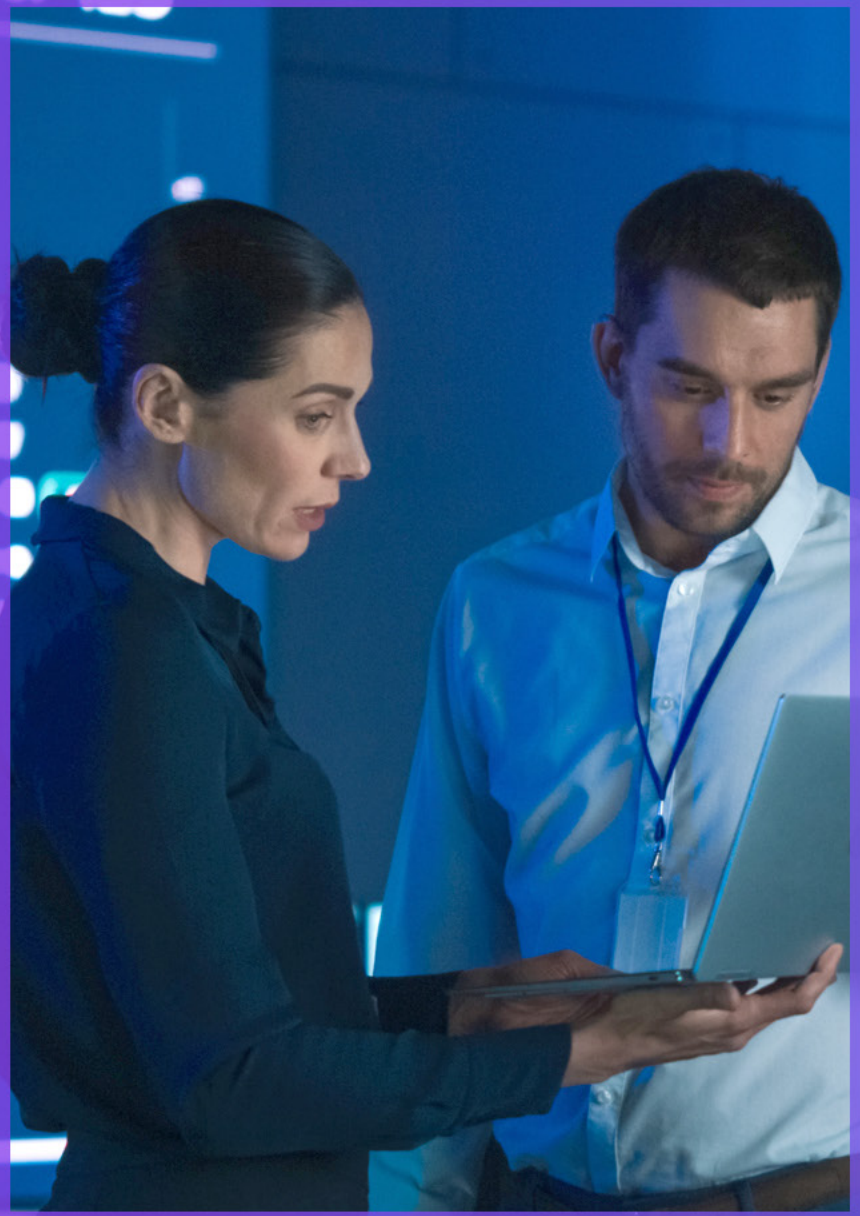


# CSA: Conservación, supresión y anonimización

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

**KPMG Asesores S.L.**

2025

—

kpmg.es

# Contenido

# Contexto

01

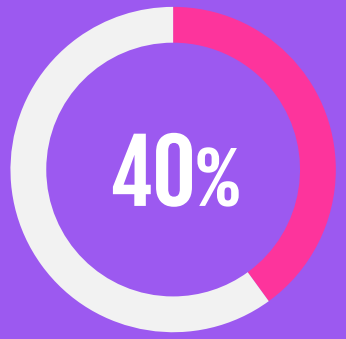
# Estado del arte en Europa

Los requisitos relacionados con el cumplimiento de limitación de conservación, bloqueo de datos y gestión de su supresión, siempre se ha identificado como uno de los retos a los que se enfrentan los responsables de privacidad dentro de una organización.

