vea la figura 4), demostrando un cambio en la opinión con respecto a su rol positivo en los negocios en la actualidad. La encuesta también descubrió que el 58% de los encuestados confían en la nube para todas las operaciones de negocios, a pesar del potencial impacto de las regulaciones pendientes de privacidad de los datos, que intentan modificar la forma en que se almacenan, transfieren y procesan los datos en todo el mundo. Así, incluso con el clima reglamentario cambiante, la computación en la nube es una decisión ya tomada. Sin embargo, la regulación de los datos contenidos en la nube se está convirtiendo rápidamente en el mayor problema al que se enfrentan los abogados, políticos y empresas a medida que intentan equilibrar la privacidad con el acceso y la productividad.

Figura 4: Respuestas a "¿En cuáles de estos entornos tecnológicos van a estar presentes sus datos regulados y confidenciales dentro de los próximos tres años (es decir, hasta mediados de 2018)?"



Ovum cree que parte de la razón de favorecer la computación en la nube es una cuestión de dotación de recursos. No es ningún secreto que las organizaciones tienen con frecuencia recursos limitados para aplicar la protección correcta de los datos regulados y confidenciales, o demostrar el cumplimiento adecuado si los datos se conservan de manera interna. Como tal, la protección de los datos en sí se está convirtiendo en otro impulsor para la adopción de la nube, debido a que los clientes ven que los proveedores de la nube tienen mayores probabilidades de "envolver" su paquete de servicios con las mejores soluciones de seguridad que puedan.

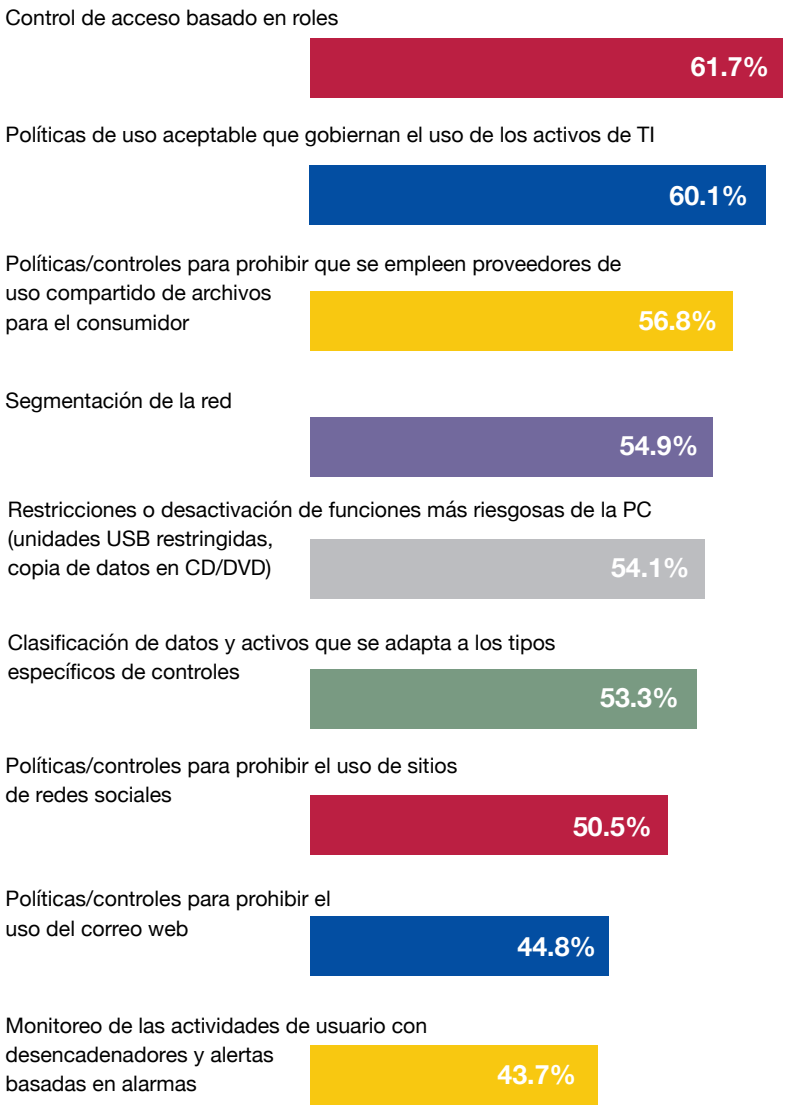
Las organizaciones no están tomando las medidas básicas para proteger los datos confidenciales

