Consejería de Justicia, Administración Local y Función Pública
Secretaría General para la Administración Pública

Junta de Andalucía

Plan estratégico de protección de datos de la Junta de Andalucía 2024-2030

13 de noviembre de 2024

13/11/2024

ÍNDICE

ÍNDICE DE ILUSTRACIONES

LISTADO DE ABREVIATURAS Y ACRÓNIMOS

ADA: Agencia Digital de Andalucía.

AR: Análisis de riesgos.

CICRA: Comisión Interdepartamental de Coordinación y Racionalización Administrativa.

CTPDA: Consejo de Transparencia y Protección de Datos de Andalucía.

DPD: Delegado o Delegada de Protección de Datos.

EAPI: Estrategia para una Administración Pública Innovadora 2023-2030.

ENS: Esquema Nacional de Seguridad

EI / EIPD: Evaluación de Impacto de Protección de datos.

IAAP: Instituto Andaluz de Administración Pública

IGS: Inspección General de Servicios.

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

MAIN: Memoria de análisis de impacto normativo.

RAT: Registro de Actividades de Tratamiento.

RGPD: Reglamento General de Protección de Datos

RPS: Registro de Procedimientos y Servicios

RPT: Relación de Puestos de Trabajo.

SirHus: Sistema de Información de Recursos Humanos de la Junta de Andalucía.

TIC: Tecnologías de la Información y las Comunicaciones.

1. Introducción

La Constitución Española proclama como derecho fundamental la protección de las personas físicas en relación con el tratamiento de sus datos personales en el artículo 18.4, disponiendo que "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Siendo en su fecha uno de los máximos textos legales pioneros en el reconocimiento implícito de un derecho a la protección de los datos de carácter personal, si bien, en consonancia con las tendencias legislativas de su época lo consideraba una manifestación del más amplio derecho al honor, a la intimidad personal y familiar y a la propia imagen.

La rápida y constante evolución tecnológica ha planteado nuevos retos para la protección de los datos personales. La recogida y el intercambio de datos personales han aumentado de manera significativa en los últimos años. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades.

Las Administraciones Públicas tratan datos personales de ciudadanos y ciudadanas constantemente, en diferentes cuestiones, siendo en algunos casos tratamientos de datos sensibles. Por tanto, las Administraciones Públicas deben adaptarse a la normativa vigente, para garantizar la integridad y confidencialidad de la información personal que tratan en el desempeño de sus funciones. La Junta de Andalucía, con el fin de poder dar servicio a una población de aproximadamente 8,6 millones de personas, trata a diario miles de estos datos personales.

La Junta de Andalucía está inmersa en varias estrategias de transformación e innovación de la Administración Pública que van a suponer de aquí a 2030 numerosos cambios en múltiples dimensiones de la organización. Estos cambios no pueden poner en riesgo la privacidad de la ciudadanía. Este Plan Estratégico de Protección de datos de la Junta de Andalucía se ha elaborado como un proyecto innovador en sí mismo, con un plan de actuación a corto plazo con proyectos perfectamente definidos y otros proyectos a medio y largo plazo que se plantean inicialmente como líneas estratégicas de actuación y cuya definición y concreción se van refinando mediante procesos iterativos. Como resultado de la ejecución de los proyectos de transformación se irán produciendo cambios normativos, organizativos, metodológicos, de procesos y también tecnológicos en la Junta de Andalucía. Este Plan Estratégico de Protección de datos tiene un doble objetivo:

- Conseguir la excelencia en el cumplimento de la normativa vigente en materia de protección de datos.
- Velar porque la trasformación de la Administración que se está realizando se haga garantizando la integridad y confidencialidad de la información personal de los datos que se tratan en el desempeño de sus funciones.

A efectos de este Plan, se entienden comprendidos en su ámbito de aplicación, las personas que prestan sus servicios como Delegados/as de Protección de Datos, responsables de tratamientos de datos, encargado/as de tratamientos, así como todo el personal empleado público que presta sus servicios en la Administración de la Junta de Andalucía y su sector instrumental.

Los principios inspiradores de este Plan, como no podría ser de otra forma, están basados en los que establece la normativa en esta materia, los cuales son los siguientes:

- Licitud, lealtad y transparencia
- Limitación de la finalidad

- Minimización de los datos
- Exactitud
- Limitación del plazo de conservación
- Integridad y confidencialidad
- Responsabilidad proactiva.

