KPMG

¿Dónde está el límite?

Impresiones de los consumidores sobre los límites de su privacidad

kpmg.es

Índice

Prólogo

Las empresas tienen más información sobre sus clientes que nunca. En las últimas 24 horas, su organización probablemente ha recabado más datos sobre sus clientes que lo que era imaginable hace una o dos décadas: los alimentos frescos que compran, dónde van de vacaciones, en qué restaurante cenaron anoche o cómo han ido a trabajar esa mañana.

Como consumidores, nos beneficiamos de esta cercanía. Las aplicaciones de fitness que miden los pasos que damos, las de mensajería que utilizamos para enviar fotos desde la playa o la tecnología telemática de nuestros coches con la que nos rebajan la prima del seguro.

Cuando utilizamos esta tecnología —ya sea en un ordenador, un smartphone o un automóvil conectado—, suele darse por supuesto que cedemos nuestros datos a cambio del servicio o producto que hace nuestras vidas más fáciles, más informadas y, en ocasiones, más baratas.

Ese es el trueque sobre el que se basa la economía de los datos, pero existen límites. Cada vez somos más conscientes de que las organizaciones obtienen, utilizan, conservan y revelan nuestra información, e incluso la compran y la venden. Y nos asalta la siguiente inquietud: ¿en qué punto se cruza la línea de la «cercanía útil» y nos adentramos en terreno «peligroso e intrusivo»?

Cuando algo es gratis, probablemente lo estés pagando con tus datos, algo que a la larga puede resultar más que caro.

KPMG planteó a casi 7.000 personas en 24 países –200 de ellas en España- una serie de preguntas a fin de entender en qué circunstancias se sentían cómodos o incómodos con la idea de que se utilicen sus datos personales, para describir dónde se ha trazado la denominada «línea de peligro».

Este informe es una guía para las organizaciones, con el objetivo de ayudarles a moverse por esta línea sin cruzarla.

No es ninguna sorpresa que cada uno traza la línea en lugares diferentes; lo que para una persona es inaceptable, para otra no lo es. El sexo, la edad, el poder adquisitivo, la nacionalidad, la formación... todo ello modifica y altera su trayectoria, a menudo de forma sorprendente.

Más de la mitad de los participantes en el estudio aceptan informar sobre su sexo, formación o grupo étnico en Internet, por ejemplo, mientras que menos del 20% está dispuesto a divulgar sus ingresos, ubicación, historial médico o dirección postal.

De los 22 países participantes, los consumidores españoles, son los terceros más preocupados por el modo en el que las empresas gestionan y utilizan su información personal, solo por detrás de India y Singapur.

La sociedad apenas acaba de empezar a afrontar las cuestiones morales y legales sobre qué es privado y qué es público en la era del análisis de datos masivo (big data). No se trata de un debate teórico que las empresas deban pasar por alto. Incumplir las normas o subestimar las sensibilidades del consumidor no solo expone a las empresas a cuantiosas sanciones económicas en mercados clave como la Unión Europea (UE) y Estados Unidos, sino que también puede traducirse en una pérdida de confianza y en el distanciamiento de consumidores que sienten que se está violando su privacidad. El precio de las acciones, los ingresos e incluso la supervivencia de algunas empresas probablemente requerirán un enfoque más inteligente y complejo.

En la UE, además, tras varios años de debate, el Parlamento europeo aprobó el pasado mes de abril de 2016 el Reglamento 2016/679, que someterá a unos estrictos estándares de gestión de datos a las compañías que presten servicios a los ciudadanos europeos, independientemente de si su sede está en la Unión Europea o fuera de ella. El marco regulatorio y la opinión pública son cada vez más estrictos.

Muy pocas empresas se están preguntando si están procesando correctamente la información de los clientes desde el punto de vista moral y legal. No obstante, ha llegado el momento de que se lo planteen.

Marc Martínez
Socio responsable de Ciberseguridad de KPMG en España

Javier Aznar
Senior manager, responsable de Privacidad en IT Advisory

¿Dónde ponen el límite los consumidores?

¿Cuándo se convierte en inaceptable lo que antes parecía correcto? ¿Cuándo lo que resulta cómodo pasa a ser intrusivo? Conocer a fondo las sensibilidades de los consumidores sobre el uso de sus datos personales es esencial para establecer y mantener una relación de confianza con las empresas.

Algunas conclusiones:

Más de la mitad de los participantes de España y a nivel global afirman estar dispuestos a compartir datos personales sobre su sexo, formación y grupo étnico en Internet.

<20%

Menos del 20% acepta revelar información sobre su historial de búsquedas en la red, sus ingresos, su ubicación, su dirección postal o su historial médico.

56%

El 56% de los encuestados españoles asegura haber dejado de realizar alguna compra online por desconfianza ante lo que podría ocurrir con sus datos.

Solo los encuestados de **España** (53%) y Alemania (66%) priorizan la comodidad sobre la privacidad. Más de la mitad de la media global cree que la privacidad es más importante.

Según los encuestados, las redes sociales y las empresas de juego y ocio solicitan una cantidad innecesaria de información personal.

El 84% de los encuestados españoles está preocupado por la venta de sus datos personales a terceros facilitados en compras online.

>2/3

Más de dos tercios a nivel global no están conformes con que las aplicaciones de teléfonos móviles y tabletas utilicen sus datos personales. En España, esta cifra alcanza el 85%.

El **68% de los españoles** borra las cookies en su navegador y el 46% gestiona los parámetros de privacidad de sus redes sociales y cambia periódicamente usuarios y contraseñas como principales medidas para proteger su información personal.

Alrededor de un **tercio global** y en España utiliza el modo incógnito o "sin seguimiento" cuando navega por Internet.

El **18% de los encuestados de España** recurre a la encriptación para proteger sus datos personales, por debajo del 25% de la media global.

50%

A nivel global, **alrededor de la mitad** aceptaría productos gratis o rebajados a cambio de menos privacidad.

El **55% de los encuestados españoles** siente que no tiene ningún control sobre el uso que las empresas hacen du sus datos.

El **nivel de estudios** no parece afectar a las opiniones sobre privacidad y lo que se considera peligroso o aceptable.

El temor a la recopilación de datos masivos

Muchas organizaciones no reconocen todavía los distintos niveles de intrusión que las personas están dispuestas a tolerar en diferentes áreas de sus vidas. Los consumidores suelen compartimentar sus relaciones con las empresas dependiendo de cuándo y dónde interactúan con ellas. Cuando las empresas entran en una zona percibida como demasiado privada, corren el riesgo de irritar a los consumidores y, en última instancia, de que se desvinculen de la marca.

Distintas sensibilidades

Aunque tal vez a las empresas les gustaría recopilar constantemente datos personales de los consumidores, esto resulta incómodo. Por lo general, las personas tienen diferentes umbrales en cuanto a la privacidad según si están en su hogar, en el trabajo o en un entorno público, y son reacias a ceder a terceros el control de la misma.

En España, el 55% de los encuestados siente que no tiene ningún tipo de control sobre el uso que las empresas hacen de sus datos personales mientras que solo un 10% tiene la sensación de controlar suficientemente cómo procesan y utilizan su información personal. Los encuestados españoles son los que en mayor porcentaje perciben esta falta absoluta de control de los 24 países participantes, seguidos de los franceses (49%) y los rusos (48%).

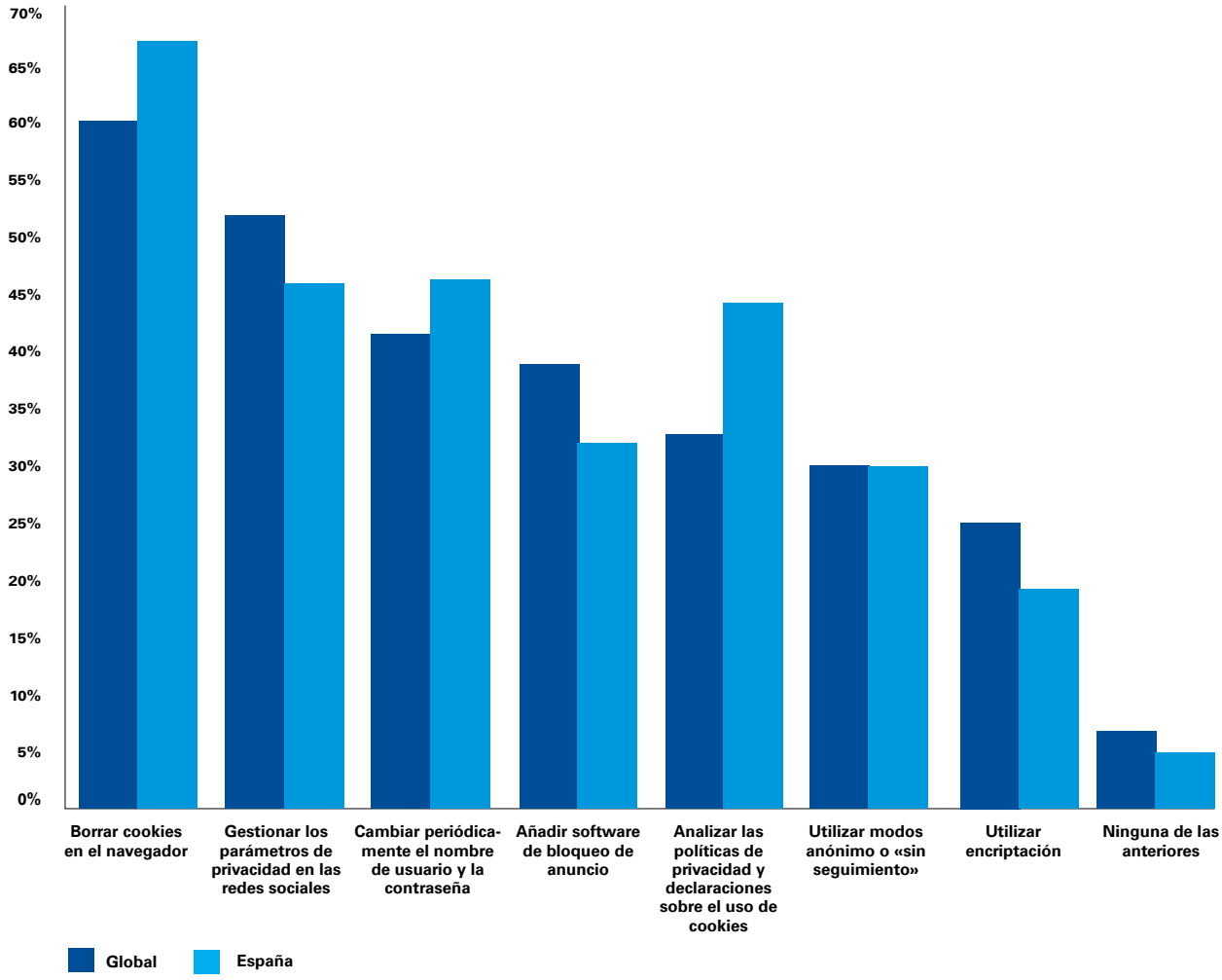
Así pues, la recolección indiscriminada de este tipo de información puede provocar un distanciamiento de los consumidores respecto a las empresas. En este sentido, cuanto más incómodas se encuentren las personas, es más probable que tomen medidas para proteger sus datos personales en la red. A escala global, el 60% de los participantes ya borra las cookies en su navegador de Internet, el 68% en España.

También más de la mitad gestiona los parámetros de privacidad de sus redes sociales, cifra que en España disminuye hasta el 46%, el mismo porcentaje que cambia nombres de usuario y contraseñas de forma habitual.

En la media global, casi un tercio de los encuestados españoles (30%) utiliza el modo incógnito. Por otro lado, mientras que un 18% recurre a la encriptación (Figura 1), por debajo del 25% global.