También descubrimos que muchos encuestados ni siquiera aplican las medidas básicas de seguridad para proteger los datos y satisfacer los requerimientos de cumplimiento actuales (vea la figura 5). Solo el 44% de los encuestados monitorean la actividad de los usuarios además de tener desencadenadores y alertas basadas en políticas, y solo el 62% han adoptado controles de acceso basados en roles. Solo un poco más de la mitad (53%) clasifica actualmente los activos de información para facilitar los controles. Descubrimos que ni siquiera se están tomando las medidas rudimentarias y solo el 54% deshabilita funciones de PC tales como unidades externas conectadas. Además, solo el 57% bloquea el acceso a aplicaciones de almacenamiento sin control y de uso compartido de archivos para el consumidor como Dropbox.

Es probable que las organizaciones con estas brechas en la protección de datos recurran a los proveedores de la nube para ayudar, en vez de invertir tiempo y recursos en tratar de corregir los problemas de datos internamente. Un análisis posterior de los resultados de la encuesta muestra que la escasez general de medidas de privacidad de los datos se aplica especialmente a las organizaciones más pequeñas y de tamaño mediano. Es probable que, para ellas, la actualización de las funcionalidades de protección de los datos requiera una inversión proporcionalmente mayor, lo que explica este resultado.

Es probable que el enfoque de los clientes de todo tipo de organización sobre el alcance preciso de esta protección aumente a medida que se toma conciencia de las mayores responsabilidades de cumplimiento para proveer salvaguardas adecuadas para los datos confidenciales, junto con el convencimiento de que las tecnologías relevantes para hacerlo están en manos de los proveedores de la nube y de SaaS.

Figura 5: Respuestas a "¿Qué políticas, procesos y controles implementa su organización actualmente para ayudar a proteger los datos y evitar el mal uso de los mismos?"



Fuente: Ovum

Las reglamentaciones de privacidad de los datos no son uniformes, lo que deja a las empresas mundiales vulnerables y confundidas

Mientras que las organizaciones ya están fracasando en implementar medidas estándar de protección de los datos, las nuevas leyes de privacidad de los datos más estrictas los dejarán todavía más a la deriva. Las leyes de privacidad de datos se están escribiendo a nivel local, sin ningún marco de trabajo gobernante global para imponer orden. Las organizaciones mundiales que operan a través de varias jurisdicciones se enfrentan a una amalgama de leyes que exigen respuestas diferentes (vea la tabla 1). Tampoco está claro cuántas leyes actuales pueden cambiar exactamente. Por ejemplo, el Puerto seguro (Safe Harbor), un acuerdo de transferencia de datos de 15 años de antigüedad entre la Unión Europea y Estados Unidos, recientemente se declaró inválido, lo que afecta a más de 4000 empresas que ya no pueden transferir legalmente datos fuera de la Unión Europea hacia Estados Unidos sin la cobertura de otros mecanismos legales como las cláusulas modelo, o las reglas corporativas vinculantes. Esto deja a las empresas mundiales, en especial las que tienen una presencia en Europa, confundidas acerca del curso de acción más seguro y preocupadas por estar ahora violando la ley.