## ¿En qué situación están las organizaciones?

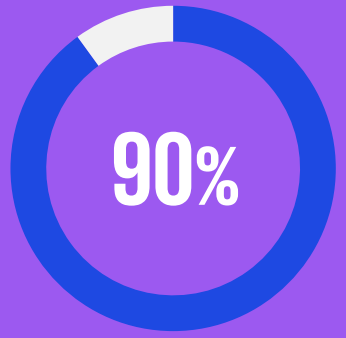
**KPMG ha realizado un estudio con otras oficinas de la red internacional para verificar el nivel de cumplimiento y preocupación de nuestros clientes con respecto a la implementación de la conservación, supresión y anonimización.**



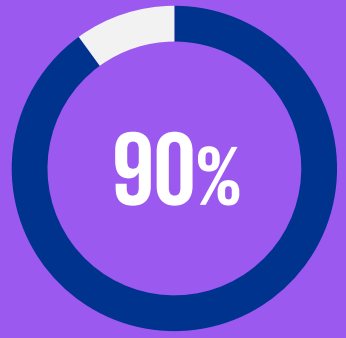



**De los países de la muestra se encuentran en niveles de cumplimiento efectivos.**


**De los países de la muestra dan prioridad a la aplicación de técnicas de borrado vs. anonimización.**




**De los países de la muestra han establecido mecanismos para aplicar bloqueo / restricción sobre los datos.**




**De los países de la muestra tiene políticas desarrolladas si bien no todos cumplen de manera efectiva.**

# Retos para las compañías

02

- Cumplimiento de normativas de diferentes países
- Cambio continuo de la tecnología y dependencias tecnológicas
- Falta de presupuesto
- Falta de concienciación de los equipos técnicos y de negocio
- Granularidad para aterrizar requisitos
- Necesidades de negocio vs. Requisitos legales de conservación

# Requerimientos normativos y riesgos tecnológicos

03

# 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 del a información, su desactualización y en definitiva afectando a su integridad.

Acceso no autoridado a la información. El volumen descontrolado de información supondrá mayor riesgo en el acceso no autorizado a la misma.

# El enfoque de KPMG

04

# 04. El enfoque de KPMG

Desde KPMG se ha trabajado en un **modelo de Gobierno del dato personal** que enmarca diferentes obligaciones en materia de privacidad, que habitualmente suponen un reto para las organizaciones: cumplimiento en materia de **conservación**, **supresión y anonimización** de datos personales, localización de **los datos personales** o correcta **gestión de derechos** de los interesados, entre otras.

Aunque este servicio parte de establecer un **marco teórico**, el principal objetivo es **aterrizar estos requisitos legales** en la realidad de una organización para alcanzar un **cumplimiento efectivo** de los mismos en sus sistemas de información, siempre con un **enfoque alineado** a la **optimización y automatización** de procesos de privacidad dentro de la organización.

## 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.

Nuestra metodología y enfoque de trabajo se centran en abordar desde el inicio de los tratamientos de datos, implementación o desarrollo de sistemas, un **modelo de gobierno integral de los datos personales que se tratan dentro de la organización**. Esta metodología se basa en la **involucración de todas las áreas implicadas en el cumplimiento de las obligaciones de protección de datos que favorecen y permiten el correcto gobierno del dato personal**. **Personas, procesos y tecnología serán los tres vectores sobre los que preparar todo el modelo de gobierno**.