Dos tercios de los encuestados españoles están preocupados o muy preocupados por la manera en que las organizaciones procesan y utilizan sus datos personales.

Figura 1: Precauciones que toman los consumidores para proteger su información personal



La esfera pública frente a la privada

Las personas nos ponemos instintivamente en alerta cuando tenemos que facilitar información relativa a nuestra vida familiar. No obstante, existen diferencias entre países. Algunas empresas suministradoras de energía y agua en Estados Unidos, por ejemplo, han experimentado ya la resistencia de algunos ciudadanos a instalar contadores inteligentes en edificios residenciales[1]. Mientras que a nivel global, el estudio revela que el 43%de los ciudadanos desconfiaría de la instalación de contadores inteligentes en sus hogares si la información obtenida pudiera servir para calcular cuántas personas viven en ellos y qué hacen en determinados momentos del día, en España casi seis de cada diez encuestados se sentirían cómodos con esta práctica.

1. http://bv.com/docs/articles/the-opt-out-challenge.pdf

¿En quién confían los consumidores?

Máxima confianza

Bancos
41%
33%

Proveedores de servicios de salud
39%
38%

Cuerpos de seguridad
36%
38%

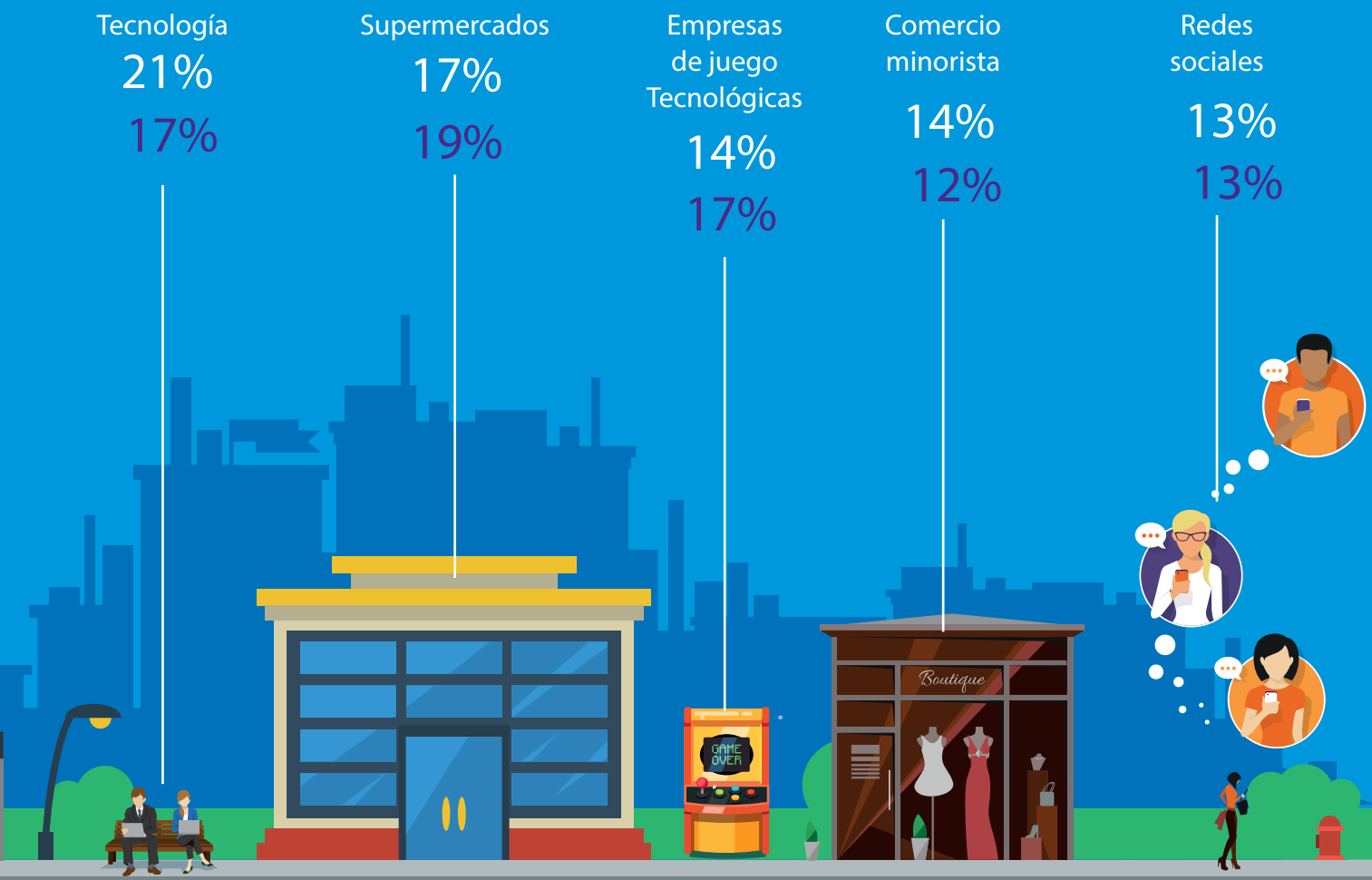
Administración local
33%
39%

Empresas de suministros públicos
23%
25%

Global

España

Mínima confianza



El mensaje que se infiere del estudio es que la postura adoptada hacia la privacidad varía dependiendo del tipo de datos personales de que se trate y del uso específico que se les quiera dar, así como de la disposición y la ubicación del consumidor. Por ejemplo, el 78% de los encuestados de España – también a nivel global- consideraría «inquietante» ver anuncios personalizados en vallas publicitarias, mientras que un 59% estaría dispuesto a que se hiciera un seguimiento de su consumo televisivo a cambio de una rebaja en el precio de su televisor. Igualmente, un 54% (el 49 a nivel global) tolera bien que organismos gubernamentales recopilen datos personales para luchar contra el terrorismo, mientras que solo un 16% está cómodo con que los comercios minoristas vendan sus datos personales a terceros.

En la foto global hay enormes diferencias regionales en términos de actitudes. En la India, el 78% opina que está «bien» que las compañías de taxis utilicen datos de geolocalización para proponer una ruta a los clientes, mientras que en Dinamarca solo lo acepta el 22% (Figura 2). Asimismo, las vallas personalizadas están bien vistas por el 60% en China, aunque no así por el 88% en Japón (Figura 3).

Esto plantea la posibilidad de una economía dual para la información personal. Algunos consumidores están dispuestos a facilitar sus datos de carácter personal (o no tienen alternativa), mientras que los más precavidos pueden implantar estrategias —o, potencialmente, pagar— para proteger su privacidad. Esta es una perspectiva desagradable tanto para los anunciantes como para las empresas, puesto que se apoyan en la información sobre sus clientes para desarrollar su oferta y comercializar sus productos de forma eficaz. Por ello, y para que los consumidores sigan facilitando dicha información de forma gratuita, es extremadamente importante que las organizaciones utilicen apropiadamente los datos personales de sus clientes.

Figura 2: Uso de la geolocalización por parte de las compañías de taxis

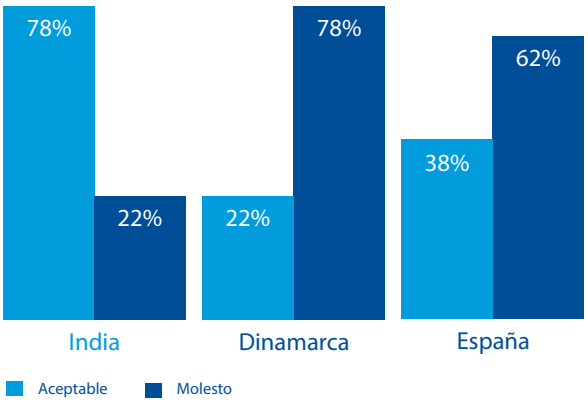
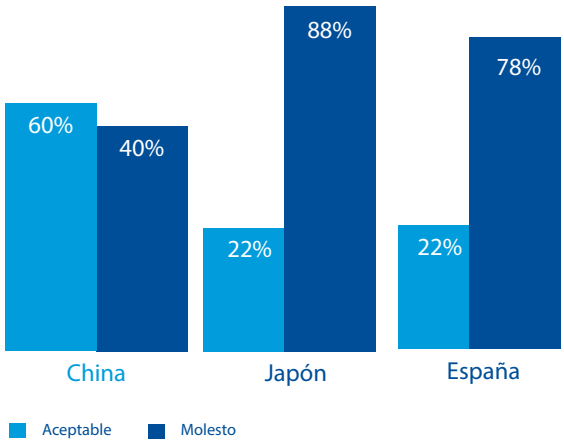


Figura 3: Publicidad personalizada en vallas electrónicas



Claves para directivos: un riesgo para la confianza

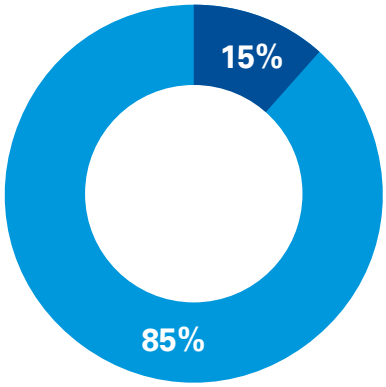
Marc Martínez
Socio responsable de Ciberseguridad
de KPMG en España

"Para no perder la confianza de los consumidores, las empresas deben actuar con mayor prudencia al recabar datos personales de ámbitos que éstos consideran más sensibles. Aunque quizás algunos sigan apreciando el intercambio de datos personales por servicios como un precio que merece la pena pagar, otros pondrán todo su empeño en protegerlos.

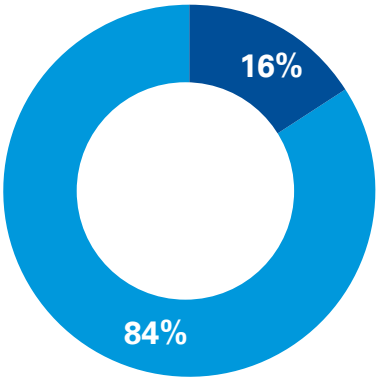
Si las empresas no presentan argumentos atractivos a la hora de solicitar datos, los consumidores que tengan la opción podrían incluso decidir denegarlos, lo que podría preconizar diferentes categorías de consumidores en cuanto a la privacidad en el procesamiento de su información personal. Las personas a quienes les preocupa su privacidad tienden a invertir en diversos métodos de protección para salvaguardarla. Así, tal y como señala el estudio, ya son muchos los que están adoptando medidas reforzadas para proteger su privacidad en la red".

Una visión general

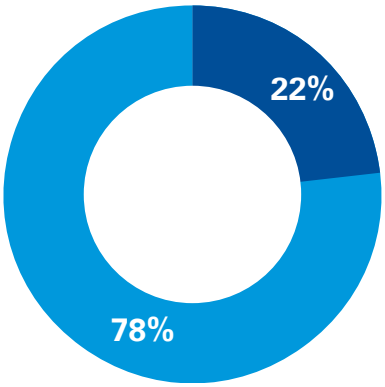
Qué le aporta valor al consumidor y qué le resulta molesto en el uso de sus datos personales (aceptable frente a molesto).



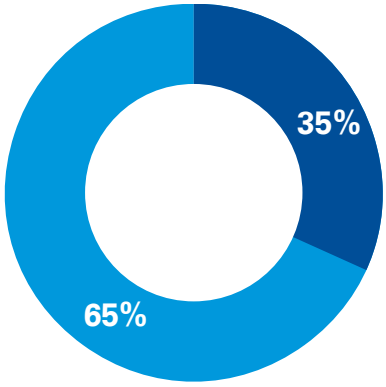
Que las aplicaciones para smartphones y tabletas utilizadas para navegar, chatear y recibir noticias puedan acceder a contactos, fotos e historial de navegación.