Tabla 1: estado actual de la reglamentación de protección de los datos

País/región	Definición de datos personales	Se requieren formularios de consentimiento para el tratamiento de los datos personales	Reglas para la transferencia de datos personales al extranjero	Solicitudes de datos de los organismos públicos	Sanciones
Unión Europea	Información relacionada con una persona física identificada o identificable. El proyecto de reglamento incluye las direcciones IP.	"Consentimiento inequívoco." El proyecto de reglamento busca introducir el consentimiento explícito.	La Unión Europea y los estados miembro deciden si un tercer país ofrece una protección adecuada; de lo contrario deben implementarse salvaguardas.	No queda claro después de la derogación de la Directiva de Retención de Datos. Las leyes nacionales siguen formalmente vigentes.	Las sanciones se deciden a nivel de país. El proyecto de reglamento propone multas de hasta el 2% del volumen anual de operaciones de una compañía.
EE. UU.	No está claro. Varía entre las distintas leyes/industrias.	"Consentimiento escrito o electrónico" previo en la Ley de Comunicaciones.	No hay reglas específicas. La Comisión Federal de Comercio (FTC) afirma que la ley estadounidense se sigue aplicando cuando los datos salen de Estados Unidos.	Por lo general se requiere una orden judicial. El FBI y otras agencias tienen excepciones según la Ley Patriota.	Las sanciones varían entre las diferentes actas.
Australia	"La información u opinión, sea verdadera o no, y sea grabada en forma material o no, acerca de un individuo identificado, o un individuo que pueda identificarse de manera razonable."	Las organizaciones deben tomar "las medidas razonables según las circunstancias" para notificar a un individuo sobre esa recolección de sus datos.	Las organizaciones de transferencia deben tomar las medidas razonables para asegurar que no se infrinjan los principios de la ley una vez que se envíen los datos a otro país.	Una agencia gubernamental no debe recolectar información personal a menos que dicha información sea razonablemente necesaria para, o esté directamente relacionada con, una o más de sus funciones o actividades.	Sanciones civiles de hasta $1.57m (A$1.7m) por infracciones graves o repetidas de la ley.
Singapur	"Los datos, sean verdaderos o no, acerca de un individuo que pueda identificarse ya sea a partir de esos datos o junto con otros datos o información a la que probablemente la organización tenga acceso."	Hay que obtener el consentimiento por escrito o registrado de modo que pueda almacenarse para una referencia a futuro, aunque puede obtenerse en forma verbal.	Se permiten las transferencias si se puede lograr el mismo nivel de protección de los datos en el país receptor.	Las agencias y organizaciones públicas que actúan en representación de una agencia pública quedan exentas de la Ley de protección de datos personales (PDPA).	Sanción financiera de una cantidad que no exceda los $799,000 (SG$1m).
Brasil	No está claro. El "marco de trabajo civil de Internet" se completará mediante una reglamentación más detallada.	"Consentimiento libre, informado y explícito." La próxima reglamentación puede definir esto con más detalle.	Se permite la transferencia, pero las compañías tienen que cumplir con la legislación brasileña si algún proceso de recolección/procesamiento de datos ocurre en Brasil.	El tiempo de retención es de un año para los registros de conexión del ISP y de seis meses para los proveedores de aplicaciones. La policía o los juzgados pueden requerir una extensión.	Hasta el 10% del volumen de operaciones de la compañía en Brasil, sin incluir impuestos, y la suspensión temporal o completa de las actividades de recolección y procesamiento de datos.

Fuente: Ovum, y texto citado literalmente de la legislación

Las regulaciones europeas pendientes establecerán el estándar para la privacidad de datos a nivel mundial, pero pondrán en riesgo la economía de la Unión Europea

Medida en función del PIB, la Unión Europea en su conjunto, es la economía más grande a nivel mundial de acuerdo con el Fondo Monetario Internacional (FMI) y el Banco Mundial. Por lo tanto, tiene la habilidad de establecer el estándar reglamentario para otras regiones mundiales, y cualquier legislación europea impactará sin duda a todas las organizaciones que operen a nivel internacional. La provisión para la protección de la privacidad de los datos dentro de la Unión Europea se realizó primero bajo la Directiva de Protección de los Datos de 1995. Sin embargo, hace unos años había un reconocimiento generalizado dentro de las autoridades de la Unión Europea de que la tecnología había avanzado, y se requeriría un nuevo régimen reglamentario (el GDPR pendiente) para lidiar con la adopción comercial de los smartphones, las tabletas, la conectividad de banda ancha universal y los servicios en la nube. La tabla 2 proporciona un resumen de algunos de los cambios importantes en el GDPR.

