



CSA: Conservación, supresión y anonimización

Enfoque para la gestión del riesgo tecnológico en la retención de datos personales.

KPMG Asesores S.L. | Technology Risk

Mayo 2022

Índice

01	Contexto y situación actual de cumplimiento	4
02	Siete retos para las compañías	5
03	Requerimientos normativos y riesgos tecnológicos	6
04	El enfoque de KPMG	7
05	Principales beneficios	9
06	Nuestra experiencia como garantía	10
07	Contacta con nosotros	11

01 Contexto y situación actual de cumplimiento

Hace 4 años que el Reglamento General de Protección de Datos (en adelante, RGPD) comenzó a ser de plena aplicación, después de dar un plazo de dos años a las entidades para adaptarse, desde su entrada en vigor en mayo de 2016. Desde entonces y hasta la fecha, muchas han sido las acciones, reflexiones y planes abordados por las empresas. **Ahora**, hemos llegado a un momento en que **el cumplimiento debe estar más que justificado**, y además, la **cultura de la privacidad** debería haber calado dentro de las organizaciones.

Ya en 2016 algunas organizaciones iniciaron los **procesos de gestión de adecuación**, si bien la mayoría de las entidades **han puesto el foco todos estos años en cumplir con los requerimientos** que tienen un **mayor impacto y visibilidad** a nivel

externo, como es el caso del clausulado y políticas de privacidad para dar cumplimiento al principio de información, adecuación de sitios web, revisión de bases jurídicas del tratamiento y gestión del consentimiento, entre otros.

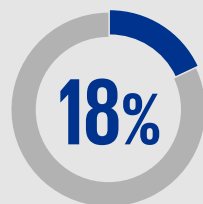
Sin embargo, existen **multitud de requerimientos** de la regulación que, afectando a la parte interna de las organizaciones, no se han abordado con la misma urgencia. Sí que se ha configurado como uno de los puntos de preocupación los registros de actividades, evaluaciones de riesgos e impactos, pero hay otros aspectos que no.

El cumplimiento del principio de limitación de la conservación, el derecho de supresión y el bloqueo de datos personales son varias de las exigencias del RGPD y de la Ley Orgánica de

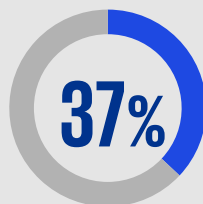
Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo, LOPDGDD) que aplican en la última fase del ciclo de vida de los datos. Estos puntos generan mayor dificultad de implementación efectiva en la práctica.

KPMG ha realizado un estudio con otras oficinas de la **red internacional** para verificar el **nivel de cumplimiento** y preocupación de nuestros clientes con respecto a la **implementación** de la conservación, supresión y anonimización.

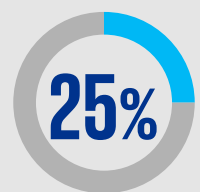
Los resultados de KPMG nos muestran que:



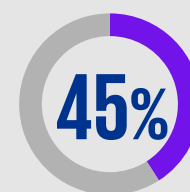
De los países de la muestra se encuentran en niveles de cumplimiento efectivos.



De los países de la muestra se encuentran en fase de diseño.



De los países de la muestra llegan a borrar/anonimizar datos personales.



De los países de la muestra tiene políticas desarrolladas si bien no cumple de manera efectiva.

02 Siete retos para las compañías

Desde KPMG se cuenta con un buen conocimiento de esta situación a la que muchas compañías se enfrentan día a día y por ello entendemos que el nivel de cumplimiento en la última fase del ciclo de vida de los datos, deriva de los **desafíos a los que se tienen que enfrentar las compañías**, tanto técnicos como organizativos, para poder implementar soluciones en la práctica.



03 Requerimientos normativos y riesgos tecnológicos

Los **requerimientos** con los que deben cumplir las organizaciones para **garantizar el principio de limitación del plazo de conservación y la supresión** de los datos personales son **altamente exigentes**, pero los riesgos derivados de su incumplimiento son igualmente relevantes:

Requerimientos normativos

- Cumplimiento del **principio de limitación del plazo de conservación**, explotando los datos sólo durante el tiempo necesario y cuando sea lícito:
 - Consentimiento.
 - Contrato o medidas precontractuales.
 - Interés legítimo o público.
 - Obligación legal.
 - Intereses vitales.
- El **bloqueo de los datos personales**, obligatorio (en España), cuando se proceda a la supresión de estos, entendido como la cuarentena de los datos, adoptando medidas para impedir su tratamiento, excepto a solicitud de Jueces y Tribunales, el M. Fiscal o la Administración competente. Transcurrido el plazo legal oportuno, se deberá proceder al borrado de los datos.
- El **borrado o anonimización** de los datos será obligatorio cuando:
 - Finalice el plazo legal de conservación.
 - Un interesado presente una solicitud de borrado que cumpla con la normativa*.
 - Se alcance la finalidad del tratamiento*.
 - Se carezca de base legal*.