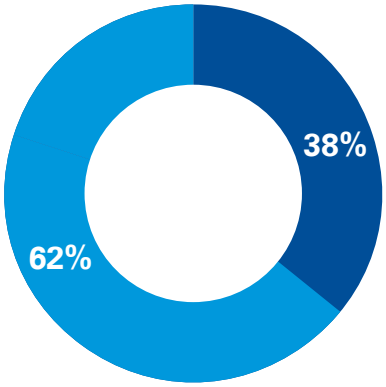
Que tiendas online que ofrecen ahorro, velocidad, comodidad, mayor gama de productos y entrega a domicilio vendan sus datos a terceros.



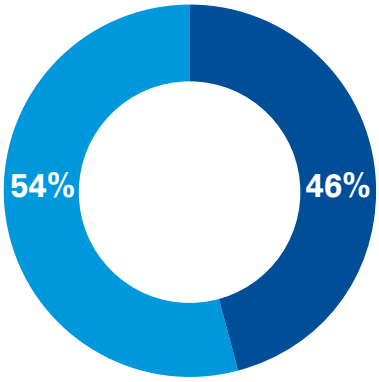
Que una valla publicitaria electrónica le salude por su nombre propio, le pregunte si ha disfrutado del desayuno y le muestre un anuncio de sus cereales favoritos.



Que al día siguiente de escribir un correo electrónico a un amigo sobre un plan para viajar a París, aparezcan anuncios de hoteles, restaurantes y excursiones en París al navegar por Internet.



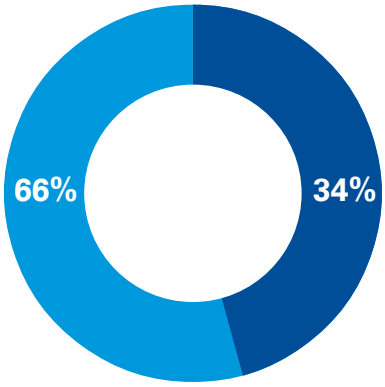
Que una empresa de taxis compre sus datos de geolocalización para poder proponerle automáticamente una ruta nada más bajarse del tren.



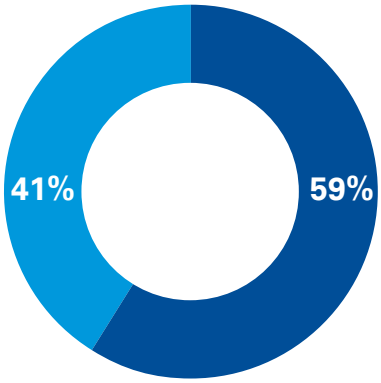
Que un dispositivo gratuito de fitness controle su bienestar y genere un informe mensual para usted y la empresa donde trabaja.

Molesto

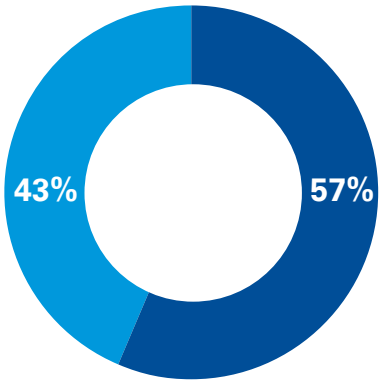
Aceptable



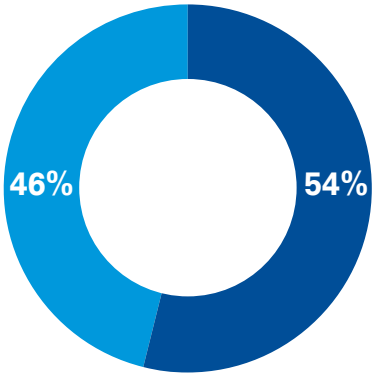
Que instalar un dispositivo telemático en su coche reduzca el precio de su seguro pero otorgue a la aseguradora el derecho a informar a la policía si conduce de forma peligrosa.



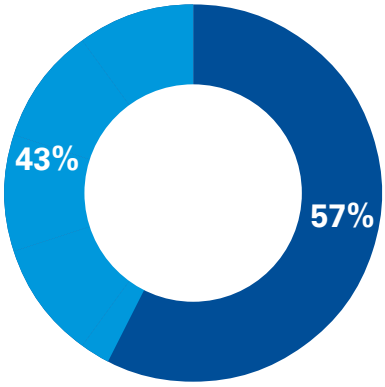
Que le ofrezcan un descuento al comprarse un televisor nuevo si permite que se haga un seguimiento de sus hábitos de consumo televisivo.



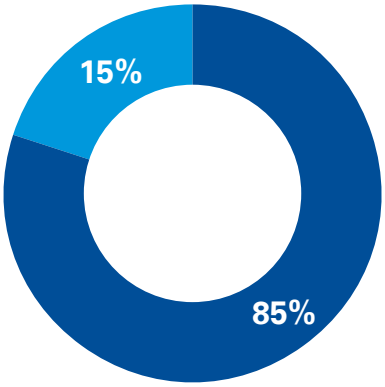
Que le ofrezcan una tablet gratuita si permite que una empresa de tecnología haga un seguimiento de cuándo, por qué y cómo la utiliza.



Que los cuerpos de seguridad monitoricen sus correos electrónicos, mensajes de texto e historial de navegación para ayudar a impedir actos terroristas.



Que le instalen contadores inteligentes de energía que permitan al proveedor deducir cuántas personas viven en su hogar, cuándo comen y duermen, y los electrodomésticos que utilizan.



Que tu coche nuevo traiga instalado un dispositivo telemático que permite a los servicios de emergencia localizar su vehículo.

Cuidado con la reacción

A diario, los consumidores aceptan facilitar sus datos personales a las organizaciones a cambio de información gratuita, conocimiento inmediato, entretenimiento ilimitado y una comodidad sin precedentes. Mientras el consumidor tenga la sensación de que está recibiendo un trato justo, el acuerdo se mantiene.

Pero, ¿qué sucedería si una parte significativa de consumidores, digamos los que consideran incómodo el uso de sus datos personales, comenzaran a sentir que no les compensa? ¿O fueran más conscientes de hasta qué punto se han estado utilizando sus datos personales? La creciente adopción del modo de navegación de incógnito, el bloqueo de anuncios y la eliminación de cookies son señales tempranas de que se trata de una cuestión cada vez más importante para muchas personas.

El estudio reveló que el 68% de los consumidores españoles (el 60% de todo el mundo) eliminan las cookies en su navegador de Internet.

Sin embargo, mientras que en India el 60% cambia periódicamente nombres de usuario y contraseñas para proteger la información personal, en España lo hace el 46%, el mismo porcentaje que gestiona los parámetros de privacidad en sus redes sociales.

En el extremo contrario, los participantes procedentes de Japón son los que menos precauciones toman para proteger sus datos personales y apenas un 30% borra cookies o gestiona la privacidad de sus redes sociales

Lo cierto es que a medida que aumenta la concienciación sobre la privacidad, las empresas se encuentran más expuestas a que los consumidores reaccionen cuando se den cuenta de las cantidades de dinero que se mueven con la comercialización de sus datos.

Los modelos de negocio de los grandes motores de búsqueda y redes sociales se basan en la venta de datos de consumidores. La Organización para la Cooperación y el Desarrollo Económicos (OCDE) estima que los datos personales de cada consumidor europeo reportan casi cinco dólares anuales a Facebook. En el caso de los estadounidenses, la cuantía se acerca a 10 dólares[2]. En 2014, una start-up de intermediación de datos denominada Datacoup ofrecía derechos exclusivos de propiedad a las personas sobre sus propios datos por 8 dólares mensuales[3], lo que presagia una hipotética realidad, discutible desde el punto de vista ético, en la que los individuos tengan que recomprar sus propios datos personales a terceros.

Las personas pueden generar datos personales a partir del seguimiento de su actividad, de sus compras y de sus comunicaciones en Internet. Los recopiladores de datos dirían que una vez que han compartido sus datos personales, dejan de pertenecerles.

El servicio nacional de salud del Reino Unido, por ejemplo, ya ha estado buscando fórmulas para monetizar sus archivos de datos personales. Los defensores de esta vía aducen que el coste de transición a un servicio de salud digitalizado se compensaría con el ahorro derivado del incremento de la eficiencia y permitiría, además, ofrecer el acceso a datos anónimos de salud previo pago.

2. OCDE (2013), Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value (Análisis del plano económico de los datos personales: un estudio sobre metodologías para cuantificar el valor monetario), OECD Digital Economy Papers, No. 220, OECD Publishing. http://dx.doi.org/10.1787/5k486qtxldmq-en

3. How much is your personal data worth? (¿Cuánto valen sus datos personales?) | Noticias | The Guardian

Agencias de datos: conocerse y conocer a otros

Probablemente saben más de usted que sus seres queridos, su madre o su padre; posiblemente incluso más que usted mismo.

Las agencias de datos recopilan y venden información acerca de miles de millones de personas de todo el mundo. Incluso pueden conocer su dirección de correo electrónico y número de teléfono, sus búsquedas por Internet de meses anteriores, patrones de compra... incluso su orientación sexual.

Una destacada agencia de datos afirma poseer información sobre 700 millones de consumidores en todo el mundo y más de 3.000 predilecciones para casi cada consumidor estadounidense.

Reparto de ingresos

Un modelo más equitativo para el reparto de ingresos procedentes de datos personales consistiría en que los consumidores ejecutaran un acuerdo formal de reparto de ingresos con las empresas que venden sus datos personales. Otra opción sería que las empresas establecieran el precio de sus productos en función de los datos personales que facilite el consumidor. Esto ya sucede en cierta medida con el dispositivo telemático que reduce las primas del seguro del conductor a cambio de la supervisión de sus hábitos de conducción. De hecho, a escala global, el 45% de los participantes aceptarían que las aseguradoras supervisasen su conducción a cambio de un abaratamiento de las primas, incluso a expensas de ser denunciados a la policía. Aunque en España solo el 34% estaría cómodo con esta opción, los consumidores encuestados de China y Brasil en su mayoría (64%) estarían conformes (Figura 4).

No es descabellado imaginar que el siguiente paso podría ser un acuerdo similar que permitiese a las personas reducir la prima de su seguro de salud a cambio de usar un dispositivo de control de su estado físico.

Según el estudio, si la empresa para la que trabajan ofreciera a los participantes en el estudio el dispositivo de fitness más novedoso para supervisar su condición física y facilitarle un informe mensual sobre cómo mantener un estilo de vida saludable, el 76% en Brasil y el 85% en la India lo aceptarían. Los participantes procedentes del norte de Europa, sin embargo, son más reacios a considerarlo aceptable. En España, solo un 46% se sentiría cómodo con esta monitorización.

Este modelo de valoración dual podría extenderse a otros dispositivos conectados. Un televisor que controla lo que está viendo el consumidor podría costar 100 dólares. El mismo aparato sin función de seguimiento podría costar 500. El «Internet de las cosas», un universo de dispositivos conectados que se estima que se ampliará a más de 20.000 millones de «cosas» de aquí a 2020, convierte está posibilidad en una consideración especialmente pertinente para los fabricantes de bienes de consumo[4].

La cuestión de la disposición de los consumidores a compartir datos personales es esencial para el futuro digital. El debate está abierto. Mientras que para los consumidores españoles la comodidad es más valiosa que el control sobre su intimidad (53%). El estudio indica que, en la gran mayoría de países, entre el 60 y el 87% lo declara al revés. Junto a España, únicamente los participantes de Alemania (66%) dan prioridad a la comodidad. No obstante, el 55% de los participantes a nivel global y, de manera similar, el 56% de los participantes de España, aseguran haber dejado de finalizar una compra online por desconfianza o preocupación ante el potencial uso de sus datos personales. (Figura 5).