Nuestra encuesta reveló que las compañías mundiales pretenden modificar las operaciones de negocios en algunos países europeos una vez que esté listo el GDPR. De acuerdo con nuestra muestra, el 78% de las compañías estadounidenses, el 62% de las compañías del Reino Unido, el 46% de las compañías de Brasil y Argentina, el 71% de las compañías alemanas, el 58% de las compañías francesas y el 71% de las compañías en Australia y Nueva Zelanda (ANZ) pretenden revisar sus metodologías. Esto podría representar un severo golpe económico para la Unión Europea, cuya prosperidad recae en los negocios internacionales. La clave de esta decisión es el costo, puesto que el 68% de los encuestados a nivel mundial creen que el GDPR incrementará drásticamente los costos de hacer negocios en la Unión Europea Además, el 85% de las compañías estadounidenses creen que será más difícil competir contra las compañías europeas, lo que podría significar que disminuirá el número de compañías estadounidenses que operan en la Unión Europea. Estos resultados demuestran una enorme incertidumbre con respecto al GDPR, en donde las compañías pronostican un impacto negativo en los negocios mundiales y probablemente en la economía de la Unión Europea como resultado.

Otra cuestión planteada por nuestros encuestados es la de los castigos potenciales. El alcance de las multas para las empresas en caso de una violación del GDPR es potencialmente el 2% de los ingresos globales, lo cual significa miles de millones de dólares para las compañías de mayor erfil a nivel mundial. De acuerdo con nuestra investigación, cerca del 50% de las empresas mundiales creen que recibirán una multa como resultado del GDPR. Si desglosamos esto por país y región, significa que el 62% de las compañías alemanas, el 59% de las compañías estadounidenses, el 53% de las compañías del Reino Unido, el 42% de las compañías francesas, el 56% de las compañías de ANZ y el 32% de las compañías de Brasil y Argentina creen que recibirán una multa como resultado del GDPR.

Tabla 2: algunos de los principales cambios en el GDPR

Cuestión del GDPR	Cambio	Impacto
Una sola solución	Las compañías acordarán su postura de cumplimiento con un solo regulador en toda la Unión Europea, en vez de uno por cada estado miembro	Simplificación del cumplimiento. NB: aún no se garantiza en un 100% que este plan vaya a entrar en vigor
Procesadores de datos	La legislación sobre la privacidad de los datos se extiende de los controladores de datos y está sujeta a una nueva clase de actor: el procesador de datos	Los proveedores de servicio en la nube, proveedores SaaS y otros necesitan cumplir con la ley de privacidad de datos de la Unión Europea
Extraterritorialidad	Las compañías con oficinas generales fuera de la Unión Europea están cubierta por la ley si manejan datos sobre residentes de la Unión Europea	Los proveedores de servicios que no sean de la Unión Europea tal vez necesiten invertir en centros de datos locales, como una metodología
Residencia de los datos	Los datos sobre personas de la Unión Europea no pueden transferirse fuera de la EEA sin una cobertura legal. (Vea la información fuera de esta tabla acerca de la desaparición de la cobertura bajo la certificación de Puerto seguro)	Como se indica arriba
Elaboración de perfiles	Una persona afectada tendrá que dar su consentimiento para que se pasen sus datos a otros controladores de datos aparte del que ya cuenta con su consentimiento para fines de elaborar su perfil	Esto impactará potencialmente a los procesadores de datos si usan o reenvían información a otros controladores de datos, o si la utilizan ellos mismos para fines de elaborar perfiles. NB: aún existe el debate acerca de si el consentimiento debe ser explícito o puede ser implícito

Fuente: Ovum

En general, la mayoría de las compañías globales (57%) creen que el GDPR es una reacción excesiva a las prácticas de vigilancia reveladas por el material que Edward Snowden publicó. Curiosamente, los encuestados europeos también están de acuerdo con esta opinión, en donde el 57% de los encuestados alemanes, el 51% de los encuestados del Reino Unido y el 46% de los encuestados franceses dicen que el GDPR es una reacción exagerada al problema de los derechos sobre la privacidad de los datos. De nuevo, la motivación detrás de estas respuestas probablemente corresponda a las implicaciones de los costos, desde la perspectiva tanto de las multas como de la estrategia de negocios.

