Junta de Andalucía

Metodología corporativa para la gestión del riesgo de protección de datos y la responsabilidad proactiva en la Junta de Andalucía

Entidad solicitante: Consejería de Justicia, Administración Local y Función Pública - Junta de Andalucía – Secretaría Generar para la Administración Pública (SGAP) - Coordinación para la Transformación e Innovación de la AAPP y Protección de datos

AEPD – Premios a las buenas prácticas de cumplimiento normativo y de responsabilidad social en el tratamiento de datos. Modalidad B – Sector público

Fecha: 30/01/2026

Listado de acrónimos

AAPP: Administraciones Públicas

ARPD: Análisis de Riesgos de Protección de Datos

AEPD: Agencia Española de Protección de Datos

CMMI: Capability Maturity Model Integration

DPD: Persona que ostenta el rol de Delegado de Protección de Datos

EIPD: Evaluación de Impacto de Protección de Datos

ENS: Esquema Nacional de Seguridad

LOPDGDD: Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales

RAT: Registro de Actividades de Tratamiento

RGPD: Reglamento General de Protección de Datos

RPS: Registro de Procedimientos y Servicios

SGAP: Secretaría General para la Función Pública

Tabla de ilustraciones

Contenido

1. Resumen ejecutivo (ampliado)

1.1. Contexto y problema público abordado

La Junta de Andalucía gestiona tratamientos de datos personales en un ecosistema administrativo de gran tamaño y heterogeneidad, con múltiples órganos, entidades instrumentales y sistemas de información que soportan servicios públicos esenciales (salud, justicia, servicios sociales, educación, empleo, entre otros) para una población de 8,7 millones de habitantes.

En este contexto, la salvaguarda de los derechos fundamentales, entre los que se encuentra **protección de datos personales** no puede sostenerse eficazmente mediante un enfoque puramente documental o reactivo, sino que exige un modelo operativo, corporativo y sostenible que incorpore el **enfoque basado en riesgos** que establece el Reglamento General de Protección de Datos (RGPD)) y que pueda adaptarse a las evoluciones tecnológicas, organizativas y técnicas que afecten, en última a instancia a la información personal.

Para ello, se han ido abordando progresivamente actuaciones relacionadas con la adecuación y cumplimiento normativo, si bien con anterioridad a este proyecto, la organización afrontaba retos recurrentes y comunes en administraciones complejas:

- **Dispersión de criterios** en la identificación y descripción de tratamientos.
- **Heterogeneidad** en la elaboración y mantenimiento del Registro de Actividades de Tratamiento (RAT), con diferentes niveles de agregación y enfoques por unidades, entidades o centros directivos.
- **Dificultad real** para aplicar el enfoque de gestión del riesgo de manera homogénea, trazable y revisable (más allá del cumplimiento formal).

A estos retos se añade una exigencia creciente de la ciudadanía en relación a la **transparencia, claridad y confianza** en cómo la Administración trata los datos personales, especialmente cuando están implicadas categorías especiales de datos y colectivos en situación de vulnerabilidad.

En este escenario, la Junta de Andalucía decidió abordar la protección de datos desde un enfoque de **responsabilidad proactiva**: diseñar e implantar un marco de gobernanza corporativo que permita **tomar decisiones informadas y justificadas**, demostrar evidencias de cumplimiento, y establecer ciclos de mejora continua basados en medición y resultados.

Esta actuación se enmarca dentro del marco del I Plan Estratégico de Protección de datos de la Junta de Andalucía 2024-2030, aprobado por Acuerdo de 13 de Noviembre de 2024, de la Comisión Interdepartamental de Racionalización Administrativa (CICRA)).

1.2. Objetivos estratégicos del proyecto

El proyecto presentado tiene como finalidad consolidar un modelo corporativo de cumplimiento efectivo del RGPD, que sea aplicable en todo el conjunto de organismos y

entidades que componen la Junta de Andalucía con independencia del grado de madurez de cada centro directivo o entidad, constituyéndose como una herramienta teórico-práctica que de manera eficaz impulse una mejora continua en el manejo y gestión de los datos personales.

El objetivo general es implantar una **metodología corporativa de análisis de riesgos y evaluación de impacto** que integre como un ciclo completo el RAT, el análisis y la evaluación del riesgo y la toma de decisiones documentadas, de forma **homogénea, reutilizable y sostenible** en el tiempo.

Adicionalmente permite conseguir otros objetivos específicos tales como:

1. **Homogeneizar criterios** para identificar, describir y publicar tratamientos en el RAT, evitando enfoques erróneos (p. ej., confundir tratamientos con procedimientos o con sistemas) y estableciendo una serie de buenas prácticas y criterios orientadores que ayuden a los responsables del tratamiento.

2. Integrar el **análisis de riesgos** como parte de la gestión ordinaria, con una metodología común, escalable y alineada con el RGPD y la LOPDGDD, apoyando con recursos y buenas prácticas.

3. Determinar de forma objetiva y trazable **cuándo procede llevar a cabo una evaluación de impacto de protección de datos (EIPD)**, en función del riesgo inherente y de los supuestos establecidos por la normativa y la doctrina de autoridades de control.

4. Facilitar la **toma de decisiones administrativas**: justificar medidas, priorizar acciones de mitigación, y definir planes de tratamiento del riesgo con seguimiento.

5. Reforzar la **transparencia y la confianza** ciudadana mediante un RAT coherente, publicable y mantenible, separando claramente la información para publicación de la destinada a control interno.

6. Consolidar una cultura organizativa de privacidad mediante **acompañamiento, formación y mejora continua**, acercando a la práctica la metodología desarrollada e incorporando métricas e indicadores sobre su implantación.

1.3. Solución corporativa adoptada: metodología + herramientas + gobernanza

La solución se articula como un **sistema integral** que conecta, de forma coherente, los elementos clave de la responsabilidad proactiva:

1) Eje "RAT–Riesgo–EIPD–Decisión–Seguimiento"

La metodología corporativa establece un proceso operativo que enlaza:

- Identificación y documentación del tratamiento (RAT)
- Análisis de riesgos de protección de datos (ARPD)
- EIPD cuando proceda

- Decisiones documentadas (medidas, prioridades, planificación)
- Seguimiento y revisión periódica (mejora continua)

Este enfoque evita la fragmentación y convierte el RAT en el punto de partida para un cumplimiento real: no se trata solo de "describir", sino de gestionar los tratamientos como verdaderos activos de información, que por su repercusión e impacto en los derechos y libertades de las personas deben considerarse críticos.

Este eje está cubierto con los documentos: *"Directrices para la gestión del RAT.pdf"*, *la plantilla del RAT en formato Excel* y un *modelo de resolución para su aprobación* y publicación. Se ha adjuntado solo la guía que consideramos el documento principal por limitación de archivos. El modelo de resolución va como anexo a esta memoria. Para la gestión del riesgo se ha adjuntado la *"Guía para la gestión del riesgo.pdf"* así como un *Excel como herramienta operativa*.

2) Metodología estructurada en fases (operativa y replicable)

El núcleo metodológico se organiza en cinco fases, diseñadas para ser comprensibles y aplicables por unidades no especializadas, con apoyo del o la persona Delegada de Protección de Datos (DPD) y equipos técnicos cuando proceda:

- **Fase I: Descripción del tratamiento / contexto** (incluye revisión del RAT y ciclo de vida del dato)
- **Fase II: Identificación de amenazas y factores de riesgo** (incluyendo los supuestos de EIPD obligatoria)
- **Fase III: Gestión de amenazas y riesgos**
- **Fase IV: Plan de tratamiento del riesgo** (estrategias y medidas)
- **Fase V: Seguimiento y verificación** (eficacia, revisión y actualización)

El modelo incorpora además conceptos clave para decisiones consistentes: **riesgo inherente vs. residual**, matriz probabilidad × impacto, y criterios de priorización basados en el factor de riesgo más alto (evitando promedios que oculten riesgos críticos).

3) Herramientas y guías corporativas (paquete reutilizable)

El sistema se materializa en instrumentos corporativos que facilitan su implantación y reducen la carga de trabajo interpretativa:

- **Directrices corporativas para elaboración y mantenimiento del RAT**, con criterios de identificación de tratamientos, contenido obligatorio y contenido adicional para control interno, análisis de riesgosy pautas para publicación.
- **Directrices corporativas para gestión de riesgos en tratamientos**, alineadas con RGPD y referencias a estándares internacionales como ISO 31000, MAGERIT, guías de las autoridades de control y el ENS, con especial foco en riesgos para derechos y libertades.
- **Herramienta operativa (Excel) de gestión del riesgo**, estructurada de forma secuencial (índice por fases) e incluyendo módulos para actividad del tratamiento,

contexto, factores de riesgo, mitigación, juicio de proporcionalidad, plan de tratamiento y hoja resumen.

Este eje lo cubren los documentos Guía para la gestión del riesgo y el Excel de la herramienta específica en formato xlsx (realmente es un documento xlsm con macros para realizar cálculos automáticos, pero facilitado en formato xlsx para evitar problemas de operatividad y carga).

4) Gobernanza y roles: "responsabilidad distribuida con coordinación corporativa"

El modelo reconoce que la gestión del riesgo requiere roles claros y coordinación transversal. Por ello, define y promueve una participación ordenada de:

- Responsables del tratamiento (centros directivos)
- DPD (asesoramiento y supervisión)
- Equipos técnicos y de seguridad / TIC (medidas, ENS, sistemas)
- Encargados y subencargados cuando participan en el tratamiento
- Órganos directivos, para aprobación de resultados, niveles de riesgos y priorización de medidas técnicas y organizativas a adoptar

1.4. Resultados y evidencias de impacto (implantación y mejora)

Dado el actual escenario en el que asistimos a un constante cambio tecnológico y social el proyecto no se concibe como una guía estática, sino como un sistema corporativo que genera **evidencias** y habilita **mejora continua** en el tratamiento de datos personales, permitiendo incorporar nuevos criterios, disposiciones u orientaciones que garanticen un ciclo de gestión completo. En este sentido, el diseño incorpora elementos diferenciales:

1.4.1. Evidencias de implantación y trazabilidad

La metodología propuesta en el marco del proyecto promueve documentación estructurada del tratamiento, del nivel de riesgo y de las decisiones a adoptar en relación al mismo, facilitando la **trazabilidad** y la capacidad de respuesta ante auditorías o inspecciones, así como la revisión periódica cuando cambian el contexto, tecnologías o fines del tratamiento.

Asimismo, se incorpora el análisis del ciclo de vida del dato, junto con el inventario de activos y de los intervinientes en el manejo de la información personal, estableciendo además la conexión con las medidas de seguridad aplicables. Esta conexión incluye la alineación con el ENS y con las medidas del anexo II del Real Decreto que lo regula en el sector público, actuando como elemento de integración entre ambas normativas y cubriendo las exigencias técnicas del RGPD.

1.4.2. Medición y retroalimentación (responsabilidad proactiva "medible")

Un elemento especialmente relevante es la incorporación de una **medición diagnóstica del grado de uso y conocimiento** del modelo propuesto, orientada a obtener evidencias sobre su adopción, detectar áreas de mejora y orientar acciones de formación y acompañamiento. Este enfoque permite que el principio de responsabilidad proactiva se

pueda implantar progresivamente en los organismos y entes de la Junta de Andalucía, además de convertirse en una práctica verificable y que permita evolucionar a modelos más complejos y no sea meramente declarativa.

1.4.3. Mejora continua basada en versiones y experiencia real

La metodología se ha desarrollado con un enfoque iterativo: desde versiones iniciales hasta versiones más maduras, incorporando feedback de unidades, centros directivos y entidades usuarias, DPD y órganos de control interno (Inspección General de Servicios), lo que refuerza su adecuación práctica y su sostenibilidad en el tiempo. En este sentido, se liberó en 2024 la primera versión y en enero de 2026 se ha liberado la tercera versión de esta metodología.

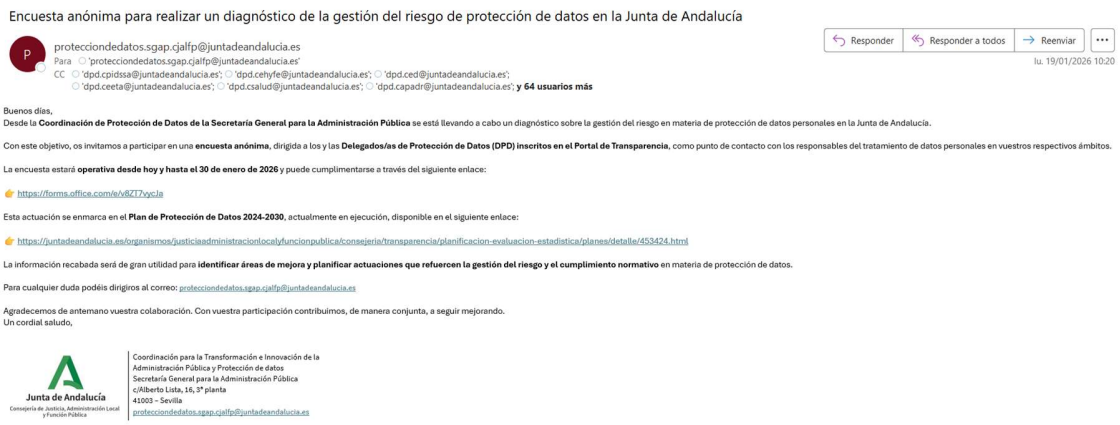
1.4.4. Resultado clave (en términos cualitativos)

Con el apoyo de esta metodología de trabajo y las herramientas diseñadas, la organización pasa de un modelo de cumplimiento "fragmentado" a un modelo corporativo que emplea criterios comunes y que integra elementos de trazabilidad, decisiones justificadas y capacidad de revisión periódica.