Sin embargo, puede ser demasiado tarde para que los consumidores recuperen el control de sus datos personales, incluso aunque quisieran hacerlo. La información personal ya está tan diseminada que sería prácticamente imposible recuperar el control pleno, y dada la aceleración de la tasa de conectividad, solo se ha compartido una fracción de los datos personales que podrían compartirse.

A más largo plazo, es probable que se inste a las empresas a trazar fronteras más claras a la hora de compartir datos personales y que reconozcan abiertamente el valor de los mismos. Hasta entonces, es probable que se trate de una cuestión de gestión y

Figura 4: Acepta la supervisión de su conducción a cambio de una rebaja en el precio de su seguro.

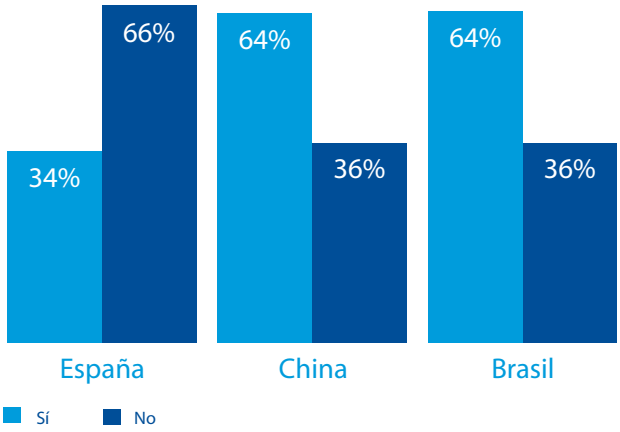
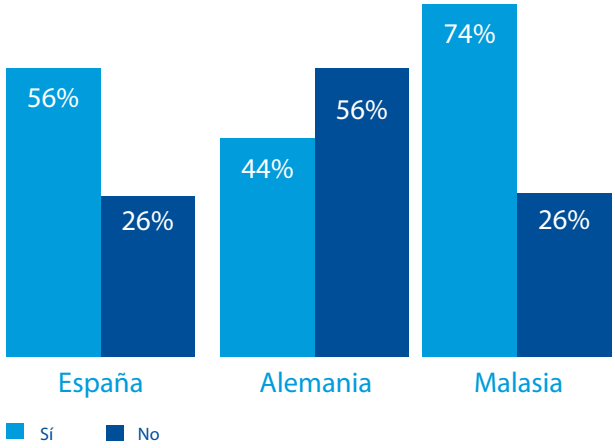


Figura 5: ¿Ha dejado de comprar online por desconfianza ante el tratamiento de sus datos?



4. http://www.gartner.com/newsroom/id/3165317

Reflexiones para ejecutivos: luz roja para los vendedores de datos

Javier Santos
Director de Ciberseguridad en KPMG en España

«Una diferencia de precio en el punto de compra sería, al menos, un agradecimiento abierto a cambio de la recopilación de datos personales. Actualmente, los consumidores tienen que elegir si utilizan o no un servicio basado en una lista larga y complicada de términos y condiciones que casi nadie lee.

Otra posible solución sería un sistema de semáforos sencillo y regulado. A las webs que venden todos los datos personales se les asignaría el rojo; a las que venden solo algunos, el ámbar; y el verde a las que ceden todo el control al consumidor. Los consumidores podrían tomar una decisión informada sobre si están obteniendo una contrapartida justa por sus datos de carácter personal.

Los primeros indicios apuntan a que una mayor transparencia y control desembocan en un intercambio más abierto por parte de los consumidores. En un experimento realizado en Trento (Italia), cientos de familias utilizaron un sistema de intercambio abierto. Su información se almacenó de manera segura y pudieron controlar quién tenía acceso a ella.

Como las familias confiaban en el sistema, finalmente facilitaron mucha más información[5]».

5. With Big Data Comes Big Responsibility (Con los macrodatos llegan las macroresponsabilidades), Harvard Business Review, noviembre de 2014.

El individuo, su privacidad y el papel de las empresas

Javier Aznar
Senior manager, responsable de Privacidad para IT Advisory de KPMG en España

«Como podemos ver a lo largo del presente estudio, el límite se sitúa en torno a la proporcionalidad del uso de los datos en función del motivo por el cual fueron recogidos y la utilización que el responsable del tratamiento hace de los mismos.

Si bien es cierto que dependiendo del país, su organización, estructura, costumbres y raíces culturales, ciertas prácticas pueden ser consideradas en algunos casos aceptables y en otros molestas por los individuos que forman parte de los mismos, no es admisible la solicitud desproporcionada de datos personales, la falta de información sobre los motivos de su tratamiento o incluso la permisividad de consentimientos tácitos en su recolección.

En esta línea el Reglamento Europeo General de Protección de Datos, RGPD, establece ciertos aspectos de manera expresa que marcan una línea claramente apegada a la protección del individuo y de su privacidad: El requerimiento de obtención de un consentimiento explícito y verificable para el tratamiento de los datos recolectados, la ampliación de los derechos del interesado respecto a la portabilidad de los datos o el derecho al olvido, así como la obligación de notificar al interesado, en determinados casos, si sus datos han sido fruto de un acceso no autorizado o brecha de seguridad, contribuyen a redundar esta idea de garantía y protección.

Por último, las empresas deben virar su enfoque en privacidad de la reacción a la prevención, gestionar el riesgo derivado de los tratamientos de datos personales que realizan, analizar los impactos que estos podrían acarrearles y establecer las medidas y salvaguardas necesarias, encontrando el equilibrio para el despliegue de su negocio y el respeto de los límites de la privacidad».

¿Dónde ponen el límite los reguladores?

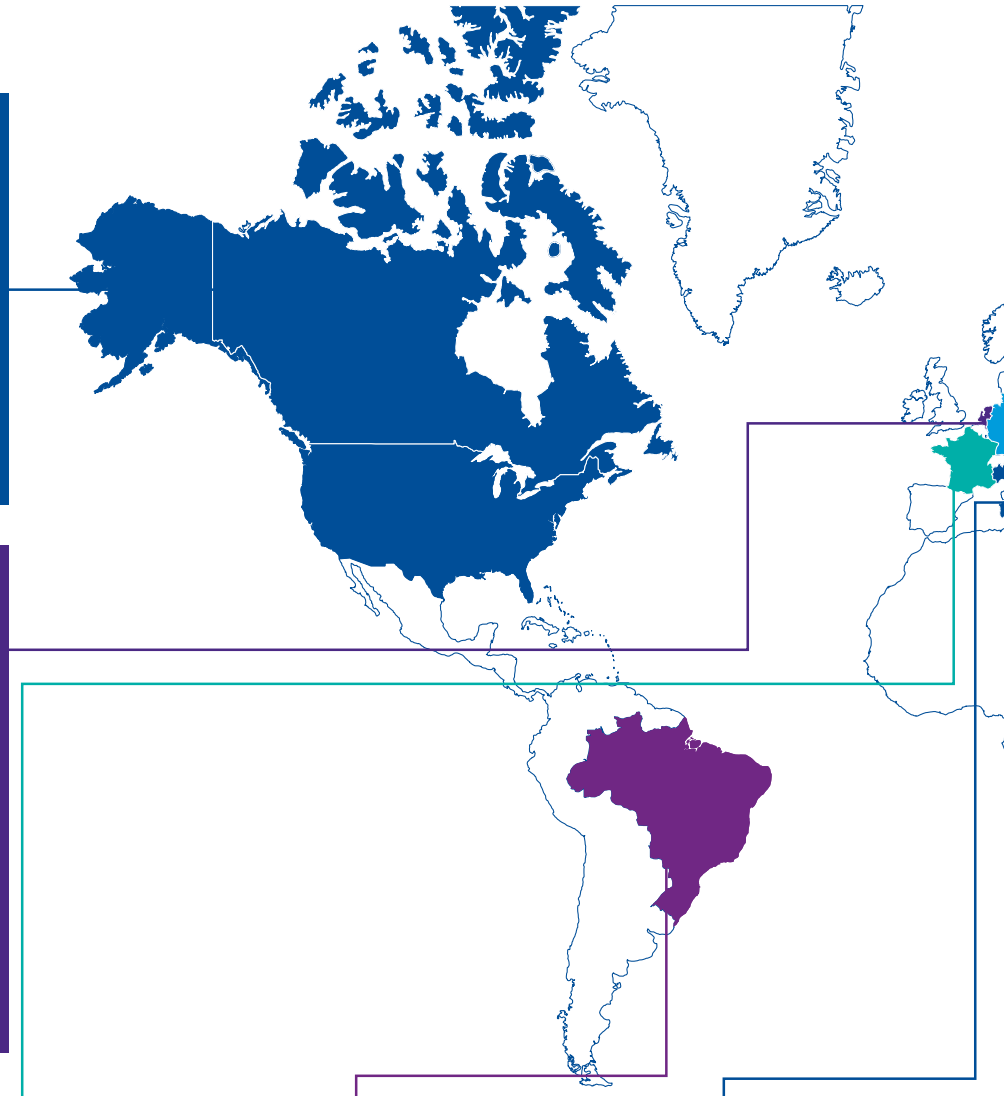
Las organizaciones ya no se pueden permitir postergar la reflexión sobre la privacidad. La ciberseguridad y la batalla contra los hackers lleva mucho tiempo ocupando la agenda del director del área de información (CIO). Pero ciberseguridad no es sinónimo de privacidad.

La nueva normativa de la UE, el Reglamento Europeo General de Protección de Datos (RGPD), supone un cambio fundamental hacia la perspectiva de que la privacidad debe ser la prioridad de las organizaciones en lo referente a los datos de consumidores. Su aplicación a partir del 25 de mayo de 2018 obliga a las empresas a adaptarse a una norma que será directamente aplicable en España aunque todo apunta, según las últimas informaciones de la Agencia Española de Protección de Datos (AEPD) a que nuestra ley se verá modificada.

Aunque la RGPD es quizás el intento más exhaustivo de definir un marco regulatorio coherente en materia de privacidad, Gobiernos de todo el mundo están incidiendo en la cuestión e introduciendo legislación para ofrecer mayor protección a los consumidores; y sanciones más duras en caso de incumplimiento con multas de hasta 20 millones de euros o hasta el 4% de volumen del negocio total anual.

El enfoque más estricto que se está adoptando a escala global eleva la privacidad al primer puesto en los radares de riesgo de las organizaciones. En este entorno de constantes cambios, las compañías tienen que plantearse una nueva actitud respecto de la privacidad; y la necesidad de hacerlo rápidamente a fin de minimizar los riesgos para su balance y su reputación.

Una perspectiva global



Estados Unidos y Canadá

Estados Unidos y Canadá son los dos países más preocupados acerca del robo de datos personales por parte de piratas informáticos. «Dado que en Norteamérica se registran vulneraciones de datos casi a diario, no resulta sorprendente que exista preocupación acerca de los piratas informáticos. El aumento de los litigios y las demandas colectivas, así como el endurecimiento de las sanciones a través de leyes como el GDPR, exigirá que las empresas con sede en Estados Unidos se planteen seriamente sus enfoques a la privacidad" —

Doron Rotman, KPMG en EE. UU

Países Bajos

Los participantes neerlandeses se encuentran entre los menos preocupados por el modo en que las empresas procesan y utilizan sus datos personales. Rusia es el único país cuyos participantes muestran menos preocupación extrema. «Quizás la mentalidad práctica de los neerlandeses tenga mucho que ver en este resultado. Por otra parte, este país se encuentra a la cabeza en lo referente al GDPR, con la ley de notificación de vulneraciones de datos y un organismo de privacidad con potestad para imponer sanciones a partir del 1 de enero de 2016. El aumento de las multas ha hecho que las empresas neerlandesas se apresuren en comunicar vulneraciones de datos y en gestionar la privacidad de forma exhaustiva.» —

Koos Wolters, KPMG en Países Bajos

Francia

Francia es el país que menos dispuesto se muestra a que los organismos públicos recopilen datos personales, aunque sea para contribuir a la lucha contra el terrorismo. «En vista del historial de trágicos sucesos que ha vivido el país, los franceses valoran las leyes sobre privacidad aprobadas por primera vez hace casi cuatro décadas. Esto pone de manifiesto que los Gobiernos han de tener en cuenta las expectativas de privacidad de los ciudadanos al intentar abordar algunos de los desafíos más complejos a los que nos enfrentamos en la sociedad moderna.»