La ubicación de los datos es el punto crítico de control, pero es difícil definirla

Desde el punto de vista legislativo, la cuestión acerca de "dónde están los datos" es crítica. En el debate sobre la soberanía de los datos, las preocupaciones fundamentales incluyen la ubicación de los datos y la definición clara del punto de control sobre los datos personales. En nuestra investigación, hay incertidumbre y confusión acerca de estos conceptos aparentemente obvios. La habilidad de ejercer la soberanía sobre los datos corporativos (para controlar el acceso a los mismos) y lograr el cumplimiento depende en gran parte de la ubicación de los datos, ya que su ubicación es un factor para determinar qué legislación es aplicable a esos datos, y el nivel de acceso que debe estar disponible. Ejercer el control sobre la ubicación de los datos es una dificultad considerable para muchas organizaciones, ya que la mayoría de los sistemas no apoyan el concepto de que la ubicación de los datos es una decisión relacionada con los negocios, y en especial los sistemas basados en la nube. La complejidad respecto a esta cuestión empeora debido a que la definición exacta de la ubicación de los datos para fines de cumplimiento varía entre las distintas disposiciones legales, y puede estar abierta a la interpretación legal en los distintos lugares. Las organizaciones que tratan de lograr el cumplimiento probablemente necesiten opciones que ofrezcan control sobre la ubicación física, lógica, legal y política de los datos. Sin duda ya estamos viendo que se presentan argumentos jurídicos en juzgados de todo el mundo que dependen del concepto fundamental acerca de dónde se ubican y controlan los datos, y quién tiene jurisdicción sobre los mismos (un ejemplo es el caso de Microsoft relacionado con los datos almacenados en Dublín, Irlanda, que están siendo solicitados por un juez de Estados Unidos).

Nuestra encuesta muestra (vea la tabla 3) que no hay un consenso claro sobre estas preguntas a la ubicación de los datos. Descubrimos también que el 50% de las organizaciones de los encuestados planeaban cambiar la metodología primaria de este control durante los próximos tres años. Esto puede reflejar incertidumbre en cuanto a la capacidad de la metodología actual de nuestros encuestados de atender los nuevos requerimientos, y también acerca de cuál metodología deben usar. También puede sugerir que las organizaciones están esperando a que surja un estándar. Plantea una fuerte necesidad de una metodología que proporcione varias opciones técnicas, como la habilidad de ofrecer controles para la ubicación física y lógica.

Tabla 3: Metodologías actuales/posibles de los encuestados para abordar la privacidad de los datos

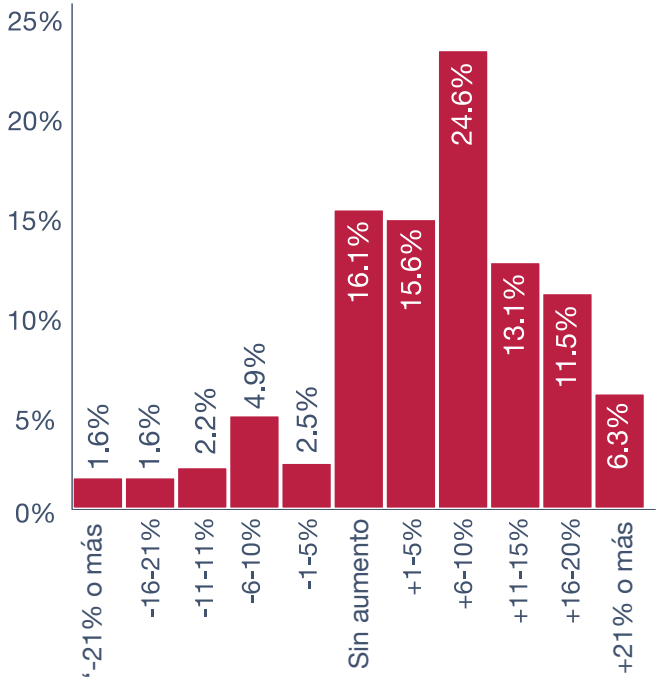
Respuesta	Metodología primaria actual	Consideraciones de esta metodología
Tomamos nuestras decisiones sobre privacidad de los datos usando la ubicación legal de los mismos (esto se refiere a un país o países que probablemente tengan una jurisdicción sobre los datos – y la jurisdicción cuyas leyes deben quebrantarse para que alguien acceda a los datos contra su voluntad). – por ejemplo, un país responsable de sus propias leyes que rigen estas cuestiones	26%	27%
Tomamos nuestras decisiones sobre privacidad de los datos usando la ubicación lógica de los mismos: (la ubicación geográfica desde donde se ejerce el control sobre una función computacional dada; es decir, en donde reside el punto de cifrado).	27%	33%
Tomamos nuestras decisiones sobre privacidad de los datos usando la ubicación física de los mismos: (tradicionalmente, la ubicación o las ubicaciones geográficas en donde se escribe la información en el medio de almacenamiento).	33%	24%
Tomamos nuestras decisiones sobre privacidad de los datos usando la ubicación política de los mismos (este es probablemente el punto de aplicación de la presión gubernamental para liberar el contenido).– por ejemplo, Estados Unidos o la Unión Europea	14%	15%