Por otra parte, para su desarrollo se ha empleado la metodología para la elaboración de planes estratégicos propuesta por el Instituto Andaluz de Administración Pública (IAAP) y se ha sometido a un proceso de evaluación dentro del marco institucional de la evaluación de políticas públicas que la Junta de Andalucía está impulsando a través del IAAP.

De esta forma, y de acuerdo con la metodología establecida, se va a realizar una evaluación ex-ante del plan, con el objetivo final de analizar la idoneidad del mismo para alcanzar los objetivos planteados y se realizarán evaluaciones periódicas y una final a lo largo del marco temporal de ejecución.

Este plan, cuya primera versión se elaboró en 2023, se realiza con un enfoque iterativo, es decir, que pretende llegar a un resultado mediante aproximaciones sucesivas. Por tanto, inicialmente se seleccionaron un conjunto de objetivos y proyectos prioritarios a corto plazo, de modo que durante la ejecución del plan se actualiza el mismo en sucesivas iteraciones, adecuando la planificación a la evolución del entorno y de la situación interna. El presente documento incluye la actualización del plan realizada en octubre de 2024, de modo que los apartados de objetivos y líneas estratégicas, y programas de actuación, están plenamente actualizados, mientras que los anteriores corresponden a la situación del año 2023.

Los cambios realizados en esta iteración responden a los avances realizados desde 2023 y, sobre todo, a la elaboración de la Estrategia para una Administración Pública Innovadora 2023-2030[1]. Dicha estrategia está terminando de elaborarse y en su elaboración se ha puesto de manifiesto que hay determinados proyectos que la Junta de Andalucía debe realizar para los que hay que ser especialmente cuidadoso con la protección de datos aplicando el principio desde el diseño y por defecto, y que van a requerir la realización de proyectos innovadores también en el área de protección de datos.

Asimismo, la ejecución de cualquier estrategia requiere realizar seguimiento y formalizarlo mediante informes periódicos. Dado que se van a redefinir los objetivos, líneas, programas y proyectos de este plan estratégico, se ha considerado oportuno realizar un informe de seguimiento que refleje los avances en la ejecución del plan hasta la finalización del tercer trimestre de 2024. Se incluye dicho informe de seguimiento como anexo.

[1] Puede consultarse en https://juntadeandalucia.es/organismos/justiciaadministracionlocalyfuncionpublica/areas/administracion-publica/planificacion-estrateg.html

2. Marco jurídico y estratégico

La protección de datos personales es un derecho fundamental y así se encuentra recogido en la Constitución Española y en la Carta de los Derechos Fundamentales de la Unión Europea.

La tendencia a nivel europeo para la protección de este derecho fundamental ha sido la de garantizar la uniformidad normativa en todo su territorio y elevar la protección de las personas físicas en el marco de una sociedad cada vez más globalizada. Para ello se aprobó en el año 2016 el 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, en adelante RGPD), aplicable en todo el territorio de la Unión Europea desde el 25 de mayo de 2018.

El último párrafo del Reglamento dispone, "El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro". Pretende con su eficacia directa, superar los obstáculos que impidieron la finalidad armonizadora de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de esos datos. La transposición de la directiva por los Estados miembros se plasmó en diferencias apreciables en cada Estado en cuanto a la protección de los ciudadanos.

Han pasado algo más de 5 años desde su aplicabilidad y se ha convertido en una pieza fundamental y referente a nivel mundial en el ámbito de la protección de datos, siendo una de sus finalidades más relevantes, crear una cultura de protección de datos generalizada en los ciudadanos, en los responsables de tratamiento de datos y en las Administraciones Públicas en general.

Hasta el año 2018, la norma de referencia en nuestro país era la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal o LOPD, norma que actualmente se encuentra derogada. A raíz de la entrada en vigor del Reglamento General de Protección de Datos, se aprobó la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), que complementa y precisa las disposiciones del citado Reglamento.

El objetivo normativo no es el de prohibir o poner trabas al uso de la información, sino al contrario, pretenden que su uso respete los derechos y libertades de las personas físicas.

2.1. Normativa reguladora nacional y autonómica

A nivel estatal, la citada Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se marca un doble objetivo. Por una parte, adaptar el ordenamiento jurídico interno al Reglamento europeo y completar sus disposiciones, y por otra parte, introduce una novedosa regulación a fin de garantizar los derechos digitales de la ciudadanía. Así se proclama en su artículo 1 que señala que "el derecho fundamental de las personas físicas a la protección de datos personales, amparado en el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta Ley Orgánica".