(*Siempre que no exista la obligación legal de conservar los datos bloqueados).

Riesgos tecnológicos

- **Sanciones de protección de datos y reputación negativa en el mercado** al carecer de un proceso de conservación, supresión y anonimización efectivo. Las sanciones y el incumplimiento de las obligaciones del RGPD y de la LOPDGDD pueden suponer una reputación negativa para la compañía generando desconfianza de cara a sus clientes, proveedores y otros actores e interlocutores.
- **Aumento de la superficie de ataque** al conservar más información y datos de los realmente necesarios. Cuanta más información se almacena en la organización, y más disgregada se encuentre esta, existirán más puntos de ataque.
- **Aumento de costes de almacenamiento**. Al almacenar datos innecesarios y mantener información no actualizada, será necesario contar con más almacenamiento tanto físico como digital, con los costes asociados que supone.
- **Duplicidad de información, desactualización e integridad de la misma**. La falta de control de la información almacenada puede redundar en la duplicidad de la información, su desactualización y en definitiva afectando a su integridad.
- **Acceso no autorizado a la información**. El volumen descontrolado de información supondrá mayor riesgo en el acceso no autorizado a la misma.

04 El enfoque de KPMG (1-2)

La metodología de trabajo es propia de KPMG y ha sido compuesta a partir de guías y documentos de autoridades así como de la experiencia adquirida realizando este tipo de trabajos en nuestros clientes:



Metodología para la Conservación, Supresión y Anonimización de dato personales, en adelante CSA, una metodología propia de KPMG

Para abordar el cumplimiento de la conservación, supresión y anonimización de datos personales en la última fase del ciclo de vida del dato, **KPMG** cuenta con una **metodología de trabajo propia** denominada **metodología CSA**. Dicha metodología es fruto del análisis de los criterios de las **autoridades** y organismos referentes en materia de protección de datos y privacidad, **ejercicios de benchmarking** con clientes y oficinas de KPMG en otros países así como de la **experiencia adquirida** en la ejecución de este tipo de proyectos.



Marco de trabajo flexible

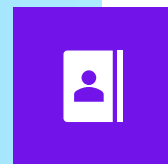
Dentro de nuestro **marco de trabajo**, se contemplan diferentes **niveles de implementación** (política, diseño y efectividad). En función del **escenario de partida** en cada organización y sus necesidades, las **fases de trabajo y los ejercicios a realizar** serán diferentes.

Aunque las actividades varíen en función del escenario, el objetivo será común e irá orientado a perseguir la implementación de un programa que cumpla con la **conservación, supresión y anonimización** de datos personales.



La tecnología es tu mejor aliado

Implementar la tecnología y las técnicas correctas, adaptadas a la organización y a sus sistemas y aplicaciones. Prestamos soporte en la **selección de las herramientas** que mejor se adapten a las necesidades de la compañía y que faciliten los procesos de conservación, supresión y anonimización de datos personales. En los casos en los que la entidad tiene capacidades para realizar **desarrollo interno**, acompañamos a los equipos durante el diseño, **desarrollo y puesta en marcha de la solución**.



Foco en personas y procesos

Implicar, coordinar y formar a las áreas y grupos de trabajo involucrados será clave para poder impulsar este tipo de proyectos.

Además se deberá también poner el foco **en identificar los flujos de los datos** así como en las necesidades de la entidad y de los negocios y operaciones de la misma.

04 El enfoque de KPMG (2-2)

La aplicación de nuestra metodología de trabajo para la **conservación, supresión y anonimización** redunda en los siguientes grupos de actividades y resultados:



Algunos ejemplos de actividades

- | | | |
|---|--|---|
| <ul style="list-style-type: none">▪ Revisión de capacidades.▪ Identificación del escenario de partida.▪ Revisión de normativa implantada en la organización.▪ Diseño de requisitos y planes de acción.▪ Seguimiento de los desarrollos. | <ul style="list-style-type: none">▪ Revisión de obligaciones locales, como por ejemplo el bloqueo en España.▪ Identificación de sistemas y datos personales.▪ Estudio y revisión de plazos de retención y plazos legales de conservación.▪ Estudio de criterios de autoridades. | <ul style="list-style-type: none">▪ Políticas de retención de datos personales.▪ Cumplimiento normativo de obligaciones propias de conservación, supresión y bloqueo.▪ Implementación de plazos de retención en sistemas y marcado de los mismos.▪ Limitación del acceso a la información. |
|---|--|---|

Nuestro marco de trabajo es flexible y adaptable a la situación de partida de nuestros clientes.

05 Principales beneficios

¿Qué beneficios aporta nuestro enfoque?