Fuente: Ovum

Las regulaciones imponen costos enormes

A medida que cambia el clima reglamentario (como en Hong Kong, Singapur y Rusia, por ejemplo), los presupuestos se están viendo afectados. La regulación de la privacidad de los datos es por tradición un problema legal, pero puesto que ahora impactará las funciones de tecnología y cumplimiento, nuestra investigación muestra que numerosas compañías esperan hacer contrataciones en estos departamentos para hacer frente a las implicaciones de las regulaciones pendientes sobre privacidad de los datos. Desglosados, el 19% anticipa contrataciones en la función legal, el 31% anticipa contrataciones en la función de tecnología y el 34% anticipa contrataciones en la función de cumplimiento. A su vez, esto genera más dudas acerca del cambio de roles laborales y las habilidades en el campo legal, de cumplimiento y tecnológicas que serán más valiosas a medida que las nuevas reglamentaciones entren en completa vigencia. De acuerdo con nuestros resultados, los encuestados creen que los profesionales de tecnología y cumplimiento son las contrataciones más apropiadas para apoyar lo que se define comúnmente como un problema legal, y es probable que veamos más especialistas en tecnología y cumplimiento aprendiendo más acerca de las leyes de privacidad de datos en los próximos años.

Figura 6: respuestas a "¿Qué alteraciones en el presupuesto espera en los próximos dos años como resultado de una reforma regulatoria mundial relacionada con la protección/soberanía de los datos?"



Fuente: Ovum

Sin duda, con un impacto de tal alcance, los costos aumentarán. Nuestra encuesta indica el efecto esperado sobre el presupuesto en general (vea la figura 6). Cabe destacar que cerca del 30% de los encuestados esperan que los presupuestos aumenten al menos en un 10%, y que casi una cuarta parte espera entre el 6% y el 10% de aumento. En general, más del 70% de los encuestados esperan que sus presupuestos aumenten debido a la regulación pendiente sobre la privacidad de datos.

Las organizaciones con sede en Estados Unidos se encuentran bajo presión

Como consecuencia de las revelaciones de Edward Snowden sobre las actividades de vigilancia de la Agencia Nacional de Seguridad de Estados Unidos, este país se enfrenta a mucha desconfianza. Pedimos a los encuestados que clasificaran a los principales países industrializados con base en quiénes creían que accederían a sus datos sin permiso, y Estados Unidos se consideró el menos confiable, con China y Rusia en segundo y tercer lugar respectivamente. En realidad, el debido proceso legal en Estados Unidos proporciona una sólida protección de la privacidad, sin duda mejor que incluso algunos países europeos, pero las opiniones han estado muy influenciadas por la tormenta de los medios que ganó impulso después de las revelaciones.

Las nuevas reglamentaciones en Europa también pondrán a las compañías estadounidenses en desventaja. En nuestra encuesta, el 63% de los encuestados creen que las reglamentaciones del GDPR propuestas por la Unión Europea harán que sea más difícil para las compañías estadounidenses competir, y el 70% creen que la nueva legislación favorecerá a las empresas con sede en Europa.