Por otro lado, como respuesta a la progresiva evolución tecnológica de nuestra sociedad hay que destacar el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad cuyo principal objetivo es determinar la política de seguridad a implantar en el sector público, estableciendo sus principios básicos y los requisitos mínimos que permitan una protección adecuada de la información, frente al nuevo escenario de la ciberseguridad y el incremento considerable de los ciberataques.

En Andalucía, el artículo 82 del Estatuto de Autonomía de Andalucía (Ley Orgánica 2/2007, de 19 de marzo, de reforma del Estatuto de Autonomía para Andalucía) establece la competencia ejecutiva sobre protección de datos de carácter personal, gestionados por las instituciones autonómicas de Andalucía, Administración autonómica, Administraciones locales, y otras entidades de derecho público y privado dependientes de cualquiera de ellas, así como por las universidades del sistema universitario andaluz. En este sentido, la Ley 1/2014, de 24 de junio, de Transparencia de Andalucía, en su artículo 43, creó el Consejo de Transparencia y Protección de Datos de Andalucía, como autoridad independiente de control en materia de transparencia y protección de datos en la Comunidad Autónoma de Andalucía. Tiene la consideración de Administración Institucional, lo que significa que posee personalidad jurídica propia y plena autonomía e independencia en el ejercicio de sus funciones.

En el ámbito de la Administración de la Junta de Andalucía y de sus entidades instrumentales, la competencia relativa a la coordinación y seguimiento del cumplimiento de la normativa aplicable en materia de protección de datos está asignada a la Secretaría General para la Administración Pública, sin perjuicio de las competencias que en dicha materia puedan corresponder a otros órganos o entidades (art. 8.2.o) del 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). Dicho Decreto también asigna a esa Secretaría General la elaboración y tramitación de planes y programas relativos al ámbito de sus competencias, lo que justifica que sea este órgano directivo el que impulse este Plan Estratégico.

Otro órgano a destacar en materia de protección de datos es la Comisión Interdepartamental de Coordinación y Racionalización Administrativa (CICRA), órgano colegiado decisorio y de asesoramiento, que tiene como finalidad el análisis de la situación, la planificación, coordinación y seguimiento de cuantas medidas se adopten para la racionalización y transformación continua de la Administración Pública y tiene entre otras funciones la de acordar el desarrollo de medidas de ejecución e impulso en materia de protección de datos (artículo 5 del Decreto 622/2019, de 27 de diciembre, de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía).

2.2. Normativa de la Junta de Andalucía relacionada con la seguridad

En el ámbito de la seguridad, aunque fuera del ámbito específico de la protección de datos, la Junta de Andalucía dispone de una política de seguridad aprobada mediante el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, modificado por el Decreto 70/2017, de 6 de junio. Asimismo, dispone de una política de seguridad interior, aprobada mediante el Decreto 171/2020, de 13 de octubre, por el que se establece la Política de Seguridad Interior en la Administración de la Junta de Andalucía. Ambas políticas se encuentran íntimamente relacionadas, abarcando conjuntamente todos los aspectos relativos a la seguridad.

Bajo este paraguas normativo, la organización corporativa de la seguridad se fundamente en un Comité Corporativo de Seguridad Interior de la Junta de Andalucía, y en un Comité de Seguridad TIC de la Junta de Andalucía, integrando este último en su seno un Grupo de Respuesta a Incidentes TIC cuya función es la toma urgente de decisiones en caso de contingencia grave que afecte a la seguridad de sistemas de información críticos. Estos comités tienen como órganos de apoyo a una Unidad Corporativa de Seguridad Interior y a una Unidad de Seguridad TIC Corporativa.

En el ámbito sectorial, cada Consejería dispone de un Comité de Seguridad Interior y Seguridad TIC, con competencias en seguridad interior y seguridad TIC, que tiene dos unidades de apoyo: la Unidad de Seguridad Interior y la Unidad de Seguridad TIC.

Desde el punto de vista de la planificación estratégica de la seguridad, la Junta de Andalucía dispone de la Estrategia Andaluza de Ciberseguridad, aprobada en 2022, que constituye el vínculo entre la Administración Autonómica y la ciberseguridad, estableciendo las líneas maestras que deben llevarse a cabo para dar respuesta a los retos y desafíos de la sociedad andaluza. La Estrategia contiene los retos, objetivos y líneas de actuación en materia de ciberseguridad para los años 2022 – 2025, involucrando a la Administración Pública de Andalucía, la ciudadanía, el sector privado y las entidades más representativas del sector.