Como muestra de las actuaciones tendentes a medir y obtener datos sobre la implantación de la metodología, con fecha 19 de enero y hasta el 30 de enero de 2026 se lanzó una encuesta a los DPD publicados en el inventario del portal de transparencia de la Junta de Andalucía:

https://juntadeandalucia.es/protecciondedatos/delegados.html

para conocer el grado de madurez de la organización con respecto a la gestión de riesgos.



Encuesta anónima para realizar un diagnóstico de la gestión del riesgo de protección de datos en la Junta de Andalucía

Responder | Responder a todos | Reenviar | ...

lu. 19/01/2026 10:20

protecciondedatos.sgap.cjalfp@juntadeandalucia.es

Para 'protecciondedatos.sgap.cjalfp@juntadeandalucia.es'

CC 'dpd.cpidssa@juntadeandalucia.es'; 'dpd.cehyfe@juntadeandalucia.es'; 'dpd.ced@juntadeandalucia.es'; 'dpd.ceeta@juntadeandalucia.es'; 'dpd.csalud@juntadeandalucia.es'; 'dpd.capadr@juntadeandalucia.es'; **y 64 usuarios más**

Buenos días,

Desde la **Coordinación de Protección de Datos de la Secretaría General para la Administración Pública** se está llevando a cabo un diagnóstico sobre la gestión del riesgo en materia de protección de datos personales en la Junta de Andalucía.

Con este objetivo, os invitamos a participar en una **encuesta anónima**, dirigida a los y las **Delegados/as de Protección de Datos (DPD) inscritos en el Portal de Transparencia**, como punto de contacto con los responsables del tratamiento de datos personales en vuestros respectivos ámbitos.

La encuesta estará **operativa desde hoy y hasta el 30 de enero de 2026** y puede cumplimentarse a través del siguiente enlace:

👉 https://forms.office.com/e/v8ZT7vycJa

Esta actuación se enmarca en el **Plan de Protección de Datos 2024-2030**, actualmente en ejecución, disponible en el siguiente enlace:

👉 https://juntadeandalucia.es/organismos/justiciaadministracionlocalyfuncionpublica/consejeria/transparencia/planificacion-evaluacion-estadistica/planes/detalle/453424.html

La información recabada será de gran utilidad para **identificar áreas de mejora y planificar actuaciones que refuercen la gestión del riesgo y el cumplimiento normativo** en materia de protección de datos.

Para cualquier duda podéis dirigiros al correo: protecciondedatos.sgap.cjalfp@juntadeandalucia.es

Agradecemos de antemano vuestra colaboración. Con vuestra participación contribuimos, de manera conjunta, a seguir mejorando.

Un cordial saludo,

Junta de Andalucía
Consejería de Justicia, Administración Local y Función Pública

Coordinación para la Transformación e Innovación de la Administración Pública y Protección de datos
Secretaría General para la Administración Pública
c/Alberto Lista, 16, 3ª planta
41003 – Sevilla
protecciondedatos.sgap.cjalfp@juntadeandalucia.es

Evidencia del envío de la encuesta

El objetivo de la misma, ha sido el de conocer el grado de madurez en la organización con respecto a la gestión de riesgos de protección de datos. Esta es la segunda encuesta que realizamos (la anterior se realizó en 2023 con el objeto de realizar el diagnóstico de situación que supuso el punto de partida para la realización del plan estratégico de

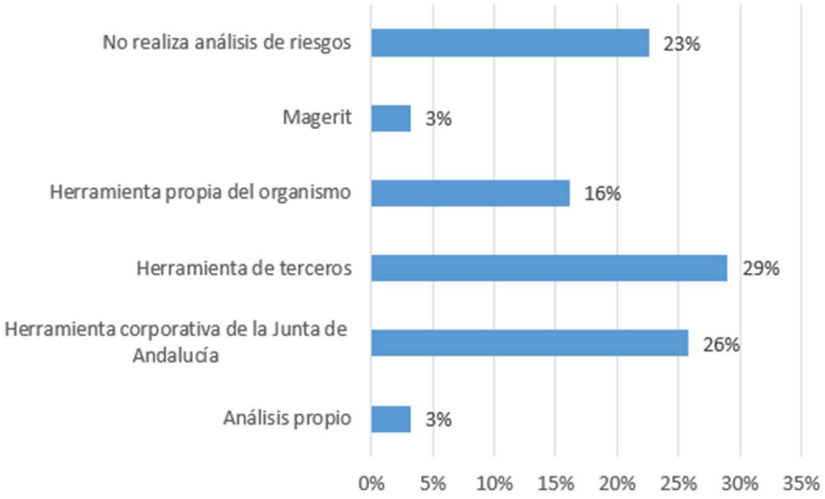
protección de datos anteriormente mencionado). El grado de participación ha sido del 46% correspondiendo el 68% a agencias o entidades del sector público instrumental y el 29% a Consejerías.

Porcentaje de participación en la encuesta para el diagnóstico del estado de situación de la gestión del riesgo en la Junta de Andalucía por tipo de organismo

Se han recibido respuestas correspondientes a 1.076 tratamientos de datos, lo que supone el 47% del total de tratamientos publicados en el RAT. De los mismos un 14,5% de los cuales tienen categorías especiales de datos.

Un total de 7 organismos declaran tener el 100% de los análisis de riesgos realizados, el resto oscila entre el 3 y el 25%. El grado de cumplimiento con respecto a las evaluaciones de impacto tienen tiene valores similares.

Un total de 8 organismos declaran utilizar la herramienta corporativa de gestión de riesgos, lo que supone un 26% de los organismos que han respondido a la encuesta. El resto se distribuyen según puede observarse en el siguiente gráfico:



Porcentaje de organismos en función de la herramienta de gestión del riesgo utilizada

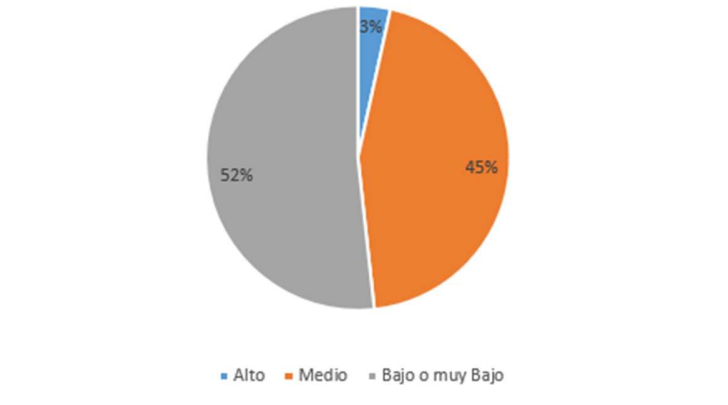
Cabe destacar que la implantación de la herramienta corporativa ha sido relativamente positiva para llevar dos años diseñada. También es importante tomar nota de la necesidad de realizar mayores actuaciones de concienciación en la gestión de riesgos ya que un 23% de organismos dicen no realizar ninguna.

Con respecto a la actualización de la gestión del riesgo un 26% declara que cuando se produce un cambio en el tratamiento frente a un 35% que declara no tener un criterio definido y otro 35% que declara no actualizarlos, desconocemos si obedece a que no hay cambios en los mismos o que simplemente no se realiza.

Un 58% de los organismos encuestados declara no conocer la herramienta corporativa, con lo cual se establece como prioridad realizar mayores actuaciones de difusión de la misma. Del resto que sí la conoce 9 organismos, que suponen el 29% consideran que cumple con todos los requisitos necesarios para ser una buena herramienta y el resto que cumple parcialmente.

De los que han utilizado la herramienta han realizado 237 análisis de riesgos y 66 evaluaciones de impacto con la misma.

Solo 1 organismo (3%) de los encuestados considera que tiene un nivel alto de madurez en cuanto a la gestión de riesgos, corresponde a una agencia. El resto consideran que tiene nivel medio un 45% y bajo o muy bajo el 52%. Queda por tanto un amplio recorrido por delante para poder seguir mejorando a este respecto.



Porcentaje de organismos en función del nivel de madurez percibido en cuanto a la gestión del riesgo

El 97% de organismos considera que debería haber una única herramienta de gestión del riesgo (sólo un organismo ha opinado que no). Las motivaciones principales han sido por uniformidad, homogeneidad, formación común y facilitar la actuación inspectora principalmente.

Las principales dificultadas encontradas a la hora de gestionar el riesgo son falta de recursos, falta de formación y falta de implicación de los responsables.

Las principales reivindicaciones han sido más recursos, más acompañamiento técnico, mayor implicación de los responsables y formación.

1.5. Valor añadido y adecuación a los Premios AEPD (modalidad B – sector público)

La iniciativa se alinea plenamente con el objetivo de los Premios AEPD en el sector público: *"Reconocer prácticas ejemplares de cumplimiento y responsabilidad social en el tratamiento de datos personales".*

1) Innovación pública (práctica y replicable)

La aportación principal no es una herramienta aislada como producto, sino la adopción de un **modelo corporativo integrado** que conecta RAT, ARPD y EIPD dentro de un flujo de decisión documentada y revisable. Este enfoque es especialmente valioso en administraciones públicas (AAPP), donde la diversidad funcional y la descentralización pueden generar heterogeneidad y riesgos de inconsistencia, con el consiguiente impacto negativo en términos de salvaguardas de los derechos de las personas.

2) Responsabilidad proactiva con evidencia (accountability operativa)

El sistema promueve la generación de evidencias de cumplimiento: informes de riesgos, elección de criterios para llevar a cabo la EIPD, planes de tratamiento del riesgo y mecanismos de revisión. La metodología enfatiza que el foco del riesgo debe ser la **persona** y sus derechos y libertades, no solo el riesgo legal o de cumplimiento para la organización, alineándose con el enfoque del RGPD.

3) Proporcionalidad, necesidad y garantías reforzadas

Cuando el riesgo inherente es alto, el modelo incorpora el análisis de **idoneidad, necesidad y proporcionalidad** como soporte a la toma de decisiones, garantizando que el tratamiento de datos se justifica por objetivos claros y que se han considerado alternativas menos intrusivas, necesarias y proporcionales a la finalidad perseguida.

4) Transparencia y confianza ciudadana

La metodología impulsa un RAT consistente y publicable, con criterios claros para evitar prácticas erróneas y reforzar la transparencia, separando información destinada a la publicación de la información interna necesaria para una adecuada gestión del riesgo de protección de datos.

5) Replicabilidad en otras Administraciones Públicas

El enfoque es reproducible en otras AAPP y entidades del sector público, si consideramos los siguientes elementos:

- Se basa en un proceso por fases,
- dispone de guías y plantillas reutilizables,
- y se apoya en herramientas accesibles y escalables, adaptables al nivel de madurez de cada organización.

En conjunto, la experiencia constituye una **buena práctica orientada al cumplimiento normativo y a la responsabilidad social**, al transformar la protección de datos en un sistema corporativo de gestión: homogéneo, trazable, revisable y orientado a la protección efectiva de los derechos de las personas, con capacidad de mejora continua y transferencia a otras AAPP.

La Junta de Andalucía ha implantado un modelo corporativo que integra RAT, análisis de riesgos y EIPD en un flujo de decisión documentada y revisable, reforzando la responsabilidad proactiva, la transparencia y la protección efectiva de los derechos.

2. Contexto organizativo y punto de partida

2.1. La Junta de Andalucía como organización compleja (estructura, diversidad y exposición al riesgo)

La Junta de Andalucía desarrolla políticas públicas y presta servicios esenciales a la ciudadanía a través de una estructura administrativa amplia y diversa, con múltiples órganos directivos y entidades del sector público instrumental que operan en ámbitos funcionales muy distintos. Esta complejidad organizativa implica una alta diversidad de **tratamientos de datos personales**, tanto por finalidades (gestión administrativa, prestación de servicios, control y supervisión, etc.) como por tipologías de datos y perfiles de personas afectadas.