Gracias a KPMG y a su amplia experiencia en este tipo de proyectos, podrás obtener los siguientes beneficios:

Mayor nivel de cumplimiento normativo

Ahorro en costes

Reputación positiva en el mercado

Automatización y eficiencia de procesos

Reducción de superficie de ataque

Mayor control / gestión del riesgo

Cumplimiento del principio de responsabilidad proactiva

Servicio de monitorización continua para verificar efectividad y cumplimiento

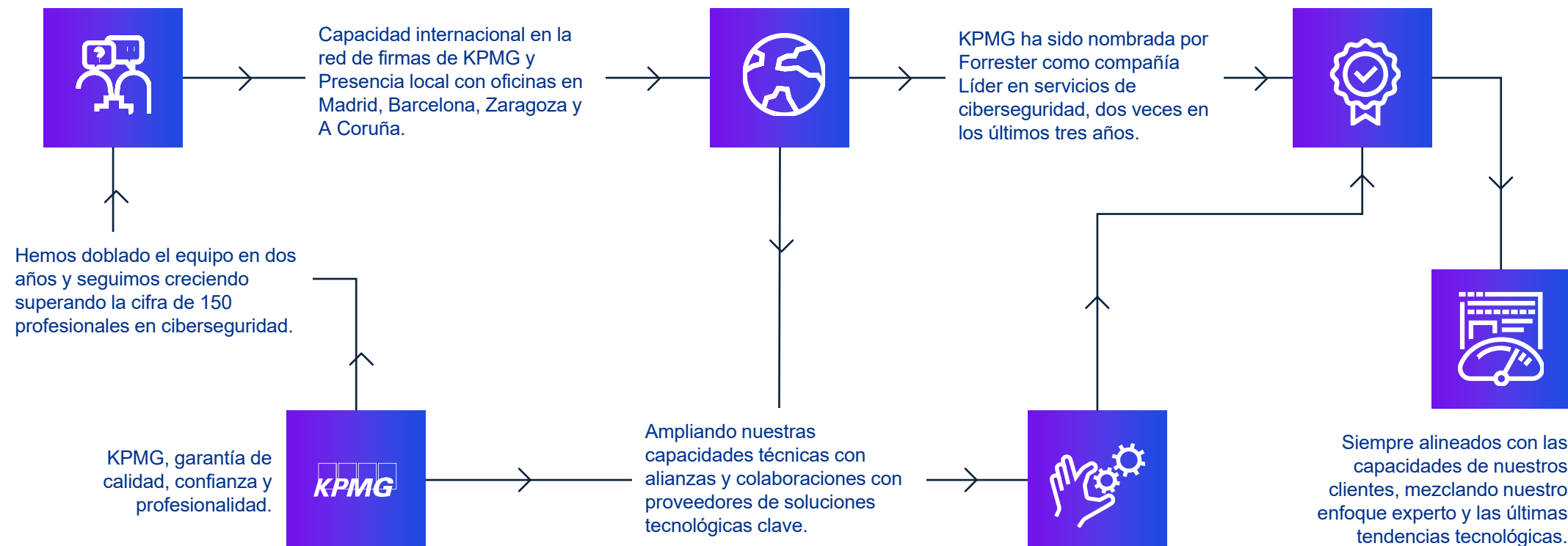
Seguridad y Privacidad desde el Diseño

Conservación, supresión y anonimización

06 Nuestra experiencia como garantía

¿Qué te aportamos?

Contamos con la experiencia suficiente para darte la confianza y confortabilidad a la hora de acompañarte durante todo el proceso de gestión de la última fase del ciclo de vida de los datos personales:



07 Contacta con nosotros



Javier Aznar

Socio
KPMG España
Technology Risk
T: 699350029
E: jaznar@kpmg.es



Ana de la Higuera

Manager
KPMG España
Technology Risk
T: 679 676 138
E: adelahiguera@kpmg.es



Ángela Manceñido

Senior
KPMG España
Technology Risk
T: 628614910
E: amancenido@kpmg.es



kpmg.es

La información aquí contenida es de carácter general y no va dirigida a facilitar los datos o circunstancias concretas de personas o entidades. Si bien procuramos que la información que ofrecemos sea exacta y actual, no podemos garantizar que siga siéndolo en el futuro o en el momento en que se tenga acceso a la misma. Por tal motivo, cualquier iniciativa que pueda tomarse utilizando tal información como referencia, debe ir precedida de una exhaustiva verificación de su realidad y exactitud, así como del pertinente asesoramiento profesional.

© 2022 KPMG Asesores S.L., sociedad española de responsabilidad limitada y firma miembro de la organización global de KPMG de firmas miembro independientes afiliadas a KPMG International Limited, sociedad inglesa limitada por garantía. Todos los derechos reservados.

KPMG y el logotipo de KPMG son marcas registradas de KPMG International Limited, sociedad inglesa limitada por garantía.