— Vincent Maret, KPMG en Francia

Brasil

En enero de 2015 se presentó un proyecto de ley para la protección de datos de carácter personal. Éste incluye medidas para obtener consentimiento, procesar y transferir datos de carácter personal, comunicar vulneraciones de datos y permitir a los ciudadanos el acceso a sus datos personales. El proyecto de ley contempla sanciones para las infracciones, incluidas multas y la suspensión o prohibición de procesar información personal durante un máximo de diez años.
— Leandro Augusto Antonio, KPMG en Brazil

Italia

Italia es uno de los países más proclives a aceptar que los organismos públicos recopilen datos de carácter personal. «Esto coincide con esa escasa percepción del riesgo de privacidad que tienen los italianos, que puede resultar peligrosa. Al analizar estos resultados nos damos cuenta de que Italia es uno de los países europeos que más redes sociales usa y el menos propenso a preocuparse por el tratamiento que podría darse a sus datos personales al comprar algún artículo por Internet. Aún queda mucho por hacer en cuanto a concienciación sobre privacidad pero, en vista de la gran relevancia que tienen los medios digitales en la sociedad italiana, esta es la única opción.» —

Luca Boselli, KPMG en Italia

Rusia

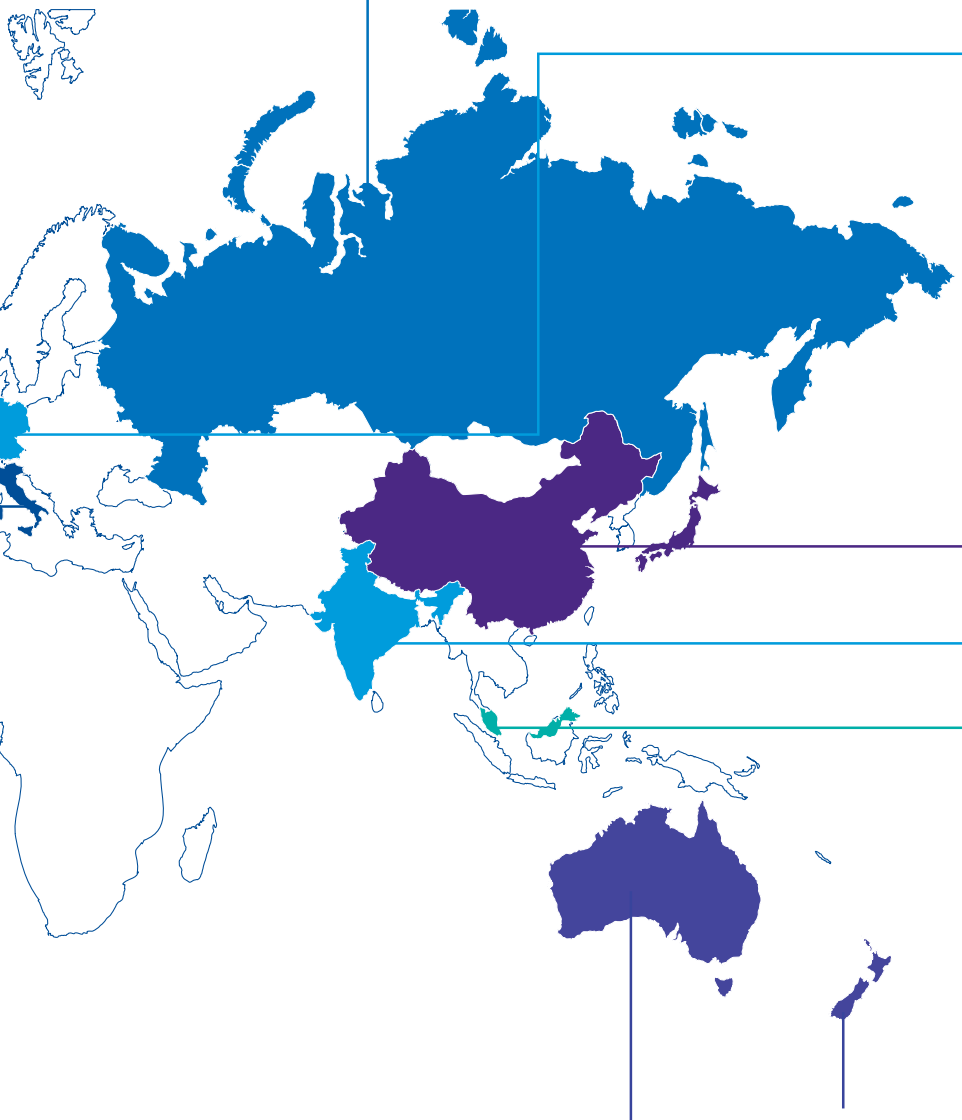
Solo el 11% de los participantes rusos se muestra extremadamente preocupado acerca del modo en que las empresas procesan y utilizan sus datos personales. «Este hecho pone de manifiesto que los rusos no son plenamente conscientes de las consecuencias que tiene una pérdida de datos de carácter personal. Las condiciones de privacidad apenas están despuntando en Rusia y el ciudadano medio de este país es menos consciente de los aspectos técnicos y de sus derechos legales en este ámbito. Además de esto, en Rusia los medios de comunicación no suelen hacerse eco de incidentes vinculados con la privacidad, lo que hace que exista poca concienciación al respecto.» —

Ilya Shalenkov, KPMG en Rusia

Alemania

Los participantes alemanes son de los menos dispuestos a aceptar un dispositivo de seguimiento de fitness gratuito por parte de su empresa. «Este dato no resulta sorprendente, en vista de la tradicional reticencia que muestran los alemanes a compartir información personal. Esto representa un reto real para las empresas alemanas, a medida que avanzan hacia una economía más digital. Estas corren el peligro de quedarse atrás, a menos que logren alcanzar el equilibrio adecuado.» —

Michael Falk, KPMG en Germany



China

En China, el 60% ve con buenos ojos la publicidad personalizada. "Aunque el 60% de los participantes está conforme con la publicidad personalizada, el 39% se muestra extremadamente preocupado sobre el modo en que las empresas procesan y utilizan sus datos personales. Para las compañías que operan en China, está bien visto utilizar innovaciones digitales para acercarse a los clientes, pero la tensión existente entre la confianza y los productos nuevos y emocionantes plantea un auténtico reto.» — Henry Shek, KPMG en China

Japón

Los japoneses son, en general, los menos dados a compartir información con empresas a través de Internet, aunque también son los menos proclives a tomar precauciones para proteger sus datos de carácter personal. «Esto plantea un interesante dilema para las empresas niponas que operan en la red, además de generar una oportunidad de éxito para las firmas que logren el equilibrio adecuado.» —

Atsushi Taguchi, KPMG en Japan

India

«La India es el país que más confía en el procesamiento que las empresas realizan de los datos personales. Al son de la evolución de la economía digital, esta confianza brinda una oportunidad real para crear valor en el mercado indio. No obstante, a medida que existe una mayor concienciación acerca de los problemas de privacidad, cabría esperar un cambio en la confianza y las expectativas de los consumidores indios.» —

Mayuran Palanisamy, KPMG en India

Malasia

«Las empresas asiáticas están apostando fuerte por la revolución tecnológica: está surgiendo numerosas start-ups nuevas y se están registrando abultadas inversiones en iniciativas digitales y de análisis. Garantizar el adecuado tratamiento de la privacidad de los clientes será fundamental para lograr el éxito.» —

Dani Michaux, KPMG en Malaysia

Australia

De los países no europeos, los australianos son los que menos tienden a leer la política de privacidad al acceder a una web. «Esto supone un reto interesante para las compañías australianas. Si, por lo general, los clientes no leen la información que se les facilita, ¿cómo pueden garantizar las empresas su transparencia de cara a estos últimos? Las compañías deberán hallar nuevas vías innovadoras y accesibles para brindar esta transparencia.» —

Jacinta Munro, KPMG en Australia

Nueva Zelanda

Los neozelandeses son los que más tienden a utilizar software de bloqueo de publicidad para proteger sus datos de carácter personal. «Los neozelandeses se toman en serio la privacidad. Las empresas han de plasmar este hecho en todos sus intercambios con clientes.» —

Souella Cumming, KPMG en New Zealand

Una visión sectorial

Sector Público

«Los ciudadanos esperan de los servicios públicos el mismo nivel de calidad, excelencia y desarrollo tecnológico que de las empresas privadas. La innovación rápida y la necesidad de dar respuesta a una ciudadanía conectada abre nuevos retos para las Administraciones públicas también en materia de protección de datos.»

Cándido Pérez Serrano. Socio responsable de Gobierno, Transporte, Infraestructuras y Sanidad de KPMG en España.

Tecnología

«Con el Internet de las cosas, es probable que todo —desde los zapatos hasta los televisores que nos monitorizan cuando están apagados, pasando por las fotocopiadoras— esté conectado a Internet. Abordar la privacidad desde el prisma incorrecto podría acarrear un perjuicio real y considerable para las empresas, además de precisar una labor de subsanación costosa en términos de tiempo y dinero.»

Jorge Santos. Socio responsable del sector de Tecnología de KPMG en España.

Mercados de consumo

«Las empresas, además de invertir constantemente en garantizar la seguridad de los datos de sus clientes, tienen que ser cada vez más sensibles en la captación de datos y mejorar sus planes de privacidad de información, ampliando y mejorando los beneficios y recompensas a sus clientes a cambio de dicha información. Los datos personales son el combustible de la futura economía, por lo que es imprescindible que las empresas pongan el foco en la seguridad de los mismos y en un uso que confiera confianza a los consumidores.»

Carlos Peregrina. Socio responsable de Distribución y Consumo de KPMG en España

Servicios financieros

«Las entidades financieras tienen integrada en su cultura la protección de los activos y la información, además de continuar realizando importantes inversiones de forma prioritaria en este ámbito. El reto al que se enfrentan, y que está siendo estrechamente monitorizado por el BCE como supervisor, es asegurarse de que las áreas en las que invierten brinden la protección que sus clientes esperan, e invertir en las capacidades adecuadas para gestionar el negocio y el perfil de riesgo de forma sostenible. Aquellas capaces de superar estos dos desafíos disfrutarán de una ventaja competitiva para llegar a convertirse en depositarios fiables de los datos de los clientes de cara a prestar servicios adicionales de privacidad e identidad por Internet.»

Francisco Uría. Socio responsable de Sector Financiero de KPMG en España

Energía y recursos naturales

«Actualmente, las compañías energéticas se están adentrando en este ámbito, y nuevas tecnologías como los contadores inteligentes pueden proporcionar información acerca de los clientes a un nivel nunca visto. Crear valor partiendo de este punto resulta fundamental, como también lo es que estas actividades innovadoras no afecten a los negocios principales de la organización y el cumplimiento de normativas como la RGPD.»