La ejecución de las acciones marcadas por la Estrategia Andaluza de Ciberseguridad se realiza a través del Centro de Ciberseguridad de Andalucía. El propósito de este centro es dar confianza y protección a ciudadanía, empresas privadas e instituciones públicas en el ecosistema digital andaluz.

2.3. Alineación estratégica

2.3.1. Agenda 2030: Objetivos de Desarrollo Sostenible

En 2015, la ONU aprobó la Agenda 2030 sobre el Desarrollo Sostenible, una oportunidad para que los países y sus sociedades emprendan un nuevo camino con el que mejorar la vida de todos, sin dejar a nadie atrás. La Agenda cuenta con 17 Objetivos de Desarrollo Sostenible, que incluyen desde la eliminación de la pobreza hasta el combate al cambio climático, la educación, la igualdad de la mujer, la defensa del medio ambiente o el diseño de nuestras ciudades. El desarrollo normativo en materia de protección de datos va de la mano con el objetivo 16, el cual trata de promover sociedades justas, pacíficas e inclusivas y entre cuyas metas se encuentran:

- 16.6. Crear a todos los niveles instituciones eficaces y transparentes que rindan cuentas.
- 16.10. Garantizar el acceso público a la información y proteger las libertades fundamentales, de conformidad con las leyes nacionales y los acuerdos internacionales.

2.3.2. España Digital 2025[2]

España Digital 2025 recoge un conjunto de medidas, reformas e inversiones, articuladas en diez ejes estratégicos, alineados a las políticas digitales marcadas por la Comisión Europea.

[2] España Digital 2025: https://avancedigital.mineco.gob.es/programas-avance-digital/Paginas/espana-digital-2025.aspx

Las acciones de la Agenda están orientadas a impulsar un crecimiento más sostenible e inclusivo, impulsado por las sinergias de las transiciones digital y ecológica, que llegue al conjunto de la sociedad y concilie las nuevas oportunidades que ofrece el mundo digital con el respeto de los valores constitucionales y la protección de los derechos individuales y colectivos:

Entre los ejes estratégicos que recoge caben destacar los siguientes:

- Impulsar la digitalización de las Administraciones Públicas (meta 2025: 50% de los servicios públicos disponibles en app móvil).
- Favorecer el tránsito hacia una gobernanza del dato, garantizando la seguridad y privacidad y aprovechando las oportunidades que ofrece la Inteligencia Artificial (meta 2025: 25% de empresas que usan inteligencia artificial y Big Data).
- Reforzar la capacidad española en ciberseguridad, consolidando su posición como uno de los polos europeos de capacidad empresarial (meta 2025: 20.000 nuevos especialistas en ciberseguridad, Inteligencia Artificial y Datos).
- Garantizar los derechos de la ciudadanía en el nuevo entorno digital (meta 2025: una carta nacional sobre derechos digitales).

Dichos ejes enlazan con la necesidad de reorganizar, potenciar y unificar la política de seguridad de los datos integrando todas las perspectivas: interior, TIC y protección de datos personales.

2.3.3. Estrategia de Administración Pública Innovadora

Esta estrategia de Administración Pública Innovadora 2024-2030[3], cuyo acuerdo de formulación se aprobó el 14 de febrero de 2023 por Consejo de Gobierno, pretende ser un marco de trabajo que permita a cada órgano directivo de la Junta de Andalucía definir sus estrategias específicas de transformación con unos criterios comunes y homogéneos , así como impulsar y coordinar iniciativas horizontales de transformación que resuelvan los principales problemas comunes de la ciudadanía en su relación con la Junta de Andalucía y su personal empleado público. Ha sido desarrollada por la Secretaría General para la Administración Pública (SGAP) de la Consejería de Justicia, Administración Local y Función Pública en colaboración con el resto de Consejerías de la Junta de Andalucía. La protección de datos y el enfoque desde el diseño y por defecto es uno de los valores que rigen esta estrategia ya que la transformación que se plantea requiere una enorme gestión del cambio, redefinición de procesos y organización que se configuran como una oportunidad para aplicar este principio y garantizar la privacidad de la ciudadanía.