En particular, el funcionamiento ordinario de una administración pública con estas características conlleva que:

- Se traten datos personales asociados a procedimientos y servicios de distinta naturaleza, alcance y finalidades, en los que intervienen diferentes unidades administrativas, soportes y sistemas de información.
- Existan tratamientos con **categorías de datos especialmente sensibles** (por ejemplo, en entornos de salud, justicia o servicios sociales), así como tratamientos que pueden afectar a colectivos en situación de especial vulnerabilidad, lo cual incrementa el nivel de riesgo para los derechos y libertades de las personas.

- El tratamiento de datos se apoye en un ecosistema tecnológico que incluye sistemas de información y aplicativos corporativos, herramientas horizontales, soluciones específicas y, en determinados casos, tratamientos no automatizados (papel), lo que obliga a contemplar el riesgo con un enfoque integral, conectando la gestión de los datos personales con otra normativa de aplicación (archivos y patrimonio documental; estadística, laboral) en un contexto legislativo cada vez más complejo.

En este escenario, la protección de datos no puede gestionarse como una tarea aislada o meramente documental; requiere un modelo de gobernanza corporativo que permita mantener coherencia, trazabilidad y revisión periódica, integrando el enfoque de riesgo en la toma de decisiones sobre el tratamiento de datos personales.

2.2. Situación previa: un cumplimiento heterogéneo y difícil de sostener

Antes de impulsar esta iniciativa, la organización se enfrentaba a una problemática común en administraciones complejas: la dificultad de aplicar de forma homogénea y sostenible las obligaciones derivadas del RGPD, especialmente en lo relativo al **RAT** y a la gestión del riesgo como elemento central de la responsabilidad proactiva.

2.2.1. Heterogeneidad en la identificación y documentación de tratamientos

Antes de impulsar esta iniciativa, la Junta de Andalucía se enfrentaba a uno de los principales retos en organizaciones complejas, la propia **identificación del tratamiento**. Las directrices corporativas sobre el RAT señalan que es esencial evitar prácticas incorrectas (por ejemplo, identificar tratamiento con un procedimiento concreto, con una fase del procedimiento, con un sistema de información o con una unidad administrativa), ya que ello genera duplicidades, desorden y dificulta la gestión posterior del riesgo.

La situación previa mostraba, en consecuencia, una variabilidad elevada en:

- el nivel de agregación o segregación de tratamientos, encontrándose con duplicidades, inconsistencias, etc.
- la claridad a la hora de identificar correctamente las finalidades de los tratamientos,
- la consistencia de categorías de datos, interesados/as y destinatarios,
- y la conexión del RAT con otras obligaciones (información a las personas, conservación, seguridad, etc.).

2.2.2. Dificultad para operar el enfoque basado en riesgos

El RGPD desplaza el cumplimiento desde un paradigma reactivo hacia uno de **gestión proactiva del riesgo** para derechos y libertades, lo que exige conocer el contexto del tratamiento, identificar amenazas, valorar probabilidad e impacto y definir medidas de mitigación.

Sin un marco de gobernanza corporativo, esta exigencia se traducía en una aplicación desigual, algunas unidades podían disponer de criterios y capacidades, mientras que otras carecían de guías operativas y herramientas accesibles para ejecutar análisis consistentes, comparables y revisables.

2.2.3. Brecha entre "documentar" y "decidir"

La experiencia previa mostraba una brecha frecuente: disponer de documentación parcial (por ejemplo, descripciones de tratamientos) no garantizaba por sí sola una **toma de decisiones basada en riesgo**, ni una planificación trazable de medidas y revisiones. La guía corporativa de riesgos enfatiza precisamente la necesidad de documentar no solo el tratamiento, sino también la valoración y gestión del riesgo, así como el seguimiento de la eficacia de los controles.

2.3. El marco estratégico: del cumplimiento formal a la responsabilidad proactiva corporativa

La iniciativa se enmarca en una estrategia institucional orientada a consolidar un modelo de protección de datos **operativo, transversal y sostenible**. El planteamiento parte del principio de que la responsabilidad proactiva requiere un sistema que permita demostrar cumplimiento mediante evidencias: registros consistentes, análisis de riesgos, decisiones justificadas y mecanismos de revisión

2.3.1. El RAT como punto de partida y elemento vertebrador

El RAT constituye el punto de partida indispensable para el cumplimiento del RGPD en el sector público, y además es el soporte para conectar obligaciones de transparencia con necesidades internas de control. Las directrices corporativas enfatizan que el RAT debe ser útil, ágil y orientado a facilitar el control de sus datos por parte de las personas interesadas, evitando enfoques que dificulten su actualización o comprensión.

Asimismo, estas directrices recomiendan incorporar, además del contenido obligatorio, información adicional para control interno (por ejemplo: ciclo de vida de datos, aplicaciones y activos intervinientes, existencia de papel, encargados, vínculos con inventarios de procedimientos administrativos, vigencia), precisamente para facilitar la gestión del riesgo y las evaluaciones de impacto incluso en aquellos tratamientos de datos que en apariencia no representen un riesgo significativo para las personas físicas.

2.3.2. Integración con el contexto administrativo y la gestión ordinaria

Un reto específico del sector público es la interacción entre tratamientos de datos y el ecosistema procedimental. Las directrices de RAT hacen referencia al Registro de Procedimientos y Servicios (RPS) como inventario relevante para coherencia y transparencia, recordando que no debe confundirse "procedimiento" con "tratamiento", y que es posible agrupar varios procedimientos bajo un tratamiento con finalidades comunes.

Este enfoque permite integrar la protección de datos en la gestión ordinaria: al revisar procedimientos y servicios, se verifica si encajan en tratamientos existentes o si es

necesario crear nuevos tratamientos, evitando duplicidades y facilitando una trazabilidad más consistente.

2.3.3. Alineación con seguridad de la información y ENS

La guía de riesgos destaca la relación entre riesgos de privacidad y riesgos de seguridad de la información, señalando la conveniencia de integrar ambos enfoques, dado que la información y el planteamiento de la normativa comparten dimensiones de seguridad (confidencialidad, integridad, disponibilidad, etc.). Es por ello que la información de carácter personal en cuanto a activo esencial en el ámbito público, debe situarse en el contexto del ENS, siendo este elemento clave para medidas técnicas y organizativas, que protejan la información en los sistemas empleados para su tratamiento.

2.4. Necesidad de una metodología corporativa común (por qué una solución "de sistema")

La decisión de diseñar una metodología corporativa común responde a una idea central: en una organización compleja, la protección de datos solo puede ser sostenible si se gestiona como un **sistema**, no como actuaciones aisladas por unidades o como una suma de documentos inconexos.

En concreto, se identificaron necesidades corporativas prioritarias:

2.4.1. Homogeneidad y comparabilidad

Un marco común permite:

- aplicar criterios consistentes para definir tratamientos y finalidades
- identificar riesgos con una lógica compartida (probabilidad × impacto),
- y comparar resultados para priorizar medidas y recursos, evitando enfoques arbitrarios.

2.4.2. Reutilización y escalabilidad

La guía de gestión de riesgos se apoya en metodologías de referencia (como ISO 31000 o MAGERIT) y en la opinión y dictámenes de distintas autoridades de control, pero insiste en ofrecer un proceso eminentemente práctico y operable en la Administración, con fases claras y herramientas de apoyo. Esto facilita que organismos con distintos niveles de madurez puedan adoptar la metodología de forma progresiva e impulsar ciclos de mejora continua con un menor esfuerzo.

2.4.3. Trazabilidad y evidencia (accountability verificable)

El enfoque corporativo permite que cada tratamiento genere un rastro documental coherente:

- descripción del contexto del tratamiento (incluyendo el ciclo de vida, intervinientes, etc.,

- factores de riesgo aplicables (bien a través de catálogos orientativos, bien con la posibilidad de añadir amenazas propias),
- decisión sobre necesidad de EIPD basada en riesgo inherente, contemplando los elementos de riesgo más críticos,
- plan de tratamiento del riesgo, como elemento de actuación fundamentalmente en el ciclo de mejora continua,
- y mecanismos de revisión, tanto de los niveles de riesgo, como de la aplicación de los planes de tratamiento del riesgo.

Esta trazabilidad es crítica para demostrar el cumplimiento del principio de responsabilidad proactiva, apoyar la realización de auditorías internas y mejorar la capacidad de respuesta ante requerimientos de las autoridades de control y las propias expectativas de la ciudadanía respecto al manejo de sus datos personales por parte de la Administración.

2.4.4. Capacidad de decisión: de la evaluación a la acción

La metodología no se limita a "evaluar": incorpora fases específicas para definir estrategias de tratamiento del riesgo (mitigar, evitar, aceptar, transferir), establecer prioridades, responsables y recursos, y verificar la eficacia de las medidas implantadas.

2.5. Retos iniciales que guiaron el diseño

A partir del diagnóstico de contexto y del análisis del marco normativo y operativo, se definieron los retos que el proyecto debía resolver.

Se presentan a continuación de forma sintética, en clave de "problema → necesidad → criterio de diseño":

2.5.1. Reto 1: Identificación coherente de tratamientos

- **Problema:** tratamientos definidos con criterios no homogéneos (por procedimiento, por unidad, por sistema), dificultando actualización y control.
- **Necesidad:** criterios corporativos claros sobre qué es un tratamiento, cómo agrupar/segregar y cómo redactar finalidades.
- **Criterio de diseño:** guía RAT con buenas/malas prácticas y plantilla normalizada (campos publicables a través del portal de la Junta de Andalucía e internos).

2.5.2. Reto 2: Convertir el RAT en una herramienta útil para la gestión del riesgo

- **Problema:** el RAT como obligación documental aislada, sin conexión operativa con decisiones y medidas.
- **Necesidad:** incorporar ciclo de vida, actores, tecnologías y elementos internos que habiliten el análisis de riesgos y EIPD.

- **Criterio de diseño:** RAT ampliado para control interno y conexión explícita con Fases de contexto y análisis de riesgos.

2.5.3. Reto 3: Aplicar un enfoque de riesgo uniforme y defendible

- **Problema:** ausencia de criterios comunes para valorar riesgo (probabilidad/impacto) y para decidir EIPD.
- **Necesidad:** un método compartido, basado en referencias reconocidas y en las indicaciones, dictámenes y opiniones de las autoridades de control.
- **Criterio de diseño:** metodología por fases, matriz de riesgo, distinción inherente/residual y criterios de alto riesgo (RGPD/LOPDGDD/autoridades) con un enfoque eminentemente práctico, de forma que sea una metodología comprensible y eficaz, mejorando su percepción por parte de los responsables del tratamiento y por los encargados de aplicarla.

2.5.4. Reto 4: Garantizar gobernanza y participación de roles críticos

- **Problema:** la gestión del riesgo exige colaboración entre distintos actores (responsables, DPD, TIC/seguridad, encargados).
- **Necesidad:** clarificar roles, canales de consulta y documentación; evitar dependencia de expertos o recursos dedicados.
- **Criterio de diseño:** definición de roles mínimos y protocolos de intervención, especialmente para tratamientos de mayor impacto en los derechos y libertades de los interesados.

2.5.5. Reto 5: Sostenibilidad en el tiempo y mejora continua

- **Problema:** sin revisiones periódicas, los tratamientos cambian y el riesgo requiere revisión y actualización.
- **Necesidad:** establecer activadores de revisión (cambios en tecnología, volumen, fines, contexto, incidencias o brechas de seguridad materializadas).
- **Criterio de diseño:** fase de seguimiento y verificación, revisión anual y reevaluación ante cambios sustanciales en los tratamientos de datos personales.

3. Objetivos, alcance y principios del proyecto

El proyecto surge ante la necesidad de superar un cumplimiento heterogéneo y formalista y avanzar hacia un modelo corporativo de responsabilidad proactiva. Para ello, se estandariza la identificación y documentación de tratamientos (RAT), se integra un proceso de gestión del riesgo por fases y se habilita la toma de decisiones basada en riesgo, con seguimiento y mejora continua.

3.1. Objetivo general

El proyecto tiene como finalidad consolidar un **modelo corporativo de responsabilidad proactiva** en protección de datos en la Junta de Andalucía, basado en la gestión del riesgo como pilar operativo del cumplimiento del RGPD.

Como objetivo general se persigue diseñar e implantar una **metodología corporativa, común y reutilizable** que integre el Registro de Actividades de Tratamiento (RAT), el análisis de riesgos, la determinación de necesidad de Evaluación de Impacto (EIPD), la definición de medidas y el seguimiento, de manera **homogénea, trazable y sostenible** en una organización pública de alta complejidad.

Este objetivo general se traduce en un cambio de enfoque: pasar de un cumplimiento predominantemente formal a un sistema de gestión que permita **tomar decisiones documentadas y revisables**, con evidencias de cumplimiento y mejora continua.

3.2. Objetivos específicos

Los objetivos específicos se formulan en clave operativa y alineados con las obligaciones y principios del RGPD (responsabilidad proactiva, protección de datos desde el diseño y por defecto, enfoque basado en riesgo), así como con las exigencias del sector público en materia de transparencia.