Alejandro Rivas-Vásquez. Director, responsable de Ciberseguridad en Energía de KPMG en España

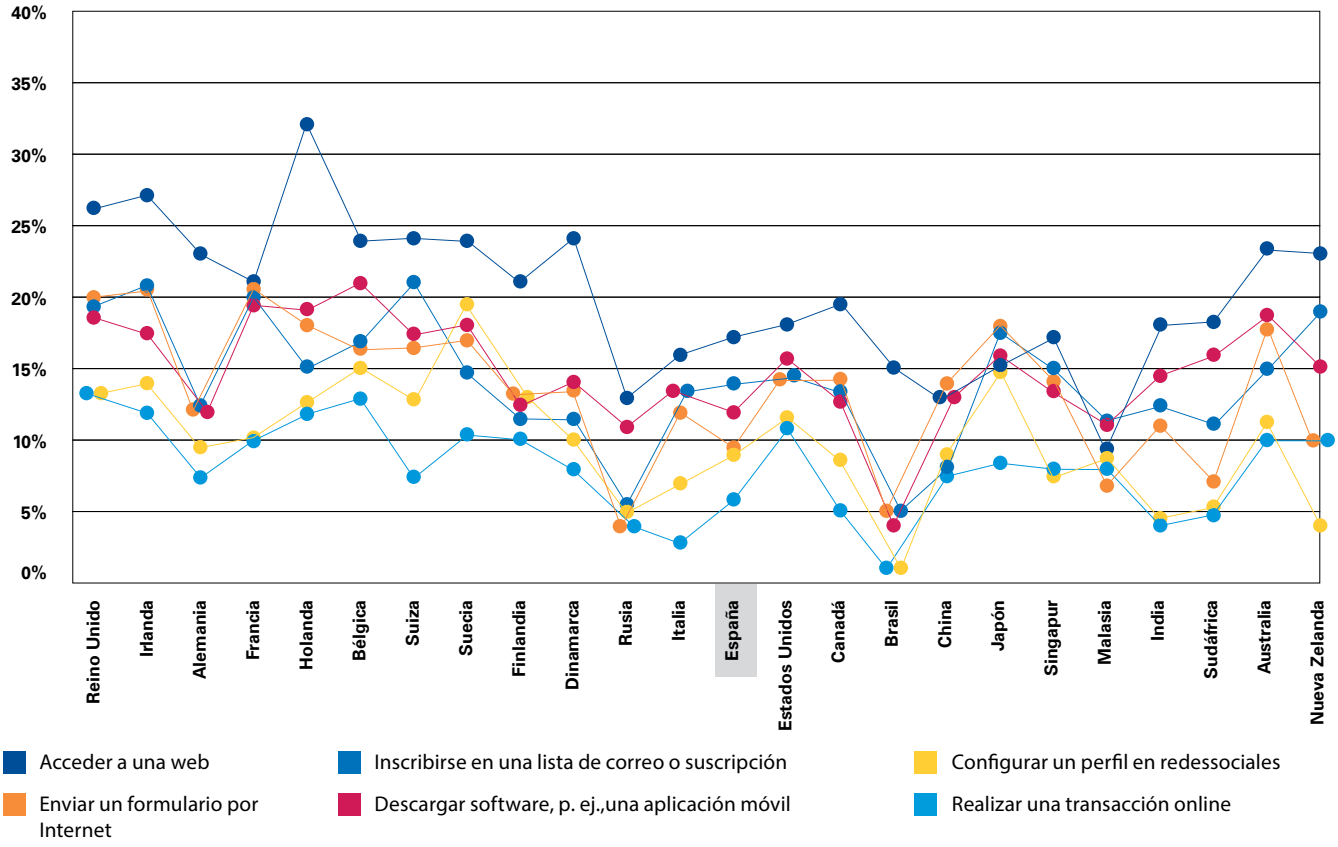
¿Cómo deben adaptarse las empresas?

Uno de los primeros aspectos que ha de abordarse es el de la mentalidad. Lo que podía resultar aceptable o, al menos, tolerable en el pasado, necesita revisarse a la luz del endurecimiento de los enfoques globales a la legislación sobre privacidad.

Obtener el consentimiento de los clientes confundiéndoles con declaraciones legales interminables y disclaimers sobre política de privacidad de veinte páginas no es una estrategia sostenible. Tal y como muestra el estudio, un 20% de los españoles no lee nunca las políticas de privacidad cuando visita webs, cifra que baja hasta el 6% al realizar una transacción. A escala global, el 57% de los participantes no lee las políticas de privacidad cuando visita webs, o lo hace muy por encima. Entretanto, a nivel regional, los europeos parecen ser menos dados a leer las políticas de privacidad que los consumidores de Norteamérica y Asia-Pacífico (Figura 6).

Con todo, la transparencia debería ser el principio rector en lo que respecta a privacidad. Las empresas han de asegurarse de entender plenamente lo que quieren hacer con los datos de los clientes, así como dónde y cómo los almacenan, para luego explicárselo de forma clara y sencilla.

Figura 6: Nivel de exhaustividad con el que los consumidores leen las políticas de privacidad al realizar las siguientes acciones*



* (No lée nunca las políticas de privacidad)

Abordar adecuadamente la privacidad

A las empresas les puede resultar complicado ser transparentes en términos de privacidad ya que desconocen cómo les afectan los reglamentos vigentes o futuros, o porque:

— no tienen una política de privacidad

— recopilan datos de carácter personal según las necesidades

— realmente no saben dónde están los datos.

Si se desconoce su ubicación, es imposible gestionarlos. Además de las listas de clientes de los departamentos de marketing y, ventas, los datos de carácter personal pasan por departamentos como tecnologías de la información (TI), desarrollo de negocio, recursos humanos y finanzas, almacenados posiblemente en cientos de sistemas diferentes que podrían no ser compatibles entre sí.

Podrían estar ubicados en servidores de datos heredados y circular por proveedores, agentes de servicios de pago, auditores, reguladores y decenas de terceros casi sin pensarlo. Es probable que existan, literalmente, miles de deficiencias que subsanar.

Las medidas de localización de datos que suelen incluirse en la nueva oleada de legislación global sobre privacidad también suponen un reto considerable para las empresas. La localización de los datos hace referencia a la obligación de almacenar y procesar tal información dentro de las fronteras nacionales. Dada la creciente dependencia de la informática en la nube (cloud computing) como medio para reducir costes, incrementar la flexibilidad y mejorar la eficiencia, los reglamentos que restringen la localización de los datos podrían fragmentar el mercado global y suponer una desventaja real para los usuarios de Internet.

Las compañías tienen que dar prioridad al tema de la privacidad en sus consejos, así como destinar los recursos adecuados a gestionar su estrategia, sistemas y procesos. De lo contrario, podrían pagar un precio muy alto. Es básico contar con un inventario de datos asociado a una identificación de procesos end to end que traten datos de carácter personal.

Seguridad

A diferencia de en la privacidad, suele ser más sencillo que los altos directivos se centren en la seguridad de los datos. En el estudio, un promedio del 32% de los participantes afirma que unos sistemas de seguridad sólidos representan la medida más efectiva para inspirar confianza, cifra que supera el 40% en España y otros mercados clave como Francia o Malasia. (Gráfico 7).

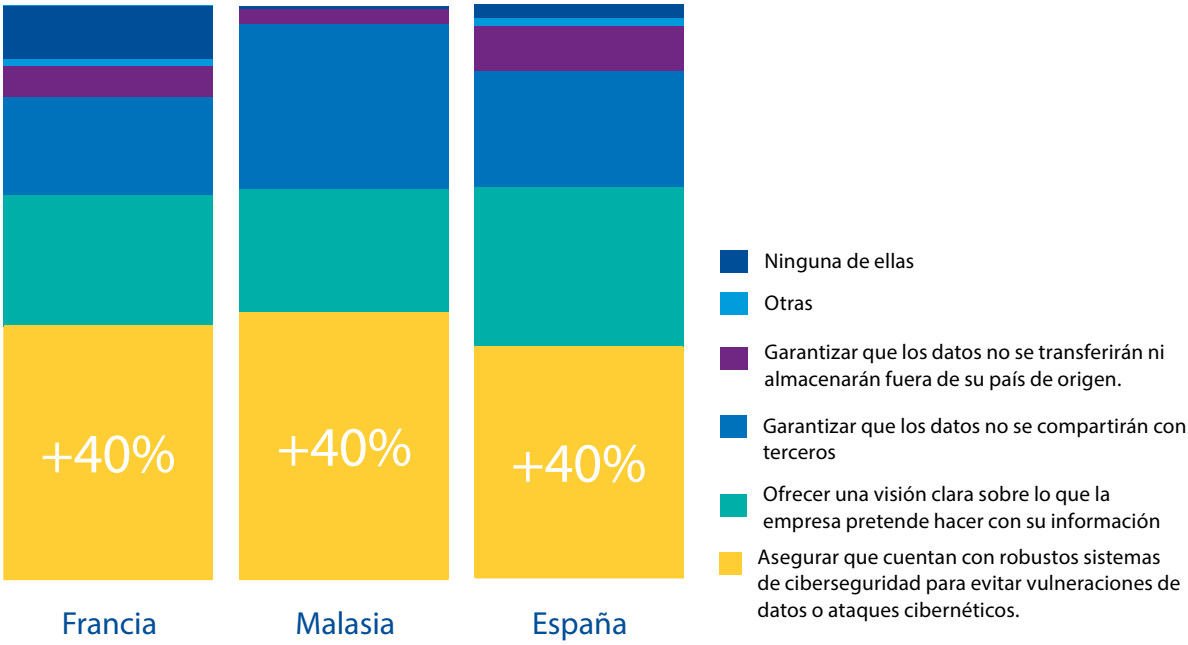
La seguridad, especialmente cuando se vulnera, acapara titulares y, por este mismo motivo, una atención y unos recursos que rara vez se destinan a la privacidad.

No obstante, en realidad, la seguridad es solo uno de los muchos factores que han de tenerse en cuenta en un marco de privacidad exhaustivo. Puede que los sistemas de seguridad de una empresa sean muy sólidos pero ¿se les notifica correctamente a los particulares y se obtiene su consentimiento? ¿Cumple la compañía con las normas en materia de transmisión transfronteriza de datos de carácter personal? ¿Está preparada para los próximos requisitos normativos? Un marco riguroso de gestión de la privacidad está compuesto por muchos otros elementos que han de tenerse en cuenta; la seguridad es solo uno de ellos.

Abordar esto adecuadamente es un enorme desafío global, incluso para un equipo amplio y especializado en privacidad – recurso con el que muy pocas empresas cuentan.

Encarar esta situación exigirá inversión, tiempo, experiencia y conocimientos. Un reto que comienza con la falta de profesionales cualificados y con experiencia en una disciplina que sigue siendo relativamente nueva.

Figura 7: Medida más efectiva para inspirar confianza



Preparados para la privacidad

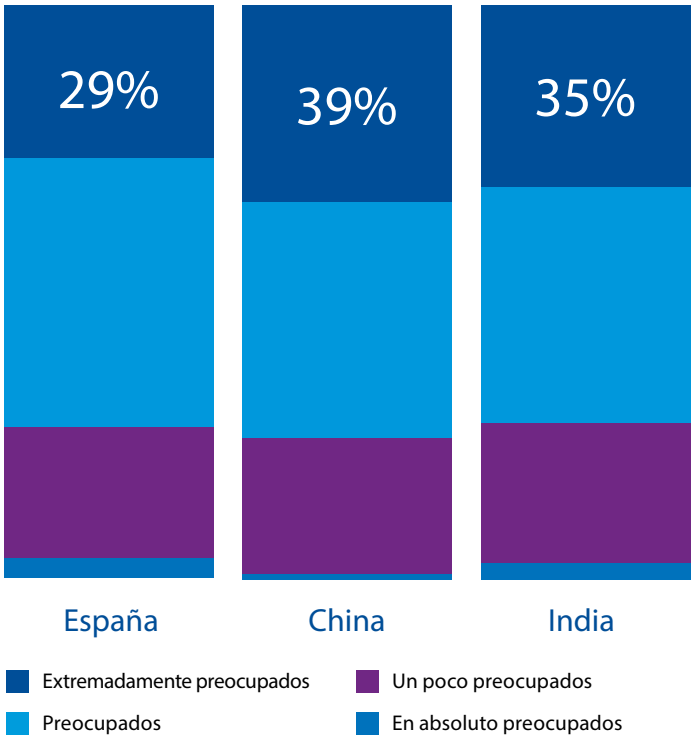
El estudio demuestra que dos tercios de los encuestados españoles están preocupados o muy preocupados acerca del modo en que las empresas procesan y utilizan sus datos de carácter personal, cifra que a escala mundial es del 56% de los participantes. (Figura 8).