2.4. Formulación del Plan

La justificación de su formulación se justifica desde el punto de vista social, este Plan Estratégico tiene una especial relevancia, dado que las Administraciones Públicas, en concreto la Junta de Andalucía, maneja una ingente cantidad de datos personales de la ciudadanía a la cual presta sus servicios, con los que se realizan operaciones de datos que tienen un alto impacto en los derechos fundamentales. Esta relevancia es aún mayor si tenemos en cuenta los grandes retos tecnológicos a los que nos estamos enfrentando, destacando la irrupción de la inteligencia artificial y sus implicaciones éticas y legales.

[3] Estrategia de Administración Pública Innovadora: https://juntadeandalucia.es/boja/2023/34/5

3. Metodología y sistema de gobernanza

El modelo de gobernanza empleado para la formulación de este Plan Estratégico constituye una de las piezas clave de dicho proceso, ya que establece un marco colaborativo con los diferentes agentes intervinientes.

El siguiente esquema refleja los distintos actores que forman parte de la estructura de Gobernanza:

1. Sistema de gobernanza (Fuente: elaboración propia)

A continuación, se enumeran la composición y funciones de cada uno de ellos:

El **Comité Directivo** es el órgano responsable de marcar la dirección estratégica del Plan y está constituido por la Comisión Interdepartamental de Coordinación y Racionalización Administrativa (CICRA), con la siguiente composición:

a) Presidencia: La persona titular de la Viceconsejería con competencias en materia de administración pública.

b) Vicepresidencia primera: la persona titular de la Viceconsejería con competencias en materia de administración Periférica.

c) Vicepresidencia segunda: la persona titular de la Secretaría General con competencias en materia de administración pública.

d) Vicepresidencia segunda: la persona titular de la Dirección Gerencia de la Agencia Digital de Andalucía.

e) Vocalías, integradas por las personas titulares de:

- El órgano directivo con competencias en materia de Estrategia Digital de la Agencia Digital de Andalucía.
- El órgano directivo central con competencias en materia de administración periférica
- La jefatura de la Inspección General de Servicios.
- Las Secretarías Generales Técnicas de las Consejerías.

Son funciones del Comité Directivo las siguientes:

- Designar a las personas integrantes del Comité Técnico, que deberán proveer a la Oficina Técnica de la información que consideren relevante para caracterizar la situación y necesidades del plan, y elaborar los programas de actuación que propongan desarrollar.
- Marcar las prioridades de la Administración General de la Junta de Andalucía en materia de protección de datos.
- Validar los objetivos estratégicos del Plan Estratégico.
- Aprobar formalmente la propuesta del Plan Estratégico de Protección de datos de la Junta de Andalucía.

El **Comité Técnico** está formado por las personas designadas como Delegados/as de Protección de Datos.

Son funciones del Comité Técnico las siguientes:

- Aportar datos e información de contexto.
- Consensuar enfoques en la fase de diagnóstico.
- Validar las acciones o medidas en las que se articulará el presente Plan Estratégico en la Junta de Andalucía.

En cuanto a las **personas expertas participantes** cabe señalar la realización de un Grupo focal en junio de 2023, cuyas conclusiones se han recogido a lo largo del presente documento.

En cuanto a la **ciudadanía**, se realizó una encuesta en el año 2021 a través del Instituto de Estadística y Cartografía de Andalucía (IECA) sobre digitalización y uso de datos personales. La muestra estaba compuesta por 4.675 personas, residentes en Andalucía y de edades comprendidas entre los 16 y 75 años.

La **Oficina Técnica del Plan** está constituida por personal al servicio de la SGAP dependiente de la Consejería de Justicia, Administración Local y Función Pública, cuya función es la de llevar a cabo su redacción, así como coordinar a todos los entes implicados en la estructura de gobernanza.

La elaboración de este Plan Estratégico ha seguido una **metodología participativa**, con el objetivo de obtener una estrategia transparente, responsable, eficaz y coherente con las necesidades reales de la organización.

Como punto de partida, la Oficina Técnica realizó un análisis de situación en materia de protección de datos en la Junta de Andalucía, con el objeto de conocer el impacto que ha supuesto la implantación de la nueva normativa en esta materia, consultándose, entre otras, las siguientes fuentes:

- Portal de transparencia de la Junta de Andalucía: para obtener el inventario del personal que presta sus servicios como Delegado/a de Protección de Datos (DPD), así como el Registro de Actividades de Tratamiento (RAT) y el registro de entes dependientes de la Comunidad Autónoma de Andalucía.