3.2.1. Estandarización y calidad del Registro de Actividades de Tratamiento (RAT)

1. **Homogeneizar criterios** para identificar y definir tratamientos, evitando prácticas incorrectas (p. ej., equiparar tratamiento a procedimiento, a fases del procedimiento, a sistemas o a unidades administrativas).

2. Establecer una **estructura de RAT corporativa** que distinga de forma clara la información destinada a **publicación/transparencia** de la información destinada a **control interno** (responsabilidad proactiva).

3. Mejorar la **calidad y coherencia** de los campos críticos del RAT (finalidad, base jurídica, categorías de datos e interesados, destinatarios, conservación y referencias generales a las medidas de seguridad técnicas y organizativas aplicadas), favoreciendo su mantenimiento y actualización.

3.2.2. Integración del análisis de riesgos en la gestión ordinaria

1. Implantar un proceso común de **análisis de riesgos para derechos y libertades** aplicable a tratamientos de distinta naturaleza y complejidad, basado en un marco metodológico organizado por fases secuenciales.

2. Incorporar el análisis del **contexto del tratamiento** como paso previo imprescindible (naturaleza, ámbito, fines, ciclo de vida de los datos, tecnologías, intervinientes, comunicaciones y conservación), garantizando una identificación de riesgos ajustada a la realidad operativa, con independencia del tipo de organismos, ente o ámbito competencial implicado.

3. Establecer criterios compartidos para valorar **probabilidad e impacto**, diferenciar **riesgo inherente** y **riesgo residual**, y priorizar riesgos críticos sin diluirlos mediante promedios (criterio del "valor máximo" como riesgo global orientativo).

3.2.3. Determinación objetiva de la necesidad de llevar a cabo una EIPD y reforzamiento de garantías

1. Determinar de forma objetiva cuándo procede una EIPD, considerando supuestos del RGPD (art. 35.3 y listados publicados por autoridades de control), LOPDGDD y obligaciones normativas.

2. Integrar la EIPD como actividad "indivisible" de la gestión del riesgo, incluyendo el análisis de **necesidad y proporcionalidad** (juicios de idoneidad, necesidad y proporcionalidad en sentido estricto) para apoyar decisiones informadas.

3.2.4. Decisión documentada, planes de tratamiento del riesgo y seguimiento

1. Facilitar la adopción de **decisiones documentadas** y trazables: selección de medidas, responsables, recursos y plazos, mediante un **Plan de Tratamiento del Riesgo**, sobre el que posteriormente pueda llevarse a cabo un seguimiento.

2. Implantar mecanismos de **seguimiento y revisión periódica**, definiendo activadores del ciclo de revisión (cambios en tecnología, volumen, fines, contexto, incidencias, marco normativo, etc.), promoviendo mejora continua.

3.2.5. Cultura organizativa, apoyo y sostenibilidad

1. Impulsar una cultura organizativa de privacidad mediante **guías accesibles, herramientas operativas y acompañamiento**, favoreciendo que la metodología sea aplicable por personal y unidades no especializadas, con apoyo del DPD y equipos técnicos cuando proceda.

2. Asegurar que el modelo sea **reutilizable y escalable** para distintos organismos, con independencia de su madurez, facilitando la replicabilidad dentro y fuera de la Junta de Andalucía.

3.3. Alcance organizativo y funcional

El alcance del proyecto se divide en dos grandes áreas, un alcance organizativo, en el que tienen cabida los actores implicados en la identificación y valoración de tratamientos de datos personales, y por otra parte un alcance sustantivo en el que se han incluido elementos necesarios para dotar a la metodología de una eficacia práctica.

3.3.1. Alcance organizativo

El proyecto se dirige al conjunto de órganos y entes del sector público de la Junta de Andalucía, y está orientado a su aplicación por **responsables del tratamiento, encargados del tratamiento y DPD**, conforme a los roles y responsabilidades definidas en las directrices corporativas.

En la práctica, esto implica un marco común aplicable tanto a Consejerías como a organismos y entes instrumentales, adaptándose a su diversidad funcional y tecnológica, considerando además el alto grado de avance en la organización y determinación de roles relacionados con la seguridad, privacidad y protección de datos.

3.3.2. Alcance funcional (qué cubre el sistema)

El modelo cubre el ciclo completo de responsabilidad proactiva sobre tratamientos de datos personales, integrando:

- **Identificación y documentación** de tratamientos en el RAT (contenido publicable y contenido de control interno).
- **Descripción del contexto** y del **ciclo de vida** de los datos como base del análisis del riesgo.
- **Identificación de amenazas y factores de riesgo**, incluyendo factores relacionados con fines, tipologías de datos, alcance, categorías de interesados, factores técnicos, comunicaciones y efectos colaterales, además de otras amenazas vinculadas a la privacidad, los derechos de los interesados y al cumplimiento normativo en sí mismo, contemplando la posibilidad de incorporar otros tipos de riesgos, como los relacionados con las brechas o violaciones de datos personales, o los derivados del uso de nuevas tecnologías o tipos de tratamiento, como la inteligencia artificial o la implantación de procedimientos administrativos que llevan a cabo tomas de decisiones automatizadas.
- **Evaluación del riesgo** desplegando una matriz de riesgos (probabilidad × impacto) reconocida y determinación de **riesgo inherente** y **riesgo residual** tras aplicar controles basados en una metodología de madurez de controles CMMI.
- **Determinación de necesidad de EIPD** según criterios normativos y doctrinales y, en su caso, realización de EIPD con juicio de necesidad y proporcionalidad.
- **Plan de tratamiento del riesgo**, priorización y seguimiento, con revisión periódica ante cambios relevantes.

3.3.3. Alcance instrumental (artefactos del sistema)

Además de lo indicado anteriormente, el proyecto se materializa en un conjunto de instrumentos corporativos que estructuran y facilitan su implantación:

- Directrices para la elaboración y mantenimiento del RAT (criterios, buenas/malas prácticas, contenido y publicación).
- Directrices para la gestión de riesgos y EIPD (metodología por fases, criterios de riesgo y seguimiento).
- Herramienta operativa (Excel) para facilitar y guiar el proceso secuencial de análisis, mitigación y documentación.

3.4. Principios rectores del modelo

Los principios rectores guían tanto el diseño como la implantación, garantizando que el sistema sea coherente con el RGPD y viable en un entorno público complejo.

3.4.1. Responsabilidad proactiva (accountability) y evidencia

El modelo se orienta a "poder demostrar" el cumplimiento: el análisis de riesgos, las decisiones y las medidas deben quedar documentados, revisables y a disposición de verificación. Para ello se promueve la elaboración de informes por tratamiento (o conjuntos) y su aprobación al nivel adecuado (órganos directivos, decisores, gerencia, etc.).

3.4.2. Enfoque basado en riesgos para derechos y libertades

El foco del análisis no es el riesgo organizativo o reputacional, sino el **riesgo para los derechos y libertades** de las personas físicas, atendiendo a naturaleza, ámbito, contexto y fines del tratamiento. Este principio guía la identificación de factores de riesgo, amenazas y la priorización de medidas técnicas y organizativas para mitigarlos.

3.4.3. Proporcionalidad, necesidad y privacidad desde el diseño

El modelo incorpora la protección de datos desde el diseño y por defecto, y cuando procede llevar a cabo la EIPD exige justificar la idoneidad del tratamiento, su necesidad (alternativas menos intrusivas) y la proporcionalidad en sentido estricto (balance daño–beneficio social), reforzando garantías especialmente en tratamientos de alto riesgo.

3.4.4. Homogeneidad y reutilización corporativa

Se apuesta por criterios y herramientas comunes para evitar dispersión interpretativa y reducir la dependencia de soluciones ad hoc. La metodología se concibe para ser reutilizable por organismos con distinto nivel de madurez y para evolucionar con la experiencia a modelos más intuitivos, completos e integradores de nuevos escenarios, requerimientos y riesgos.

3.4.5. Transparencia y claridad hacia la ciudadanía

El diseño del RAT y su publicación se orientan a facilitar el control de los datos personales por las personas interesadas, con información comprensible, completa y coherente, separando lo publicable de lo interno sin perder trazabilidad.

3.4.6. Coordinación y corresponsabilidad operativa (roles determinados)

La metodología define la necesidad de intervención de roles mínimos (responsables del tratamiento, técnicos/gestores, TIC/seguridad, DPD y, cuando proceda, encargados/subencargados) para asegurar que la gestión del riesgo sea completa y eficaz.

3.4.7. Mejora continua y revisión periódica

El modelo incorpora seguimiento, verificación de eficacia y revisión periódica (al menos anual o ante cambios sustanciales), con activadores explícitos (cambios de tecnología, alcance, fines, incidencias, normativa, etc.), garantizando sostenibilidad y actualización del riesgo.

4. Diseño del modelo corporativo de responsabilidad proactiva

4.1. Enfoque integral: cumplimiento normativo + gestión + evidencia ("accountability" operativa)

La Junta de Andalucía adopta un modelo que entiende la protección de datos como un **sistema de gestión** integrado en la actividad ordinaria, y no como un conjunto de obligaciones aisladas o meramente documentales. Este enfoque se alinea con el cambio de paradigma que introduce el RGPD: pasar de modelos reactivos a modelos basados en la **gestión proactiva del riesgo** para los derechos y libertades de las personas, con capacidad de demostrar el cumplimiento mediante evidencias verificables.

El diseño del sistema parte de tres ideas o premisas fundamentales:

1. **El cumplimiento efectivo requiere operatividad.** La organización necesita mecanismos y herramientas que permitan a las unidades responsables identificar tratamientos, evaluar riesgos, decidir medidas y revisarlas de forma periódica.

2. **El riesgo es el núcleo de la responsabilidad proactiva.** El foco del análisis es el impacto potencial sobre las personas (derechos y libertades) y su contexto de tratamiento, no únicamente el riesgo organizativo, reputacional o de incumplimiento.

3. **La evidencia es tan importante como la acción.** Para demostrar el cumplimiento del principio de accountability es imprescindible conservar trazabilidad documental: qué se analizó, con qué criterios, quién intervino, qué se decidió, qué medidas se implantaron y cuándo se revisaron.

Con este punto de partida, el modelo se construye como una arquitectura corporativa que conecta coherentemente los elementos esenciales del RGPD en el sector público: **RAT → Análisis de riesgos → (EIPD cuando proceda) → Decisiones y plan de tratamiento del riesgo → Seguimiento y revisión**.

4.2. Marco normativo y doctrinal de referencia (síntesis aplicada)

El modelo se apoya en un conjunto de referencias normativas y metodológicas reconocidas, con un objetivo práctico: ofrecer un **criterio común** para todos los organismos y unidades, manteniendo flexibilidad para adaptarse a su diversidad y madurez.

4.2.1. Marco normativo base

- **RGPD**: enfoque basado en riesgos, responsabilidad proactiva, seguridad del tratamiento, evaluaciones de impacto y protección de datos desde el diseño y por defecto.

- **LOPDGDD**: obligaciones específicas del sector público, publicación del inventario/RAT y criterios de necesidad de EIPD en determinados supuestos.

- **ENS (Esquema Nacional de Seguridad)** como marco de referencia para medidas técnicas y organizativas en administraciones públicas, con referencias generales adecuadas en el RAT para publicación.

4.2.2. Referencias metodológicas para la gestión del riesgo

La metodología corporativa de riesgos se basa en el uso de metodologías y estándares ampliamente reconocidos (p. ej ISO 31000, ISO 27001, ISO 27701, ISO 29100, ISO 27005 (gestión de riesgos), ISO 29134 (evaluación de impacto). y metodologías de riesgo como MAGERIT) como soporte para estructurar el proceso y dotarlo de coherencia.

Asimismo, integra criterios doctrinales y herramientas de autoridades de control para la identificación de riesgos y determinación del nivel de riesgo, incluyendo referencias a **directrices europeas (WP248/CEPD)** y guías de la **AEPD**, así como instrumentos orientativos como **EVALÚA** (como referencia metodológica de apoyo).

Aplicación práctica del marco: la Junta de Andalucía traduce estas referencias a un procedimiento corporativo por fases, con plantillas y herramienta operativa, para garantizar que el enfoque sea aplicable por unidades no especializadas y comparable entre organismos.

4.3. Diseño del sistema integral: RAT–Riesgo–EIPD–Decisión–Seguimiento

El sistema corporativo se diseña como un "circuito" de gestión que comienza en la descripción del tratamiento (qué se hace con los datos) como activo sobre el cual asignar amenazas y riesgos propios, y termina en el control continuo (cómo se verifica y mitigan los riesgos identificados). La clave es que cada etapa alimenta a la siguiente, evitando documentos desconectados.