Recommendations

Las cuestiones de soberanía de los datos que surgen de la legislación van a tener un impacto considerable en numerosas organizaciones que tienen alcance operacional internacional. Las organizaciones necesitan equilibrar los requerimientos de negocios, legales y de los consumidores al momento de manejar la información personal. Las acciones necesarias ahora son:

Establecer una estrategia de soberanía de los datos

Las compañías que operan a nivel internacional y recopilan información personal identificable (PII) están sujetas a las reglamentaciones de privacidad de los datos en todos los países en los que realizan negocios. Las organizaciones no están protegidas de la responsabilidad debido a que dependen de un proveedor de nube independiente para administrar los datos. El primer paso es reconocer esta responsabilidad y crear una estrategia para reaccionar. Esta estrategia debe ser administrada por un equipo ejecutivo básico, responsable de establecer controles corporativos, políticas y procedimientos para mantener el cumplimiento. Su equipo de GRC tal vez ya se haya embarcado en este proceso, pero su equipo ejecutivo necesita ser el patrocinador.

Realizar una evaluación del riesgo de la privacidad

La buena gobernanza debe incorporar la identificación de riesgos considerables para la organización. El contexto es en extremo importante al evaluar la exposición a la privacidad, y ciertas industrias como las compañías de ciencias de la vida y los proveedores de seguros se enfrentan a una supervisión y escrutinio reglamentario considerables. La evaluación del riesgo de la privacidad debe comenzar por clasificar la información en categorías amplias (por ejemplo, PII, información confidencial de la compañía) y asociarla a los procesos de negocios existentes y las geografías relacionadas. Identifique y revise las regulaciones pertinentes sobre la privacidad en cada jurisdicción en la que opere. Esté preparado para cambiar los procesos de negocios y cumplir con las exigencias reglamentarias. Tal vez ya cuente con tecnologías que puedan ayudarle a evaluar su contenido (por ejemplo, herramientas de clasificación de datos como Atlas) y, por el contrario, probablemente tenga tecnologías en uso que incrementen su riesgo (por ejemplo, las herramientas de uso compartido de archivos para el consumidor, como Dropbox).

Incluir a las personas

Cuestiones legales y de tecnología dentro del alcance de evaluar los efectos de las cuestiones de soberanía de los datos: reconozca que la privacidad y la soberanía de los datos son desafíos complejos que afectan a toda su empresa. Educar su fuerza laboral es tan imprescindible como implementar soluciones de tecnología para administrar los flujos de datos. No es financieramente viable ni legalmente pertinente enfocarse solo en la tecnología, los procesos o la actividad de los empleados, ya que los tres son importantes.

Comenzar las discusiones ahora

Con los proveedores existentes de tecnología y servicio acerca de sus planes para atender los nuevos requerimientos legales: los distribuidores expertos ya están preparados para ofrecer opciones para abordar las cuestiones de privacidad de los datos. La disponibilidad de diferentes opciones es imprescindible debido a que las leyes serán inconsistentes de un país a otro y cambian con rapidez. Los distribuidores deben ser capaces de responder a las preguntas sobre la ubicación lógica y física de los datos, y tener contratos de servicio que también proporcionen una flexibilidad global.

Apéndice

Metodología

La encuesta de Ovum, realizada en el tercer trimestre de 2015, incluye 366 respuestas de organizaciones de distintos tamaños, en diferentes áreas del mundo y a través de un rango de industrias. El análisis de los resultados de las encuestas se llevó a cabo en el contexto de consultas continuas con clientes de Ovum, discusiones con proveedores de la industria y una investigación secundaria.

Autor

Alan Rodger, analista sénior, gestión empresarial de las TIC
alan.rodger@ovum.com

Asesoramiento de Ovum

Esperamos que este análisis le ayude a tomar decisiones de negocios informadas e imaginativas. Si tiene requisitos adicionales, tal vez el equipo de asesoramiento de Ovum pueda ayudarle.

Para obtener más información acerca de las capacidades de asesoramiento de Ovum, contáctenos directamente en consulting@ovum.com.

ovum

COMUNÍQUESE CON NOSOTROS

www.ovum.com
askananalyst@ovum.com

OFICINAS INTERNACIONALES

Pekín
Dubái
Hong Kong
Hyderabad
Johannesburgo
Londres
Melbourne
Nueva York
San Francisco
Sao Paulo
Tokio

INTRA LINKS