- Encuesta realizada a todos/as los/as DPD.
- Grupo focal con un grupo representativo de personas relacionadas con la protección de datos en la Junta de Andalucía.
- Para contextualizar resultados se han obtenido datos del Sistema de Información de Recursos Humanos de la Junta de Andalucía, (en adelante SirHus) y de la Oficina de Seguridad de las Tecnologías de la Información y la Comunicación (TIC) de la Agencia Digital de Andalucía (ADA).
- Portal de transparencia de la autoridad de control andaluza: Consejo de Transparencia y Protección de Datos de Andalucía (CTPDA).
- Portal del Instituto de Estadística y Cartografía de Andalucía (IECA) con resultados de la "Encuesta Social 2021. Digitalización y uso de datos personales. Capacidades y actitudes de la población andaluza".

Con este análisis de situación se realizó un diagnóstico participativo que dio lugar a una lista de los problemas, las necesidades y los retos detectados tras la situación inicial.

El Comité Directivo, seleccionó aquellos problemas, necesidades y retos a los que debía dar solución este Plan Estratégico, de cara a priorizar actuaciones y acotar el alcance del mismo.

La Oficina Técnica del Plan, partiendo de la lista priorizada de problemas necesidades y retos, elaboró los objetivos estratégicos y líneas de actuación, que se deberán abordar. Para cada objetivo estratégico se han definido unos indicadores de contexto e impacto, que con posterioridad nos permitirán medir la consecución de los mismos.

Partiendo de los objetivos estratégicos establecidos se marcan unos objetivos específicos que, a su vez, se concretan en programas de actuación y proyectos. Cada programa de actuación y proyecto llevará asociado uno o varios indicadores de resultados y de realización.

Con el conjunto de todos los indicadores citados, se construye un sistema de seguimiento y evaluación que permitirá realizar un análisis previo de evaluabilidad para medir la pertinencia y relevancia del plan, una evaluación ex ante (previa a su ejecución), intermedia (a lo largo de la ejecución) y final. Con este sistema se podrá medir el impacto que la ejecución del Plan Estratégico tendrá sobre las líneas estratégicas definidas y el nivel de cumplimiento de los objetivos marcados.

Con todas las aportaciones recibidas, se conforma el Plan Estratégico de Protección de Datos de la Junta de Andalucía, para los años 2024-2030, que se remitirá a la CICRA para su aprobación definitiva mediante Acuerdo.

4. Misión, visión y valores

A continuación, se enuncian la misión, la visión y los valores del Plan, que constituyen el punto de referencia para su formulación, así como la inspiración y motivación para su futura implementación. Con todo ello, y por ende con el mismo, se pretende dar respuesta a los principales problemas, necesidades y retos identificados en el diagnóstico realizado.

Misión: garantizar que la normativa de protección de datos en la Junta de Andalucía se cumpla conforme a sus principios inspiradores.

Visión: Ser una Administración referente en la ejecución y adaptación normativa de la protección de datos personales en Andalucía.

Este Plan sustenta su labor en los pilares de los siguientes valores:

- La ciudadanía como eje central.
- Transparencia y participación.
- Eficiencia y sostenibilidad en la actuación administrativa.
- Racionalidad organizativa.
- Credibilidad.
- Servicio público.

5. Análisis de la situación actual

En la Comunidad Autónoma de Andalucía se presta servicio a un total de 8.472.407[4] de andaluces y andaluzas cuyos datos se manejan en centros de procesos de datos cuyo principal encargado del tratamiento es la ADA. Desde 2018, fecha en que entró en vigor el RGPD no se ha hecho de forma global o transversal diagnóstico de situación acerca de la adaptación al mismo, en la Junta de Andalucía.

Todo lo cual ha hecho necesario la realización del presente estudio sobre la aplicación del RGPD y la LOPDGDD en el ámbito de la Comunidad Autónoma de Andalucía.

Las áreas objeto de estudio son las siguientes:

1. Delegados/as de Protección de Datos
2. Política de seguridad de los datos
3. Registro de Actividades de Tratamiento
4. Responsabilidad proactiva
5. Formación y concienciación
6. Violaciones de seguridad
7. Medidas de seguridad y auditoría
8. Consulta y ejercicio de los derechos
9. Costes de implantación del RGPD y normativa asociada

A continuación, se realiza una exposición de la situación actual en cada una de las áreas que se quieren abordar para llevar a cabo este plan.