- Personas
- Procesos
- Tecnología

## 01 Estudio y recopilación de necesidades — 02 Cómo ayudamos a nuestros clientes — 03 Qué resultados obtendrán nuestros clientes

### Algunos ejemplos de actividades

- **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.**

- **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.**

- **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.**

# Principales beneficios

05

# ¿Qué beneficios aporta nuestro enfoque?

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

- Mejorar el nivel gobierno del dato personal
- Ahorro en costes
- Reputación positiva en el mercado
- Automatización y eficiencia de procesos
- Independencia de las áreas técnicas y de negocio en el cumplimiento de la privacidad
- Mayor control / gestión del riesgo
- Cumplimiento del principio de responsabilidad proactiva
- Servicio de monitorización continua para verificar efectividad y cumplimiento
- Modelo de cumplimiento global y transversal dentro de la organización
- Conservación, supresión y anonimización

# Equipo y experiencia como garantía

06

# En KPMG somos diferenciales

Adicionalmente, nos mantenemos en constante formación, crecimiento y evolución, para trabajar en definir las mejores metodologías y enfoques de trabajo adaptadas a las novedades regulatorias y tendencias en privacidad.

## Privacy for IA

Con el objetivo de **integrar las obligaciones de IA** y **protección de datos** en los procesos desarrollados, utilizando la **metodología TrustedAI** y promoviendo la **privacidad desde el diseño** con un enfoque end-to-end para facilitar la implementación.

## Optimización y mejora

Fomentando el uso de la **metodología Power Privacy** para cubrir el ciclo completo de protección de datos y **agilizando** las **tareas del DPO con tecnología o soluciones que mejoren el rendimiento**. El enfoque cuenta con una parte agnóstica y otra diseñada con OneTrust.

## Certificaciones (Europrivacy)

**Reconocida** en la UE y **adaptable** a regulaciones específicas, **permitiendo identificar riesgos** anticipadamente. Certifica actividades de tratamiento, demostrando **conformidad con el RGPD**, entre otros beneficios.

## Presencia en foros de referencia

Nuestro equipo participa activamente en foros del sector a nivel nacionales e internacional como **ISMS Forum** o acciones de la **IAPP**.

## Coliderazgo del grupo global de privacidad de KPMG

Desde hace un **tiempo lideramos** este grupo interno permitiéndonos estar a la última en nuestro sector.

## Nos apoyamos en tecnología para la gestión

Nuestras **alianzas** con **líderes tecnológicos** nos permiten ofrecer **servicios innovadores** que fortalecen la protección de datos y optimizan los procesos. Esto nos posiciona como socios tecnológicos de confianza.

## Somos líderes en servicios de privacidad

La confianza y satisfacción de nuestros clientes nos avalan. Nuestro enfoque **personalizado y la calidad** de los servicios consolidan nuestra posición en el mercado.

## Nuestro equipo está certificado y formado

Nuestro equipo de más de **40** consultores **expertos en privacidad** está **certificado y formado** (CIPPE, DPO, ISO27001 etc).

## Actualización periódica de buenas prácticas y qué hacen otros clientes

Contamos con la posibilidad de ofrecer update periódico sobre para compartir las **novedades del mercado y qué están haciendo otros clientes**.

# Presencia de KPMG Privacidad

Experiencia con normativas locales de diversos países

Áreas de protección de datos en más de 60 países

Marco de control transversal que cubre normas locales

# Contacta con nosotros


**Javier Aznar**
Socio,
Technology Risk
Ciberseguridad y Privacidad
KPMG Asesores S.L.
jaznar@kpmg.es

**Ángela Manceñido**
Manager,
Technology Risk
Privacidad y Riesgo Tecnológico
KPMG Asesores S.L.
amancenido@kpmg.es

**María Cristina Köhler**
Manager,
Technology Risk
Privacidad y Riesgo Tecnológico
KPMG Asesores S.L.
mariacristinakohler@kpmg.es


**kpmg.es**