4.3.1. El RAT como punto de partida (qué se trata y por qué)

El **RAT** actúa como inventario estructurado y como base para cumplir con la transparencia y la rendición de cuentas. En el modelo corporativo, el RAT no es un "fin" sino el **origen** de la gestión del riesgo: describe el tratamiento con suficiente consistencia para identificar amenazas, valorar impacto y decidir medidas.

La guía corporativa del RAT establece criterios prácticos para identificar y configurar tratamientos (buenas y malas prácticas), evitando errores típicos como asociar tratamiento a procedimiento o a sistema, y promoviendo una finalidad suficientemente amplia para englobar operaciones relacionadas sin caer en "cajones de sastre".

Además, el modelo diseñado distingue entre:

- **Información obligatoria/publicable** (alineada con el RGPD y la normativa aplicable).
- **Información adicional para control interno**, orientada a responsabilidad proactiva (ciclo de vida, nivel de riesgo, aplicaciones intervinientes, existencia de papel, encargados, etc.).

4.3.2. Análisis de riesgos como núcleo operativo (cómo puede afectar a las personas)

La gestión del riesgo se organiza en un proceso secuencial por fases que parte del contexto del tratamiento y culmina en la planificación de medidas y su verificación. La guía corporativa de riesgos estructura el proceso en **cinco fases** (I a V), diseñadas para asegurar una visión integral y revisable.

La herramienta operativa (Excel) materializa esta lógica secuencial en pestañas/módulos que guían al usuario por: actividad del tratamiento, contexto, ciclo de vida, supuestos de EIPD, factores de riesgo, mitigación, juicio de proporcionalidad, plan de tratamiento y un recopilatorio de datos que faciliten su extracción a los efectos de elevar los informes que sean preceptivos

4.3.3. Evaluación de Impacto (EIPD) cuando procede (garantías reforzadas)

El sistema incorpora la EIPD como componente integrada y no como actividad independiente. La guía de gestión de riesgos señala que la EIPD forma parte de la gestión del riesgo y que debe ejecutarse en su marco, especialmente en fases de concepción/diseño o cuando cambian condiciones relevantes del tratamiento.

La determinación de necesidad de EIPD se basa principalmente en el **riesgo inherente** identificado (antes de medidas), y en los supuestos previstos por normativa y criterios de autoridades de control.

4.3.4. Decisión documentada y plan de tratamiento del riesgo (qué medidas y con qué prioridad)

El modelo exige que el resultado del análisis se traduzca en decisiones trazables: selección de controles, justificación, responsables, recursos y plazos, mediante un **Plan de Tratamiento del Riesgo** (mitigar/evitar/aceptar/transferir) y un esquema de seguimiento posterior.

4.3.5. Seguimiento, revisión y mejora continua (cómo se mantiene el cumplimiento)

La guía de riesgos incorpora una fase específica para verificar eficacia de medidas y activar ciclos de revisión ante cambios sustanciales (tecnología, fines, volumen, contexto, incidencias, marco normativo, etc.), recomendando revisiones periódicas (p. ej., anual) para mantener actualizado el nivel de riesgo.

4.4. Flujo corporativo por fases: proceso operativo (de extremo a extremo)

A continuación, se describe el flujo de trabajo del sistema, con un enfoque mixto (técnico-jurídico + operativo), para evidenciar cómo se integra la protección de datos en la gestión ordinaria.

4.4.1. Fase I — Descripción del tratamiento (contexto) y revisión del RAT

Objetivo: conocer el tratamiento con el nivel de detalle necesario para una valoración realista del riesgo. La guía de riesgos subraya que la descripción del contexto (naturaleza, ámbito, fines, ciclo de vida) es el punto de partida indispensable de cualquier análisis.

Contenido mínimo recomendado para la actividad de tratamiento (visión práctica):

- Identificación del tratamiento y finalidad(es).
- Base jurídica y marco competencial (adecuación a funciones atribuidas).
- Categorías de datos, interesados y destinatarios, incluyendo comunicaciones y transferencias.
- Conservación y ciclo de vida del dato (recogida → uso → cesión → conservación/bloqueo → supresión).
- Tecnologías y sistemas intervinientes (incluido papel cuando exista).
- Encargados y subencargados, cuando corresponda.

Instrumentos del sistema que soportan esta fase:

- Directrices corporativas para RAT y ficha/plantilla normalizada.
- Módulos de "Actividad del tratamiento" y "Descripción del contexto" en la herramienta Excel (incluye campos sobre RAT, procedimientos, ciclo de vida, intervinientes y medidas generales).

Resultado esperado de la fase I: un tratamiento descrito de forma consistente, con información suficiente para identificar amenazas y justificar decisiones posteriores.

4.4.2. Fase II — Identificación de amenazas y factores de riesgo

Objetivo: identificar qué puede salir mal (amenazas) y qué condiciones incrementan el riesgo (factores), en relación con los derechos y libertades de las personas. La guía de riesgos incorpora un catálogo de factores basado en criterios de la AEPD y categorías (fines, tipos de datos, alcance, interesados vulnerables, factores técnicos, comunicaciones, efectos colaterales, brechas, etc.), así como un catálogo de amenazas a la privacidad que pueden dirigirse a plasmar una adecuada gestión del riesgo y plasmar sus resultados en una evaluación de impacto.

Elementos característicos del enfoque corporativo:

- Se promueve la **granularidad**: identificar riesgos concretos evita análisis genéricos que no conducen a medidas eficaces.
- Se contemplan expresamente tratamientos con tecnologías emergentes o disruptivas y escenarios como decisiones automatizadas o uso de IA, como ámbitos que pueden añadir nuevas amenazas y requieren atención específica.

Soporte instrumental:

- La herramienta Excel incluye un apartado específico de "Factores de riesgo" y un bloque adicional de "otras amenazas" (catálogo), alineado con la metodología por fases e incorporando catálogos predefinidos apoyados en estándares internacionales.

Resultado esperado de la fase II: listado documentado de amenazas y factores aplicables, con hipótesis claras para valorar probabilidad e impacto.

4.4.3. Fase III — Evaluación del nivel de riesgo y decisión sobre necesidad de EIPD

Objetivo: valorar el riesgo del tratamiento de forma objetiva para decidir: (a) nivel de riesgo inherente, (b) necesidad de EIPD y (c) prioridades.

La guía corporativa define el uso de una matriz **Riesgo = Probabilidad × Impacto**, con escalas para determinar niveles (bajo/medio/alto/muy alto).

Aspectos clave del modelo propuesto:

- **Riesgo inherente**: se calcula sin considerar medidas mitigadoras; es el que guía la decisión de llevar a cabo una EIPD.
- **Riesgo residual**: se calcula tras considerar controles y medidas, valorando su madurez y eficacia de acuerdo a un modelo de valoración de controles.
- **Criterio de riesgo global**: se recomienda considerar como riesgo global el valor máximo de los factores evaluados para no invisibilizar riesgos críticos.

Determinación de EIPD:

La guía recoge supuestos del RGPD (art. 35.3), así como los listados/criterios de autoridades de control (art. 35.4) y supuestos recogidos en la LOPDGDD, además de criterios doctrinales, para concluir cuándo un tratamiento probablemente entraña alto riesgo y requiere EIPD.

Soporte instrumental:

- La herramienta Excel incorpora pestañas de “Supuestos EIPD obligatoria” y módulos para la evaluación y hoja resumen, facilitando consistencia y trazabilidad.

Resultado esperado de la fase III: nivel de riesgo inherente y residual documentados; decisión motivada sobre EIPD; y base para el plan de tratamiento del riesgo.

4.4.4. Fase IV — Plan de tratamiento del riesgo (medidas, responsables, plazos)

Objetivo: pasar de la evaluación a la acción, definiendo una estrategia para cada riesgo relevante y medidas concretas.

La guía de riesgos contempla estrategias típicas: **mitigar/reducir**, **evitar/eliminar**, **aceptar/asumir** o **transferir** el riesgo, y recomienda establecer planes concretos con recursos y calendario, incluyendo controles organizativos, legales y técnicos (con especial referencia al ENS en el sector público).

Soporte instrumental:

- La herramienta Excel incorpora un apartado de “Plan de Tratamiento del Riesgo” con campos para identificación del riesgo, estrategia, controles, responsables, recursos, fechas y verificación.

Resultado esperado de la fase IV: plan de acción priorizado y verificable que permita ejecutar y monitorizar la mitigación del riesgo.

4.4.5. Fase V — Seguimiento, verificación y revisión (mejora continua)

Objetivo: comprobar la eficacia real de las medidas adoptadas y activar revisiones cuando cambien condiciones del tratamiento.

La guía corporativa establece que el responsable debe prever revisiones periódicas (p. ej., anual) y también revisiones ante cambios sustanciales: modificaciones en tecnología, alcance, volumen, fines, contexto, incidencias/brechas, cambios normativos o sociales, etc.

Además, se enfatiza la necesidad de auditoría/verificación de eficacia: si las medidas no alcanzan el efecto esperado, el riesgo residual puede permanecer alto y exigir acciones adicionales o incluso decisiones de rediseño del tratamiento.

Resultado esperado de la fase V: ciclo de control continuo que sostiene el cumplimiento en el tiempo y refuerza la responsabilidad proactiva como práctica.

4.5. Evidencias, trazabilidad y mejora continua (qué genera el sistema y cómo se gobierna)

Una característica diferencial del modelo es que está diseñado para producir **artefactos y evidencias** alineados con el principio de responsabilidad proactiva. Esto es especialmente relevante en el sector público, donde la rendición de cuentas y la transparencia requieren documentación consistente y accesible.

4.5.1. Evidencias principales que genera el sistema

Sin perjuicio de la adaptación a cada organismo, el modelo impulsa evidencias tipo:

- **RAT corporativo actualizado**, con contenido publicable y contenido interno orientado a control.
- **Descripción de contexto y ciclo de vida del dato**, como base para el análisis del riesgo.
- **Listado de riesgos/factores aplicables** y justificación de probabilidad/impacto.
- **Determinación de riesgo inherente y residual**, y criterio del riesgo global (valor máximo) para priorización.
- **Decisión motivada sobre necesidad de EIPD** (cuando aplica) y documentación del juicio de proporcionalidad en la EIPD.

- **Plan de tratamiento del riesgo** con medidas, responsables, recursos, plazos y verificación.
- **Registros de seguimiento y revisiones** ante cambios sustanciales, incidencias o revisiones periódicas.

4.5.2. Trazabilidad: quién decide, con qué criterio y cuándo se revisa

La guía de riesgos recomienda que los informes documenten: quién realiza el análisis, quién lo aprueba, metodología empleada, riesgos identificados, decisión sobre EIPD, medidas y plan, criterios de revisión y fecha. Esta estructura de documentación refuerza la trazabilidad y la capacidad de auditoría.

La guía del RAT, a su vez, incorpora un procedimiento orientativo para la creación/modificación/publicación de tratamientos, incluyendo intervención del DPD y comunicación de cambios, reforzando la trazabilidad institucional del inventario publicado.

4.5.3. Mejora continua y evolución del modelo

El sistema está concebido para evolucionar: incorpora mecanismos de revisión del riesgo y de adaptación a cambios tecnológicos y organizativos, así como a nuevos escenarios (p. ej., automatización e IA) que pueden alterar el contexto de amenaza.

En términos corporativos, esto se traduce en:

- actualización periódica de guías y plantillas,
- alineación con criterios de autoridades de control,
- retroalimentación de unidades usuarias y roles implicados,
- y capacidad de incorporar nuevas necesidades de gobernanza y seguridad.

5. Registro de Actividades de Tratamiento (RAT) como eje del modelo (metodología corporativa y transparencia)

5.1. Finalidad del RAT en el modelo corporativo: de inventario a “palanca” de responsabilidad proactiva

El RAT constituye el punto de partida del cumplimiento del RGPD en la Junta de Andalucía, al permitir identificar y describir de forma estructurada los tratamientos de datos personales que se realizan bajo responsabilidad de cada organismo o centro directivo.

En el modelo corporativo implantado, el RAT no se concibe únicamente como una obligación formal de registro, sino como un **instrumento vertebrador** que habilita:

- **Transparencia** hacia la ciudadanía mediante la publicación del inventario de tratamientos accesible por medios electrónicos.

- **Coherencia interna**: facilitar una descripción homogénea de tratamientos (finalidades, bases jurídicas, categorías de interesados y datos, destinatarios, conservación, referencias a seguridad).
- **Responsabilidad proactiva**: incorporar información adicional para control interno que permita conectar el tratamiento con el análisis de riesgos y, cuando proceda, con la evaluación de impacto.

En suma, el RAT actúa como "columna vertebral" del sistema: **un RAT bien construido** reduce ambigüedades, evita duplicidades y hace viable la gestión del riesgo de manera sostenible y revisable.

5.2. Criterios corporativos para identificar y configurar tratamientos (unidad de criterio)

La guía corporativa de la Junta de Andalucía establece que, para conformar un RAT útil y mantenible, es imprescindible decidir un nivel de agregación/segregación adecuado y aplicar criterios comunes, evitando asociar automáticamente cada procedimiento administrativo a un tratamiento independiente.