La Junta de Andalucía, a la fecha de este estudio (abril-junio 2023), está compuesta por 13 Consejerías que constituyen su Administración Central, 11 Agencias Administrativas, 19 Agencias Públicas Empresariales, 3 Agencias de Régimen Especial, 3 Consejos y un total de 57 entes instrumentales pertenecientes al sector público, en el que se incluyen Universidades, sociedades mercantiles, consorcios e instituciones sin ánimo de lucro.

No está incluido el Consejo de Transparencia y Protección de datos de Andalucía (CTPDA) por ser la autoridad de control, en consecuencia, se abarca a un total de 102 organismos.

El RAT incluía, a la fecha del estudio, 2.022 actividades de tratamiento distribuidas entre 64 organismos distintos que conforman el 63% del total. Un 37% de organismos no tienen publicado el RAT en el portal de transparencia.

[4] Datos del Instituto Nacional de Estadística a 31 de diciembre de 2022.

La encuesta se envió a los 64 organismos, de los cuales respondieron 39, lo que representa un 61%, tal como se aprecia en el siguiente gráfico:

Organismos	Total	%Total	%Encuestados
Totales	102	100%	
En la web de Transparencia	64	63%	
Encuestados	39	38%	**61%**

2. Organismos de la Junta de Andalucía totales, en la web de transparencia y encuestados (Fuente: elaboración propia a partir de información del portal de transparencia de la Junta de Andalucía (03/2023))

5.1. Delegados/as de Protección de Datos

El artículo 37 del RGPD, en su apartado 1a) establece que el responsable y el encargado del tratamiento de los datos designarán un Delegado/a de Protección de Datos (DPD), pudiéndose designar una única persona o varias, en función de la estructura organizativa y tamaño de los organismos públicos a los que preste sus servicios.

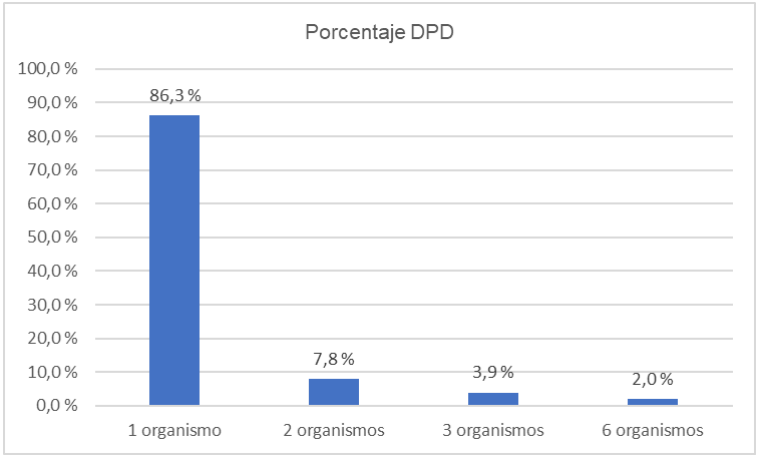
Esta figura tiene encomendadas relevantes funciones, entre las cuales se pueden citar las siguientes:

- Informar y asesorar a las personas responsables o encargadas de los tratamientos de datos, así como al personal empleado público de las obligaciones que les incumben, con arreglo al Reglamento.
- Supervisar su cumplimiento.
- Asesorar sobre la evaluación de impacto relativa a la protección de datos.
- Cooperar con la autoridad de control

Asimismo, el apartado 5 del mencionado artículo indica que el/la DPD debe ser nombrado atendiendo a sus conocimientos especializados en derecho.

Desde la Oficina Técnica del Plan, se ha solicitado información a las diferentes Consejerías, Agencias y entidades instrumentales que conforman el ámbito del presente diagnóstico, en relación con las personas que prestan sus servicios en ellas, como Delegados/as de Protección de Datos, obteniéndose los siguientes datos:

El inventario de DPD incluía a 51 personas designadas en 64 organismos distintos, 44 de ellas asignadas a un solo organismo, 4 asignadas a 2 organismos, 2 prestaban su servicio en 3 organismos y 1 lo hacía en 6 organismos diferentes, tal como se aprecia en el gráfico siguiente expresado en porcentajes.