Por tanto, es fundamental priorizar la privacidad. Por ejemplo, un fabricante internacional con miles de empleados podría empezar por los datos de sus trabajadores. Por otra parte, para los negocios de cara al cliente, la prioridad debería ser resolver cualquier problema con los datos de sus consumidores.

Si se diseña bien, un marco de privacidad completo no debería verse como un lastre para el marketing y las ventas , sino como una herramienta para ayudar a los negocios a entender mejor a sus clientes, mejorar sus productos y servicios, y adaptarlos a las necesidades específicas de los consumidores.

Independientemente de que lo veamos como una oportunidad o como una amenaza, las empresas han de entender el alcance y la complejidad del problema y actuar con rapidez. La privacidad ha de integrarse en todas las acciones que las empresas llevan a cabo con datos personales, desde el momento en que los recogen y durante todo su ciclo de vida. Puede parecer una labor ardua pero, teniendo en cuenta que las autoridades de todo el mundo les van pisando los talones, cuanto antes se pongan a ello, mejor.

Figura 8: Nivel de confianza en el procesamiento que las empresas realizan de los datos de carácter personal



La privacidad ha de integrarse en todas las acciones que las empresas llevan a cabo con datos personales, desde el momento en que los recogen y durante todo su ciclo de vida.

Próximos pasos

Los datos de carácter personal son el combustible de la futura economía: fuente de ingresos y catalizadores de prosperidad. A medida que el público general va tomando consciencia de la amenaza para su privacidad, están surgiendo nuevos modelos de negocio para abordar las preocupaciones de los clientes, lo que representa tanto oportunidades como retos para las empresas existentes.

Normalmente, disponer de datos personales suele facilitar el desarrollo de tecnologías revolucionarias. Los servicios de trayectos compartidos basados en aplicaciones, por ejemplo, se sirven de las ubicaciones GPS de los usuarios. Como tal, esto sustituye la necesidad de procesos en segundo plano, como introducir manualmente su ubicación, y reduce los costes. No obstante, existe una tensión natural entre los modelos de negocio cimentados sobre los datos de carácter personal y la privacidad de los consumidores.

Dado que el 90% de los españoles siente que tiene un control insuficiente del modo en que las empresas utilizan sus datos personales -el 55% percibe que no tiene ningún control-, ha llegado la hora de que las nuevas tecnologías ayuden a los clientes a recuperarlo[7].

Normalmente, las personas facilitarán sus datos personales siempre que perciban un beneficio claro en ello. Habitualmente esto se traduce en un coste cero o reducido para el consumidor, pero también existen claras ventajas para las empresas. Por ejemplo, en el sector de los servicios financieros, compañías innovadoras como Kreditech[8] en Alemania y Fair Isaac Corporation (FICO)[9] en Estados Unidos están reinventando el análisis crediticio tradicional al utilizar los perfiles online y en redes sociales de las personas para ayudarles a cuantificar su riesgo de crédito. El proceso tradicional en el que se basan los criterios de concesión de préstamos está perdiendo relevancia.

Para los consumidores, utilizar los datos personales es sinónimo de avanzar hacia la economía participativa, en la que los particulares pueden obtener préstamos, seguros o inversiones de otros individuos. A cambio, los inversores potenciales comprueban sus datos de carácter personal, incluidos sus perfiles en redes sociales, antes de prestar el dinero.

El 90% de los participantes españoles considera que tiene un control "insuficiente" del modo en que las empresas utilizan sus datos personales.

7. Privacy and Cybersecurity: Key findings from Pew Research (Privacidad y ciberseguridad: principales conclusiones del estudio Pew), Pew Research Center, 15 de enero de 2015.
8. FT: Kreditech: A credit check by social media (Kreditech: comprobación crediticia a través de las redes sociales), Financial Times, 19 de enero de 2016
9. Forbes: Your social media posts may soon affect your credit score (Sus publicaciones en redes sociales pronto influirán en su calificación crediticia), Forbes.com, 23 de octubre de 2015

La mercantilización de los datos personales

No resulta complicado imaginar un futuro no muy lejano en el que los datos de carácter personal se empaqueten y negocien en el mercado de valores, donde la información sobre los consumidores más acaudalados tendrá mayor valor. Las empresas podrán comenzar a ofrecer productos y servicios a los clientes a distintas tarifas, en función del porcentaje de datos personales que estén dispuestos a compartir.

Un giro en la concienciación

La mayoría de las personas siguen sin ser conscientes de la cantidad de datos personales que las empresas tienen de ellas, ni del efecto que esto podría tener en sus vidas, pero las cosas podrían estar cambiando.

Entre los últimos avances se encuentran aplicaciones que rastrean a los rastreadores. Diseñadas por equipos de académicos estadounidenses, la idea es mostrar a las personas exactamente qué empresas les están siguiendo en Internet[10]. Conocer este tipo de aspectos bien podría concienciar a un elevado porcentaje de la población acerca de cómo se utilizan sus datos personales, además de detectar cualquier vulneración de la privacidad.

Agencias de datos para los consumidores

Otra opción es un «intercambio de atributos de identidad», donde un tercero gestionará los datos personales de un particular en su nombre. Ya hay empresas privadas que buscan ofrecer este servicio. Todavía no existen herramientas y reglamentos suficientemente asentados como para que esto sea real pero, a tenor de la velocidad a la que está teniendo lugar el cambio, podría ocurrir más pronto que tarde.

¿Seguirán tolerando las personas aquellos modelos de negocio que utilizan sus datos personales mientras estén satisfechas con el servicio que reciben a cambio? Resulta complicado imaginar a los principales buscadores o empresas de software perdiendo su posición dominante en el mercado a corto plazo, pero el incremento de los servicios de protección de la privacidad pone de manifiesto el deseo esencial del público de controlar sus datos personales.

A medida que el mercado se va desarrollando, las empresas han de reconocer que proteger los datos de los consumidores no se limita a marcar una casilla para tranquilizar a unos reguladores excesivamente celosos. La concienciación de los clientes y las expectativas del mercado ya han aumentado hasta tal punto que cualquier percepción de falta de seriedad acerca de la protección de datos o de la privacidad no sólo puede mermar la confianza del cliente sino también perjudicar la estabilidad financiera del propio negocio.

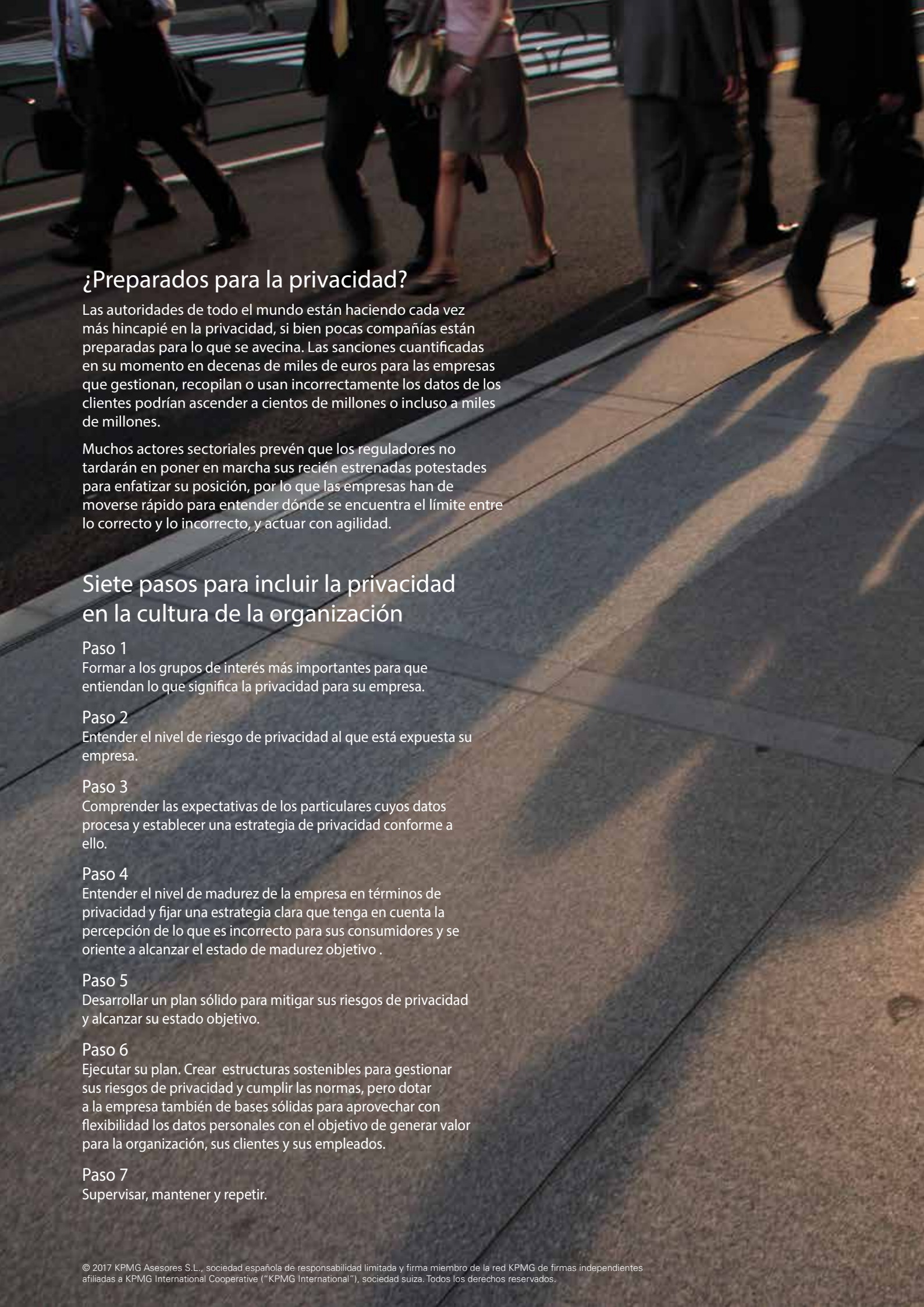
10. Privacy apps to help fight back against companies that track you (Aplicaciones de privacidad para luchar contra las empresas que le rastrean), New Scientist, 25 de noviembre de 2015

Reflexiones para directivos: ¡Quiero un intermediario!

Juan Ignacio Ríos
Manager en IT Advisory experto en Privacidad de KPMG en España.

«A pesar de que aún queda un largo camino por recorrer, cada vez es más habitual que nos encontremos con que el nivel de la concienciación de las personas en materia de privacidad está creciendo. De manera paralela, también la preocupación y las acciones en materia de concienciación en protección de datos de carácter personal en las empresas, crecen con el afán de demostrar a sus clientes que son confiables en estos aspectos.

Por otra parte, ¿Quién sabe si asistiremos en el futuroa la aparición de intermediarios personales que operen directamente con los consumidores?¿Nos imaginamos la posible existencia de una agencia de datos personales que medie entre el particular y las empresas que quieran utilizar sus datos personales? Imagínese que su coche se ha averiado. Podría ponerse en contacto con su agencia de datos (que ya conoce su ubicación, su modelo de coche, matrícula e información bancaria) para que gestionase la recogida y reparación. El modelo de la agencia de datos ofrece a los consumidores un único punto de contacto, con toda la información relevante a la mano, para gestionar el proceso de principio a fin.»