5.2.1. Qué se entiende por "tratamiento"

Partiendo de la definición del RGPD (conjunto de operaciones sobre datos personales), el RAT debe reflejar actividades de tratamiento con sentido operativo: con fines y elementos comunes que permitan gestionar riesgos y obligaciones asociadas.

5.2.2. Buenas prácticas para identificar tratamientos

La guía corporativa propone criterios prácticos (no exhaustivos) para identificar tratamientos de forma consistente, por ejemplo:

- **Partir de los antiguos ficheros notificados** (como referencia histórica) y adaptarlos al RGPD.
- **Basar tratamientos en competencias y esferas de decisión**, de modo que el tratamiento se relacione con fines y medios determinados por el órgano competente.
- **Agrupar procesos/procedimientos con nexo común** (normativa reguladora, finalidad, base jurídica, categorías de interesados y datos) bajo un mismo tratamiento, evitando duplicidades.
- **Englobar el ciclo de vida completo** de la información dentro del tratamiento (recogida, uso, publicaciones, evaluaciones, etc.), lo que mejora la gestión de riesgos.

5.2.3. Malas prácticas que deben evitarse

La guía identifica prácticas erróneas que deterioran la calidad del RAT y dificultan el cumplimiento real, entre ellas:

- **Identificar tratamiento con procedimiento administrativo concreto** (genera proliferación y duplicidades).
- **Identificar un tratamiento por cada fase del procedimiento** (se recomienda integrar bajo una finalidad común).
- Crear “cajones de sastre” o tratamientos-buzón (“Agenda”, “Contactos”, “Gestión interna”) sin finalidad clara ni responsable definido.
- **Confundir tratamiento con sistema o soporte** (“Consultas GIRO”, “Base de datos Access”, “Archivo de papel”): el sistema es relevante para seguridad, pero no define el tratamiento.
- **Identificar tratamientos por unidades administrativas** sin delimitar finalidades, datos, cesiones, etc.

Criterio clave de diseño corporativo: el tratamiento debe describirse por su **finalidad** y por el conjunto de operaciones coherentes que integra, no por su instrumento (sistema/archivo), ni por el procedimiento aislado, ni por la unidad.

5.3. Determinación del Responsable del tratamiento (criterio jurídico-operativo)

La identificación correcta del **Responsable del tratamiento** es esencial para que el RAT sea útil y para garantizar la responsabilidad proactiva. La guía corporativa establece pautas para determinarlo, apoyándose en la definición del RGPD y en criterios doctrinales, advirtiendo que no es adecuado atribuir genéricamente la responsabilidad al conjunto de la “Junta de Andalucía” sin análisis de hecho y de derecho.

5.3.1. Criterio general

El Responsable será quien determine fines y medios esenciales del tratamiento. La determinación puede venir:

- por **situaciones de derecho** (normas que atribuyen competencias y por tanto requieren el tratamiento), o
- por **situaciones de hecho** (quién decide de manera efectiva elementos esenciales).

5.3.2. Aplicación práctica en el ámbito corporativo

En la práctica, la guía señala que, en Consejerías, se viene identificando como responsables a los **Centros Directivos**; y en entes instrumentales, a órganos equivalentes o gerencias, sin perjuicio del análisis caso por caso.

5.3.3. Corresponsabilidad

Se contempla que, cuando dos o más entidades determinan conjuntamente fines y medios de una operación de tratamiento, puede existir corresponsabilidad, que debe

articularse mediante un acuerdo o instrumento que delimite funciones y responsabilidades.

6. Evaluación de Impacto (EIPD) y proporcionalidad (garantías reforzadas)

6.1. Cuando procede una EIPD: criterio corporativo de activación por alto riesgo

La Evaluación de Impacto en Protección de Datos (EIPD) se integra en la metodología corporativa como una actividad **indivisible de la gestión de riesgos** para los derechos y libertades. En el modelo adoptado, la EIPD no se entiende como un trámite aislado, sino como un instrumento para **apoyar decisiones** que afectan al diseño, alcance o funcionamiento de un tratamiento cuando existe un riesgo elevado.

6.1.1. Regla general: el "disparador" es el riesgo inherente

El criterio operativo central del modelo es que la decisión de realizar una EIPD debe basarse en el **riesgo inherente (o intrínseco)** del tratamiento: el riesgo calculado antes de considerar medidas mitigadoras concretas. Si el riesgo inherente es **alto o muy alto**, debe realizarse EIPD.

Idea clave para el jurado: la EIPD se activa por el riesgo "de partida" que el tratamiento entraña para las personas, no por la "tranquilidad" que produzcan medidas a posteriori.

6.1.2. Supuestos típicos de EIPD (criterios normativos y doctrinales)

La metodología corporativa recopila y alinea los supuestos en los que la normativa y las autoridades de control consideran probable un alto riesgo, incluyendo (de forma no exhaustiva):

- Evaluaciones sistemáticas y exhaustivas basadas en tratamiento automatizado (incluido perfilado) con efectos jurídicos o significativamente similares.
- Tratamiento a gran escala de categorías especiales de datos o de datos relativos a condenas e infracciones.
- Observación sistemática a gran escala de una zona de acceso público.
- Criterios y listados de alto riesgo difundidos por autoridades de control (criterios AEPD/CEPD, entre otros), que incluyen, por ejemplo, sujetos vulnerables, nuevas tecnologías, combinación/enlace de bases de datos, impedimento del ejercicio de derechos, etc.

6.1.3. Momento idóneo: concepción y diseño (y también revisiones)

La guía corporativa establece que la EIPD debe ejecutarse preferentemente en fases de **concepción y diseño** del tratamiento, para que funcione como herramienta de decisión y se cumpla el principio de privacidad desde el diseño y por defecto. No obstante, también puede ser necesaria para tratamientos ya vigentes cuando se revisan riesgos por cambios relevantes (tecnología, fines, alcance, incidencias, etc.).

6.1.4. Recomendación ante duda

Como criterio de prudencia y responsabilidad proactiva, cuando existan dudas razonables sobre la necesidad de EIPD, se recomienda su realización, en línea con directrices doctrinales.

6.2. EIPD como herramienta de decisión: juicio de idoneidad, necesidad y proporcionalidad

En el modelo corporativo, la EIPD incorpora de manera estructurada la evaluación de **necesidad y proporcionalidad** del tratamiento, conforme a los requisitos del RGPD y la doctrina aplicada. Esta evaluación no es un mero formalismo: determina si el tratamiento es viable tal y como está planteado o si debe rediseñarse.

6.2.1. Juicio de idoneidad (¿sirve realmente para el fin perseguido?)

El juicio de idoneidad exige demostrar, de forma objetiva y basada en evidencias, que el tratamiento es **adecuado** para la finalidad y puede alcanzar un nivel suficiente de eficacia. La metodología recomienda:

1. definir un **umbral de efectividad** (por ejemplo: margen de error, porcentaje mínimo de detección, tasa máxima de fraude u otros indicadores verificables), y
2. evaluar si el tratamiento, tal y como se diseña, cumple ese umbral.

Clave: si la eficacia no se puede justificar con evidencias, el tratamiento no supera el juicio de idoneidad y debe replantearse.

6.2.2. Juicio de necesidad (¿hay alternativas menos intrusivas igual de eficaces?)

El juicio de necesidad requiere analizar si la finalidad pudiera alcanzarse mediante opciones menos lesivas para la privacidad:

- verificar la relevancia de los fines,
- comprobar que cada operación de tratamiento es pertinente para esos fines, y
- justificar que no existen alternativas igualmente eficaces con menor impacto (p. ej., datos menos intrusivos, anonimización/seudonimización, reducción de alcance, limitación de colectivos, tecnologías menos invasivas, ajustes procedimentales).

6.2.3. Juicio de proporcionalidad en sentido estricto (balance daño–beneficio)

Una vez acreditada idoneidad y necesidad, la proporcionalidad en sentido estricto implica:

1. describir el **impacto** del tratamiento en derechos y libertades (basado en el análisis de riesgos),
2. detallar **medidas compensatorias** incorporadas para disminuir ese impacto,

3. identificar **beneficios** del tratamiento para las personas y el interés general (beneficio social),
4. comprobar la **simetría de la información** (misma calidad en la justificación del beneficio que en la descripción del daño), y
5. realizar el análisis **BDB (Balance Daño–Beneficio)**, concluyendo si los beneficios compensan el impacto.

Nota estructural: el modelo recuerda que nunca puede vaciarse el contenido esencial del derecho a la protección de datos; si el impacto es desproporcionado, el tratamiento debe modificarse o no realizarse.

6.2.4. Decisión final de la EIPD: continuar, modificar o descartar

El resultado de los juicios debe culminar en una decisión clara sobre la viabilidad del tratamiento. Si la evaluación es desfavorable, debe identificarse qué elementos deben modificarse (fines, datos, alcance, tecnología, medidas, etc.) para superar los juicios.

6.3. Contenido mínimo de una EIPD (estructura corporativa de documentación)

La metodología corporativa enfatiza que la documentación de la EIPD debe estar disponible como evidencia de responsabilidad proactiva y, en su caso, para actuaciones ante autoridades de control. Aunque no existe un formato único obligatorio, se recomienda una estructura coherente con modelos de referencia del sector público.

6.3.1. Elementos esenciales de la documentación

Como contenido mínimo práctico, una EIPD debe recoger:

- Descripción sistemática del tratamiento (naturaleza, ámbito, contexto y fines).
- Categorías de datos e interesados, destinatarios, transferencias, conservación y medios/tecnologías.
- Evaluación de necesidad y proporcionalidad (juicios de idoneidad, necesidad y proporcionalidad estricta).
- Identificación y evaluación de riesgos (amenazas, probabilidad, impacto, riesgo inherente y residual).
- Medidas previstas para abordar los riesgos y garantizar cumplimiento (controles organizativos, legales y técnicos; coherencia con ENS).
- Participación/consulta del DPD y, cuando proceda, de actores relevantes del tratamiento (técnicos, seguridad, encargados).

6.4. Consulta previa a la Autoridad de Control (CTPDA): cuándo y cómo se articula

La metodología contempla la posibilidad de **consulta previa** a la autoridad de control (Consejo de Transparencia y Protección de Datos de Andalucía) cuando el tratamiento,

aun incorporando medidas, mantenga riesgos residuales elevados o en supuestos en los que proceda por normativa.

6.4.1. Criterio de activación: riesgo residual inaceptable

La consulta previa se concibe como una medida excepcional para escenarios en los que:

- se ha realizado EIPD,
- se han propuesto y evaluado medidas, y
- persisten riesgos residuales que no se consideran aceptables (o existe obligación de consultar por la naturaleza del tratamiento).

6.4.2. Requisitos previos (condiciones de "madurez" documental)

Antes de consultar, la metodología señala requisitos esenciales:

- intervención y asesoramiento del DPD,
- definición clara de fines y medios del tratamiento,
- evaluación de conformidad RGPD documentada,
- gestión de riesgos completa (EIPD incluida),
- medidas y garantías identificadas,
- y superación (o análisis justificado) del juicio de necesidad/proporcionalidad.

6.4.3. Contenido orientativo de la consulta

La consulta debe incorporar información suficiente para que la autoridad de control valore el tratamiento: responsabilidades de los implicados, fines/medios, medidas y garantías, datos de contacto del DPD, la EIPD y cualquier información adicional requerida.

La EIPD se realiza cuando el tratamiento presenta un riesgo inherente alto o muy alto (o concurre un supuesto normativo/doctrinal). Se integra en la gestión del riesgo y debe ejecutarse preferentemente en diseño/concepción. La EIPD evalúa idoneidad (umbral de eficacia), necesidad (alternativas menos intrusivas) y proporcionalidad estricta (balance daño–beneficio), además de documentar riesgos, medidas y decisión final. Si el riesgo residual permanece inaceptable, se contempla consulta previa a la autoridad de control, aportando EIPD completa, medidas y datos de contacto del DPD.

7. Herramientas operativas y guías de apoyo (soporte instrumental de la metodología)

7.1. Principios de diseño del paquete instrumental (por qué estas herramientas y no otras)

La metodología corporativa se concibe como un **sistema aplicable** en una organización pública compleja. Para ello, se diseñó un "paquete instrumental" compuesto por **guías** (criterios y procedimiento) y una **herramienta operativa** (soporte de ejecución) con los siguientes principios de diseño:

1. **Secuencialidad y guiado**: la herramienta ordena el análisis en pasos, evitando omisiones y facilitando que unidades no especializadas avancen de forma coherente por el proceso.

2. **Trazabilidad y evidencia**: todo dato introducido debe poder relacionarse con una decisión, un control y un resultado (riesgo inherente/residual), de modo que la responsabilidad proactiva sea demostrable.

3. **Alineación normativa y doctrinal**: la estructura y el contenido se alinean con RGPD/LOPDGDD y con guías y criterios de autoridades de control, y se integra la coherencia con medidas de seguridad y marcos del sector público (ENS).

4. **Modularidad y reutilización**: se diseñan módulos/pestañas independientes pero conectadas, reutilizables en múltiples tratamientos y escalables a distintos niveles de madurez.

5. **Ayuda contextual y reducción de errores**: se incorporan instrucciones y ayudas en la propia herramienta para minimizar interpretaciones divergentes y favorecer la homogeneidad.

6. **Compatibilidad con la gestión ordinaria**: se opta por un formato accesible y ampliamente disponible en la organización para facilitar adopción, actualización y transferencia interna sin barreras tecnológicas.

7.2. Componentes del soporte instrumental (qué integra el sistema)

El soporte instrumental se compone de dos bloques complementarios:

7.2.1. Guías corporativas (criterio común)

- **Directrices para la elaboración y mantenimiento del RAT**: establecen criterios para identificar tratamientos, buenas/malas prácticas, campos obligatorios y contenido adicional interno, así como pautas de publicación y relación con procedimientos/inventarios.

- **Directrices para la gestión de riesgos y EIPD**: definen el proceso por fases (contexto, amenazas, evaluación, plan, seguimiento), criterios de riesgo inherente/residual, y el encaje de la EIPD en la gestión del riesgo.

7.2.2. Herramienta operativa (ejecución y evidencia)

- **Herramienta Excel de gestión del riesgo y apoyo a EIPD**: implementa de forma secuencial la metodología, facilita la evaluación y genera salidas trazables (hoja resumen, plan de tratamiento del riesgo, validación).

Principio de integración: las guías aportan el "criterio" y el "cómo hacerlo"; la herramienta aporta el "cómo ejecutarlo de forma homogénea" y el "cómo dejar evidencia".

7.3. La herramienta Excel de gestión del riesgo: estructura, módulos y lógica de uso

La herramienta Excel se ha diseñado como un flujo guiado y modular, con pestañas que corresponden directamente a las fases metodológicas y a los apartados típicos de un informe de análisis de riesgos/EIPD.

7.3.1. Estructura general (pestañas/módulos)

De forma resumida, la herramienta incluye:

- **Portada y control del documento** (identificación, fecha, clasificación, estado).
- **Índice**: navegación por el proceso secuencial.
- **1. Actividad del tratamiento**: datos que alimentan el inventario/RAT (responsable, finalidad, interesados, datos, cesiones, conservación, medidas, base jurídica).
- **2. Descripción del contexto**: profundización en naturaleza/ámbito/contexto/fines, sistemas y operaciones, medidas de seguridad, IA, incidentes y brechas.
- **2.1 Ciclo de vida**: recogida, uso, conservación, cesión, bloqueo y supresión con detalle por fases.
- **3. Supuestos EIPD**: checklist de supuestos RGPD/LOPDGDD/criterios de autoridades para determinar EIPD.
- **4. Factores de riesgo**: catálogo estructurado (por categorías) para seleccionar riesgos/amenazas aplicables.
- **5. Mitigación / riesgo residual**: identificación de controles, madurez, justificación y cálculo de riesgo residual.
- **6. Juicio de proporcionalidad**: idoneidad, necesidad y proporcionalidad (con medidas compensatorias y beneficios).
- **7. Plan de tratamiento del riesgo**: estrategia, controles a implantar, responsables, recursos, fechas y verificación.
- **8. Hoja resumen**: salida sintética para evidenciar conclusiones y facilitar su incorporación a informes.

- **9. Validación**: registro de revisión/aceptación, observaciones y fechas (incluida intervención del DPD).
- **10. Controles / catálogos** y hojas de **datos/fórmulas/ayuda**: lógica de cálculo, escalas, criterios de aceptación y soporte al usuario.

7.3.2. Lógica de cálculo y consistencia interna

La herramienta incorpora:

- **niveles de riesgo** (bajo/medio/alto/muy alto) y reglas para riesgo inherente y residual;
- **madurez de controles** (desde inexistente hasta optimizado) para estimar mitigación;
- y **criterios de aceptación/estrategia** (mitigar, evitar, transferir, aceptar) como salida operativa del análisis.

7.4. Ventajas operativas, reutilización y escalabilidad (por qué es una buena práctica)

7.4.1. Ventajas operativas (implantación realista)

El objetivo perseguido con el desarrollo continuo de una herramienta soporte pasa por los siguientes elementos:

- **Estandariza** el modo de describir tratamientos y evaluar riesgos, reduciendo variabilidad entre unidades.
- **Automatiza** parte del trabajo repetitivo (cálculos, consistencia de escalas, resumen), disminuyendo errores.
- **Facilita auditoría y rendición de cuentas**, al producir evidencias trazables (riesgos, controles, plan, validación).
- **Integra la dimensión organizativa y técnica**, permitiendo registrar controles y madurez, y vincularlo a medidas y verificación.

7.4.2. Reutilización y escalabilidad (modelo transferible)

El diseño modular actual permite:

- aplicar la herramienta a **nuevos tratamientos** sin reconstruir metodología (solo cambiando inputs);
- incorporar **nuevos factores de riesgo o controles** conforme evolucionan criterios o contextos tecnológicos;

- extenderla a unidades con distintos niveles de madurez, manteniendo un núcleo común comparable;
- y facilitar la **replicabilidad** en otras administraciones públicas, al basarse en un proceso por fases y artefactos reutilizables (guías + herramienta).

8. Gobernanza, implantación y resultados (despliegue y evidencia)

8.1. Modelo de gobernanza y roles (responsabilidad distribuida con coordinación corporativa)

El modelo implantado se apoya en una gobernanza que combina **responsabilidad distribuida** (cada responsable del tratamiento gestiona sus tratamientos) con **coordinación corporativa** (criterios, herramientas y acompañamiento comunes). Este enfoque es coherente con el principio de responsabilidad proactiva y con la necesidad de integrar la gestión del riesgo en la operativa diaria.

8.1.1. Roles mínimos y participación obligatoria

La metodología corporativa define la intervención, al menos, de los siguientes roles en la gestión del riesgo y, cuando proceda, en la EIPD:

- **Responsable del tratamiento** (centro directivo u órgano competente): titular de la decisión, aprobación del análisis y de las medidas.
- **Técnicos/gestores del tratamiento**: aportan conocimiento operativo del ciclo de vida del dato, procedimientos y uso real de la información.
- **Técnicos TIC/seguridad y responsable de seguridad**: evalúan y proponen medidas técnicas y organizativas; aportan visión de seguridad de la información alineada con ENS.
- **Delegado/a de Protección de Datos (DPD)**: asesoramiento y supervisión; participa especialmente en revisiones del RAT, análisis de riesgos y EIPD, sin asumir la responsabilidad del tratamiento.
- **Encargados y subencargados**: participan cuando realizan operaciones por cuenta del responsable, especialmente para medidas y garantías en el tratamiento y seguridad.

8.1.2. Papel de la Agencia Digital de Andalucía (ADA) y la integración con ENS

El modelo incorpora explícitamente la necesidad de integrar riesgos de protección de datos con riesgos de los sistemas de información (confidencialidad, integridad, disponibilidad…), dada la convergencia entre RGPD y el marco ENS en el sector público. En este contexto, la guía corporativa destaca la participación de áreas TIC y de la **Agencia Digital de Andalucía (ADA)** en la valoración de sistemas, redes e

infraestructuras y en la gestión del riesgo tecnológico, especialmente en tratamientos automatizados donde actúa como encargado.

8.2. Estrategia de implantación (despliegue progresivo y acompañamiento)

La implantación se planteó como un proceso progresivo que permite avanzar desde un punto de partida heterogéneo hacia un marco común, con iteraciones y mejora continua. La metodología por fases (I–V) facilita este despliegue porque permite "entrar" por la revisión del tratamiento y escalar hacia análisis de riesgos y EIPD cuando corresponde.

8.2.1. Enfoque por iteraciones: empezar por consistencia y ganar profundidad

La estrategia operativa se articula típicamente en tres niveles de madurez:

1. **Nivel 1 — Normalización del RAT**: unificar criterios de identificación, finalidad y contenido, evitando prácticas erróneas (tratamiento ≠ procedimiento ≠ sistema ≠ unidad).
2. **Nivel 2 — Gestión del riesgo aplicada**: describir contexto y ciclo de vida, identificar factores y valorar riesgo inherente/residual para priorizar medidas.
3. **Nivel 3 — EIPD y proporcionalidad**: activar EIPD en tratamientos de alto riesgo, incorporando juicios de idoneidad/ necesidad/ proporcionalidad y decisiones justificadas.

8.2.2. "Instrumentos + proceso": implantación centrada en artefactos reutilizables

El despliegue se apoya en un paquete instrumental que reduce variabilidad interpretativa:

- guías corporativas (RAT y riesgos/EIPD),
- y herramienta Excel secuencial con módulos de contexto, riesgos, mitigación, proporcionalidad, plan y validación.

8.2.3. Integración con la operativa administrativa

La guía del RAT recomienda coherencia con inventarios procedimentales y cláusulas informativas, evitando equivalencias automáticas procedimiento=tratamiento, para mantener el sistema útil y mantenible.

8.3. Formación, acompañamiento y comunidad de práctica (cultura de privacidad)

La sostenibilidad del modelo exige que las unidades responsables dispongan de **capacidad real** para aplicarlo. Por ello, el despliegue se acompaña de acciones de transferencia de conocimiento y soporte continuado.

8.3.1. Formación orientada a la práctica

El programa de formación se ha orientado a:

- explicar el enfoque basado en riesgos,

- enseñar a describir correctamente tratamientos (finalidad, base jurídica, categorías, ciclo de vida),
- y entrenar el uso de la herramienta operativa (paso a paso por pestañas, outputs y validación).

En 2025 se formaron 60 personas en gestión de riesgos con esta metodología y en 2026 está prevista formación adicional (30 personas), además de acciones de difusión y trabajo colaborativo.

8.3.2. Acompañamiento y soporte "en casos reales"

El despliegue se apoya en:

- asesoramiento del DPD (revisión y recomendaciones),
- participación TIC/seguridad/ADA cuando el tratamiento exige medidas técnicas o afecta a sistemas,
- y uso de artefactos comunes (plantillas y herramienta) para resolver dudas recurrentes y mantener coherencia.

8.3.3. Comunidad de práctica y coordinación

La red de DPD y espacios de trabajo colaborativo favorecen la homogeneización, detectan áreas de mejora y facilitan la actualización del modelo, reforzando el enfoque de mejora continua.

8.4. Medición y evidencia de implantación (encuesta diagnóstica y trazabilidad)

Un elemento diferencial del proyecto es incorporar medición del grado de implantación y uso, como manifestación práctica del principio de responsabilidad proactiva: evaluar si el sistema funciona, dónde se usa y qué necesita mejora.

8.4.1. Encuesta diagnóstica: propósito y utilidad

La medición se concibe para:

- obtener evidencia del grado de conocimiento y utilización,
- identificar barreras (capacidad, recursos, dudas frecuentes),
- priorizar formación y mejoras,
- y consolidar un ciclo de mejora continua basado en experiencia real.

8.4.2. Trazabilidad generada por la herramienta

La herramienta Excel refuerza la evidencia operativa mediante:

- hoja resumen, plan de tratamiento del riesgo y módulo de validación (fechas, responsables, observaciones),
- relación directa entre factores seleccionados, controles y nivel de riesgo residual,

- y soporte al seguimiento posterior (planificación, verificación y revisión).

8.5. Resultados (cuantitativos y cualitativos) e impactos observados

Los resultados se presentan en dos planos: **resultados cuantitativos de despliegue** y **resultados cualitativos de mejora del control y la decisión**.

8.5.1. Resultados cuantitativos (despliegue)

- **Volumen corporativo**: RAT con 2.291 tratamientos; estructura con 13 Consejerías y 102 organismos (incl. sector instrumental).
- **Adopción inicial**: implantación en 7 organismos desde 2024.
- **Ejecución metodológica**: 237 análisis de riesgos y 66 EIPD realizadas con la metodología.
- **Capacitación**: 60 personas formadas en 2025 y plan de 30 en 2026, más acciones de difusión.