¿Preparados para la privacidad?

Las autoridades de todo el mundo están haciendo cada vez más hincapié en la privacidad, si bien pocas compañías están preparadas para lo que se avecina. Las sanciones cuantificadas en su momento en decenas de miles de euros para las empresas que gestionan, recopilan o usan incorrectamente los datos de los clientes podrían ascender a cientos de millones o incluso a miles de millones.

Muchos actores sectoriales prevén que los reguladores no tardarán en poner en marcha sus recién estrenadas potestades para enfatizar su posición, por lo que las empresas han de moverse rápido para entender dónde se encuentra el límite entre lo correcto y lo incorrecto, y actuar con agilidad.

Siete pasos para incluir la privacidad en la cultura de la organización

Paso 1
Formar a los grupos de interés más importantes para que entiendan lo que significa la privacidad para su empresa.

Paso 2
Entender el nivel de riesgo de privacidad al que está expuesta su empresa.

Paso 3
Comprender las expectativas de los particulares cuyos datos procesa y establecer una estrategia de privacidad conforme a ello.

Paso 4
Entender el nivel de madurez de la empresa en términos de privacidad y fijar una estrategia clara que tenga en cuenta la percepción de lo que es incorrecto para sus consumidores y se oriente a alcanzar el estado de madurez objetivo .

Paso 5
Desarrollar un plan sólido para mitigar sus riesgos de privacidad y alcanzar su estado objetivo.

Paso 6
Ejecutar su plan. Crear estructuras sostenibles para gestionar sus riesgos de privacidad y cumplir las normas, pero dotar a la empresa también de bases sólidas para aprovechar con flexibilidad los datos personales con el objetivo de generar valor para la organización, sus clientes y sus empleados.

Paso 7
Supervisar, mantener y repetir.

Cómo puede ayudar KPMG

Los expertos en privacidad de KPMG en España forman un equipo multidisciplinar entre las áreas de Legal y de IT Advisory, respaldando a nuestros clientes para asesorarles en materia de privacidad a múltiples niveles, desde desafíos muy específicos hasta programas integrales de cumplimiento normativo en sectores complicados y muy regulados.

A continuación figuran algunas de las áreas en las que suelen trabajar nuestros especialistas en privacidad:

— **Evaluación**: brindar una evaluación independiente del riesgo de privacidad y cómo reducirlo.

— **Diseño**: diseñar programas de cumplimiento normativo sobre privacidad.

— **Implantación**: implantar sólidos procesos, políticas y controles de privacidad.

— **Estrategia**: desarrollar estrategias de privacidad pragmáticas y obtener el visto bueno de la alta dirección.

— **Operaciones**: facilitar apoyo continuo para ayudar a los clientes a poner en marcha su marco de privacidad.

— **Seguimiento**: ayudar a los clientes a mantener los sistemas de privacidad y a supervisar los resultados.

— **Terceros**: proyectos encaminados a revisar los niveles de privacidad y seguridad de terceras partes respecto a los datos de nuestros clientes.

¿Cómo puede ayudarle KPMG ante la aplicación inminente de la RGPD?

KPMG puede ayudarle con nuestro Equipo de Privacidad que integra a consultores expertos en IT y a abogados expertos en regulación de protección de datos, llevando a cabo las siguientes actuaciones:

Gap análisis

Realizando un diagnóstico de situación de la empresa o grupo empresarial en materia de protección de datos e identificando los gaps de la organización frente a la nueva norma.

Planificación

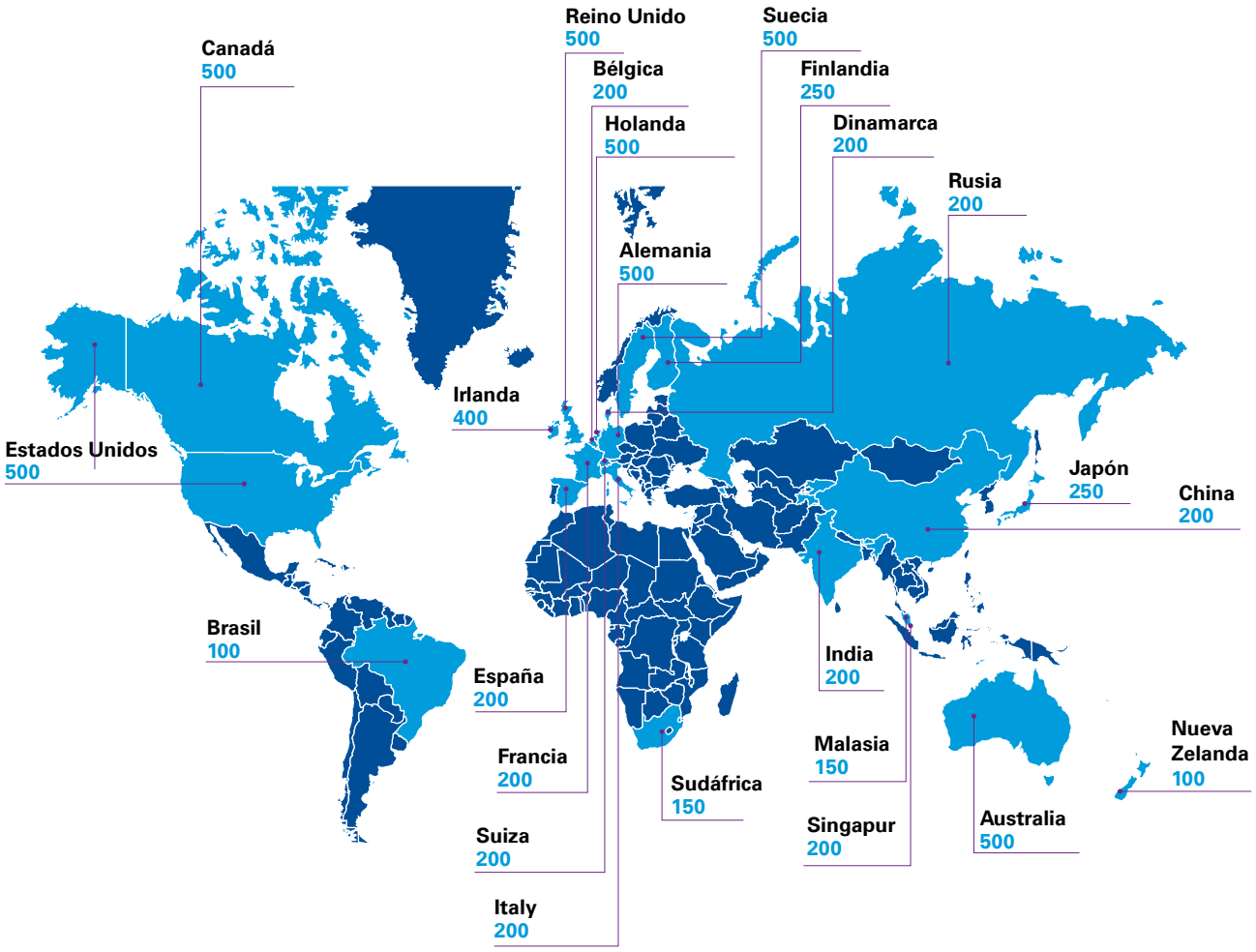
Planificando las necesidades de adaptación y coordinándolas para que sean coherentes y la empresa pueda terminar el proceso de cambio antes de mayo de 2018.

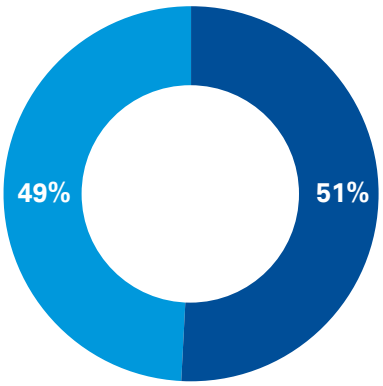
Diseño e implementación

Asistiendo a la empresa en el diseño e implementación de los cambios necesarios: organizativos, de procesos, de soportes documentales, de tecnología, etc.

Sobre el estudio

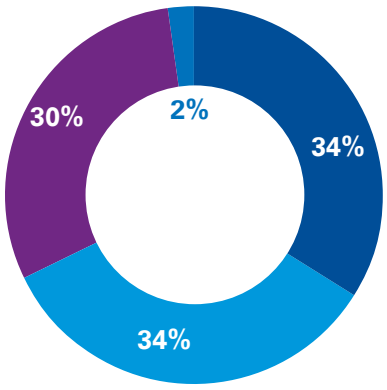
6.900 respuestas de 24 países diferentes:





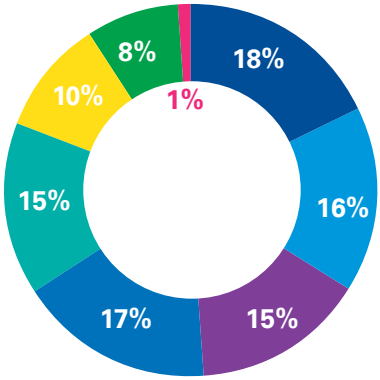
Indique su sexo

	Hombre	(3.451)
	Mujer	(3.449)
	Total	(6.900)



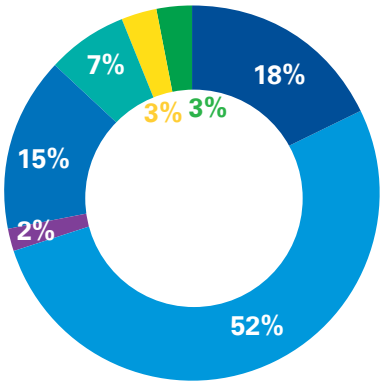
¿Qué edad tiene?

	Millenials	(2.555)
	Generación X	(2.142)
	Babyboomers	(2.009)
	Más de 71	(194)
	Total	(6.900)



¿Cuál de estas etapas vitales le describe mejor?

	Adulto joven sin hijos	(965)
	Familia joven - p. ej., niños en edad preescolar)	(585)
	Familia media - p. ej., con hijos entre 5 y 9 años	(683)
	Familia mayor - p. ej., con hijos entre 10 y 16 años	(811)
	Dependientes mayores - p. ej., hijos a partir de 16 años que viven en casa	(738)
	Nido vacío - hijos que se han independizado	(1.090)
	Adulto(s) sin hijos	(1.762)
	Otros (especifique)	(155)
	Prefiero no contestar	(111)
	Total	(6.900)



¿Cuál de estos estados le describe mejor?

	Soltero/a (nunca me he casado)	(1.792)
	Casado/a	(3.077)
	Pareja de hecho	(230)
	Vivo en pareja	(729)
	Viudo/a, divorciado/a o separado/a y vivo solo/a	(701)
	Con pareja aunque no vivimos juntos	(278)
	Otros	(93)
	Total	(6.900)

Note: Los totales pueden no sumar 100 debido al redondeo

Contactos

Marc Martínez
Socio Responsable de Ciberseguridad
de KPMG en España
E. marcmartinez@kpmg.es

Javier Santos
Director de Ciberseguridad en
KPMG en España
E. javiersantos@kpmg.es

Alejandro Rivas-Vasquez
Director de Ciberseguridad en
KPMG España.
E. arivasvasquez@kpmg.es

Ana López
Directora de Cumplimiento legal,
administrativo y contencioso en el
Área Legal de KPMG Abogados
E. analopez1@kpmg.es

Javier Aznar
Senior manager, responsable de
Privacidad para IT Advisory de
KPMG en España
E. jaznar@kpmg.es

Juan Ignacio Ríos
Manager de Privacidad para IT
Advisory de KPMG en España
E. juanignaciorios@kpmg.es

kpmg.es