8.5.2. Resultados cualitativos (qué mejora y por qué)

a) Homogeneización de criterios

La guía de RAT establece buenas/malas prácticas y evita errores típicos (tratamiento≠procedimiento, tratamiento≠sistema, tratamientos “cajón de sastre”), lo que reduce duplicidades y mejora consistencia del inventario.

b) Mejora de trazabilidad y defensabilidad

La metodología exige documentar contexto, riesgos, decisión EIPD por riesgo inherente, medidas, plan y revisión. Esta estructura fortalece la capacidad de auditoría y la rendición de cuentas.

c) Integración del riesgo en la toma de decisiones

El modelo consolida decisiones basadas en riesgo (probabilidad×impacto, riesgo inherente vs residual), evitando análisis genéricos y permitiendo priorizar mitigaciones.

d) Coherencia con seguridad (ENS) y participación técnica

La guía de riesgos integra la visión de seguridad de la información y recomienda coordinación con TIC/ADA y con el ENS, reforzando medidas técnicas y organizativas y la visión integral del tratamiento.

e) EIPD como garantía reforzada (proporcionalidad y alternativas)

En tratamientos de alto riesgo, el juicio de idoneidad/necesidad/proporcionalidad y el balance daño–beneficio orientan rediseños y medidas compensatorias, vinculando EIPD a decisiones reales, no a un documento aislado.

f) Sostenibilidad: revisión y mejora continua

La metodología identifica activadores de revisión (cambios en tecnología, alcance, fines, incidencias, marco normativo) y promueve revisión periódica, lo que hace el sistema sostenible.

8.6. Lecciones aprendidas y próximos pasos (roadmap 12–24 meses)

La implantación en un entorno amplio y diverso aporta aprendizajes relevantes y líneas claras de evolución:

8.6.1. Lecciones aprendidas (síntesis)

1. **Sin un RAT consistente no hay gestión del riesgo sostenible**: el esfuerzo de normalización del RAT es condición previa para análisis de riesgos de calidad.
2. **La herramienta reduce variabilidad y genera evidencia**, pero requiere acompañamiento inicial para consolidar criterios comunes.
3. **La integración con TIC/ENS es imprescindible**: muchos riesgos se materializan en el plano tecnológico; la coordinación con ADA y seguridad mejora eficacia de medidas.
4. **La EIPD debe "servir para decidir"**: cuando se aborda como instrumento de diseño (idoneidad/necesidad/proporcionalidad) genera mejoras reales; cuando se aborda como trámite, pierde valor.

8.6.2. Próximos pasos (orientativos)

- **Extender implantación** a más organismos, priorizando ámbitos con datos especialmente sensibles o gran escala.
- **Consolidar el ciclo de revisión anual** y los activadores de reevaluación en tratamientos críticos, integrándolo con gobernanza de seguridad/ENS.
- **Refinar catálogos de riesgos y controles** conforme evolucionen tecnologías (automatización/IA) y experiencia de uso.
- **Potenciar medición periódica** (encuestas/indicadores) para evidenciar adopción y orientar mejora continua.

El modelo ha permitido estandarizar el RAT y conectar su contenido con la gestión del riesgo y la EIPD en un flujo trazable. La herramienta operativa genera evidencias (hoja resumen, plan y validación) y facilita revisiones periódicas. La gobernanza distribuye responsabilidades, incorpora asesoramiento del DPD y coordinación con TIC/ADA y ENS, y se apoya en formación y acompañamiento. El proyecto incorpora medición de implantación como práctica de accountability y se orienta a escalado progresivo y mejora continua.

La gobernanza y el despliegue del modelo han convertido la protección de datos en un proceso corporativo operativo: criterios homogéneos (RAT), gestión del riesgo por fases, EIPD cuando procede y planes verificables, con medición y mejora continua, y con una

integración efectiva de seguridad/ENS y coordinación TIC/ADA para sostener el cumplimiento en el tiempo.

Anexo I. Modelo de publicación y aprobación del RAT

Junta de Andalucía

<Organismo>
<Centro Directivo>

RESOLUCIÓN DE LA <CENTRO DIRECTIVO> POR LA QUE SE ACTUALIZA SU REGISTRO DE ACTIVIDADES DE TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL DE LAS QUE ES RESPONSABLE Y SE ORDENA SU PUBLICACIÓN EN EL PORTAL DE LA JUNTA DE ANDALUCÍA

La aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en adelante Reglamento General de Protección de Datos o RGPD, supone la necesidad por parte de los responsables del tratamiento de aplicar a su actividad el principio de responsabilidad proactiva demostrable en el ámbito de la protección de datos personales, de conformidad con su artículo 5.2, siendo el responsable del tratamiento el responsable del cumplimiento de las exigencias señaladas en el apartado 1 del mismo artículo, relativas a la licitud, lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación e integridad y confidencialidad.

A este respecto, el artículo 4.7) del RGPD define al responsable del tratamiento como la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento, diferenciándola de la figura del encargado del tratamiento o encargado, definida en el apartado 8 siguiente, como la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Una de las principales obligaciones para el responsable del tratamiento, que comporta el principio de responsabilidad activa demostrable, y en su caso, de su representante, es llevar un registro de actividades de tratamiento (RAT) efectuadas bajo su responsabilidad, en cumplimiento de lo establecido en el artículo 30 del Reglamento general de protección de datos y el 31 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Dicho RAT debe ponerse a disposición de la autoridad de control que lo solicite, debiendo hacerse público por medios electrónicos un inventario de las actividades de tratamiento que contiene, respecto de cada una de ellas, la información establecida por el artículo 30.1 del Reglamento general de protección de datos; esto es: *a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos; b) los fines del tratamiento; c) una descripción de las categorías de interesados y de las categorías de datos personales; d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales; e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas; f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos; g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.*

De conformidad con el artículo XX de la Orden de X de XXX de 20XX, por la que se establece la política de la seguridad de las tecnologías de la información y comunicaciones en el ámbito de la Consejería de XXX, será responsable de la información la persona con capacidad de decisión sobre la finalidad, contenido y uso de la información. Esta responsabilidad recaerá en la persona titular del órgano directivo central o periférico, o en su caso, órgano colegiado en cuyo ámbito de decisión se incluya la información tratada. A los efectos previstos en el RGPD y en la Ley Orgánica 3/2018, de 5 de diciembre, el responsable de

la información tendrá, asimismo, respecto de los datos personales contenidos en la información incluida en su ámbito de actuación, la consideración de responsable del tratamiento.

Asimismo, en el citado artículo 13 de la Orden de 7 de diciembre de 2023, además de establecerse las funciones del responsable de la información, en el apartado 4 se dispone que como responsable del tratamiento le corresponderá, adoptar la decisión sobre la creación del tratamiento, su finalidad, así como el contenido y uso de los datos tratados a lo largo de todo el ciclo de vida del tratamiento. La información actualizada de dicho responsable junto a sus tratamientos se recogerá en el Registro de Actividades de Tratamiento de la Consejería, de conformidad con lo establecido en el artículo 31 de la Ley Orgánica 3/2018, de 5 de diciembre.

De acuerdo con ello, corresponde a este <Centro directivo> llevar un registro de actividades de tratamiento y consecuentemente resolver sobre la inscripción en el mismo de las altas, modificaciones y bajas de actividades de tratamiento al objeto de que sea un fiel reflejo de las actividades de tratamiento de las que en cada momento sea responsable, así como ordenar su publicación electrónica.

El contenido de este RAT es el establecido en el artículo 30.1 del Reglamento General de Protección de Datos, en el formato aprobado por la Comisión Interdepartamental de Coordinación y Racionalización Administrativa con fecha 22 de marzo de 2018 para toda la Administración de la Junta de Andalucía, incluyendo la base legal de cada tratamiento.

Se ha apreciado la necesidad de actualizar el RAT de este/a (*identificar el órgano directivo)* como consecuencia de *(describir someramente la causa que motiva la actualización: de forma general o porque se trata de una actividad de tratamiento que debe inscribirse por resultar nueva - ya sea porque una norma lo determina o porque no se ha inscrito aún - o cuando se pretende la modificación de una actividad de tratamiento ya inscrita. Si se trata de una nueva actividad de tratamiento hay que identificarla y describir su finalidad).*

A la vista de los antecedentes anteriormente descritos y en el uso de las competencias que tengo atribuidas por el Decreto 164/2022, de 9 de agosto, por el que se establece la estructura orgánica de la Consejería de Justicia, Administración Local y Función Pública,

RESUELVO

Primero.- Actualizar el Registro de Actividades de Tratamiento de <Centro directivo>, quedando conformado del modo en que figura en el Anexo a esta resolución, a efectos del cumplimiento de la obligación establecida en el artículo 30 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y el artículo 31 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Segundo.- Ordenar que, para el cumplimiento de la obligación de publicar un inventario de actividades de tratamiento accesible por medios electrónicos, se publique el Registro de Actividades de Tratamiento (RAT) correspondiente a <Centro directivo>, salvo los datos de carácter personal que contenga

y no deban ser objeto de publicación, en el apartado "Protección de datos" del Portal de la Junta de Andalucía, pudiendo accederse al Inventario de actividades de tratamiento de datos, a través del siguiente enlace: https://juntadeandalucia.es/protecciondedatos/buscador.html

~~Tercero.-~~ Ordenar que se difunda entre las unidades administrativas y el personal adscrito a este órgano directivo el Registro de Actividades de Tratamiento del/de la <Centro directivo> y que se lleven a cabo las actuaciones necesarias para que se mantenga permanentemente actualizado.

~~Cuarto.-~~ Ordenar que se dé traslado de esta resolución al delegado de Protección de Datos de la <Consejería de >, en cumplimiento del deber de comunicarle cualquier adición, modificación o exclusión en el contenido del registro que recoge el artículo 31.1 párrafo tercero de la Ley Orgánica 3/2018, de 5 de diciembre.

~~Quinto.-~~ Las actualizaciones del Registro de Actividades de Tratamiento se formalizarán a través de la correspondiente resolución de este/a <Centro directivo>, salvo que se trate de correcciones de errores o de actualización de referencias normativas u orgánicas, en cuyo caso la actualización se remitirá directamente desde la Coordinación General de este órgano directivo, al delegado de Protección de Datos.

En Sevilla, a la fecha de la firma electrónica.

El cargo firmante

Fdo.: <Nombre>

Anexo II: Encuesta: Encuesta diagnóstico gestión del riesgo de protección de datos (Junta de Andalucía)

Disponible hasta el 30 de enero. Es una encuesta anónima.

Realizada por la Coordinación de Protección de Datos de la Consejería de Justicia, Administración Local y Función Pública. Se dirige a los y las DPD de la Junta de Andalucía con el fin de recabar la información necesaria de los responsables de tratamiento dentro de su organismo (protecciondedatos.sgap.cjalfp@juntadeandalucia.es). Gracias.

1. Seleccione el tipo de organismo:
   - Consejería
   - Agencia o entidad instrumental
   - Otras
2. ¿Cuántos tratamientos de datos personales tiene aproximadamente su organismo en los que actúa como responsable?
3. ¿Qué porcentaje de esos tratamientos tienen categorías especiales de datos (artículo 9 RGPD)?
4. ¿Qué porcentaje de tratamientos en su organismo tienen análisis de riesgos realizado?
5. ¿Qué porcentaje de tratamientos que precisan evaluación de impacto la tienen realizada?
6. ¿Qué herramienta utiliza su organismo para realizar análisis de riesgos en protección de datos?
   - Herramienta corporativa de la Junta de Andalucía
   - Herramienta propia del organismo
   - Herramienta de terceros
   - No realiza análisis de riesgos
7. ¿Con qué frecuencia se actualizan los análisis de riesgos?
   - Anualmente
   - Cada dos años
   - Solo cuando cambia el tratamiento
   - No existe un criterio definido
   - No se actualizan
8. ¿Considera adecuada la herramienta corporativa para la gestión del riesgo?
   - Sí
   - Parcialmente
   - No
   - No la conozco/ no la he utilizado
9. En caso de que no le resulte adecuada o parcialmente adecuada, ¿podría decirnos por qué?
10. En el caso de utilizar la herramienta corporativa de análisis de riesgos, ¿cuántos análisis ha realizado con la misma? (Ponga 0 si ninguno)
11. En el caso de utilizar la herramienta corporativa de evaluación de impacto, ¿cuántas evaluaciones ha realizado con la misma? (Ponga 0 si ninguna)

12. ¿Qué dificultades encuentra para realizar o actualizar los análisis de riesgos y evaluaciones de impacto?
    - Falta de recursos
    - Falta de formación
    - Falta de implicación de los responsables
    - Complejidad de la herramienta
    - Falta de tiempo
    - Otra (especificar)
13. ¿Quién realiza la gestión del riesgo en su organismo?
    - Responsables de tratamiento
    - DPD
    - Otros (indicar)_____
14. ¿Cómo valora el nivel de madurez de su organismo en gestión del riesgo de protección de datos?
    - Muy bajo
    - Bajo
    - Medio
    - Alto
    - Muy algo
15. ¿Qué apoyos considera más necesarios para mejorar la gestión del riesgo?
    - Formación
    - Herramienta corporativa
    - Acompañamiento técnico
    - Mayor implicación de los responsables de tratamiento
    - Recursos humanos o económicos
    - Otros (indicar):_____
16. Para terminar, ¿ve oportuno que exista una herramienta única de gestión del riesgo para toda la Junta de Andalucía?
17. Por favor, justifique su respuesta.