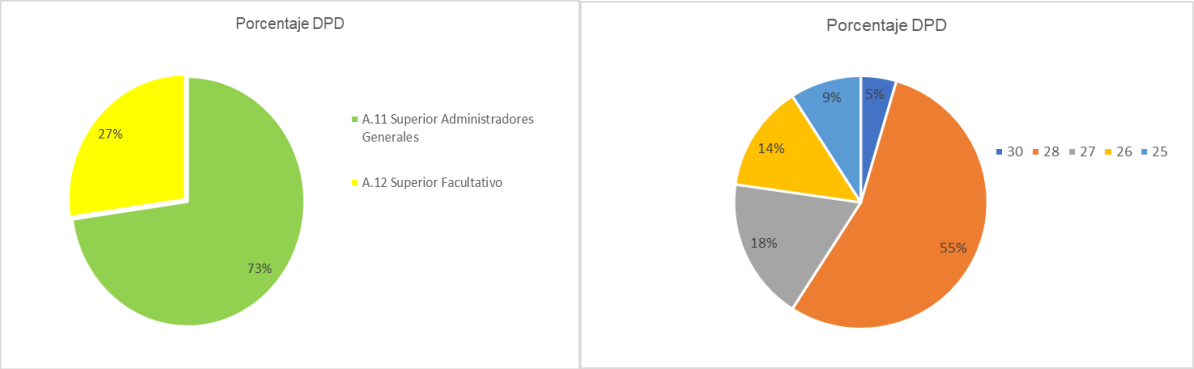
3. DPD y asignación de organismos (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

Hay que destacar que, según los datos obtenidos a través del SirHus, a la fecha del presente estudio, un 66,2% del personal al servicio de la Administración General de la Junta de Andalucía, son mujeres, frente a un 33,8% que son hombres. Es una Administración muy feminizada, en contraposición con este colectivo en el que el 74% de los DPD encuestados son hombres frente al 26% que son mujeres. Es un colectivo muy masculinizado por encima del equilibrio normativo con un IPRHM de 0,51[5].

En cuanto a la relación jurídica que les une con la Administración, un 56% resultó ser personal funcionario, un 33% personal laboral específico que da servicio a aquellas Agencias en las que no existe personal funcionario, un 8% personal externo contratado por una empresa de servicios y sólo el 3%, es una persona laboral del VI Convenio Colectivo del personal laboral de la Junta de Andalucía.

El 73% del personal funcionario pertenece al Cuerpo Superior de Administradores Generales y se distribuye por niveles del puesto de trabajo, tal como se puede apreciar en los siguientes gráficos, siendo el nivel 28 el más frecuente con un 55% de representatividad, seguido de lejos de los niveles 27 con el 18%, 26 con el 14%, 25 con el 9% y 30 con el 5%. No constan las categorías profesionales del personal laboral ni externo.

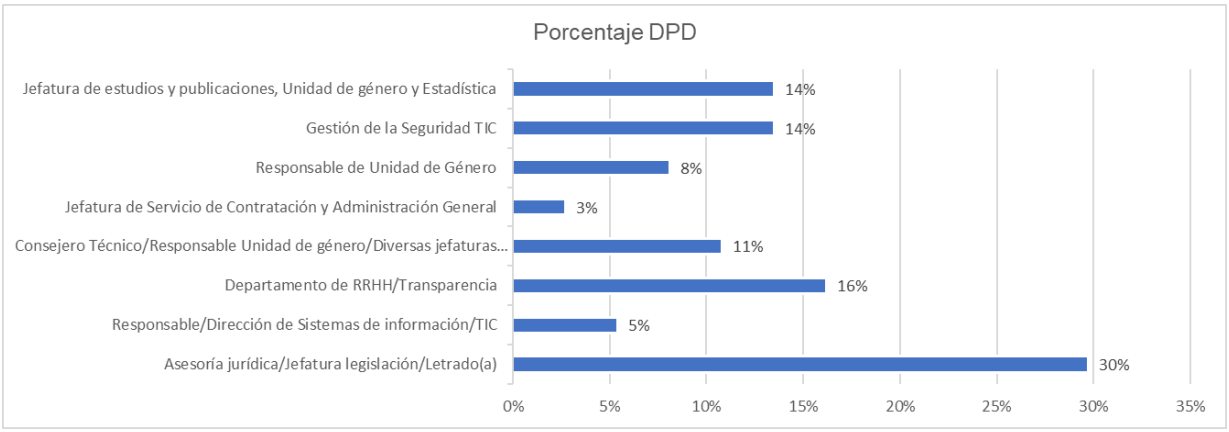
[5] El IPRHM hace referencia al índice de presencia relativa de hombres y mujeres. Con este índice se hace una traslación de los porcentajes de representación equilibrada 60%-40% que establece la normativa de igualdad. El valor 1 indica paridad, por debajo de 0,8 el colectivo está masculinizado y por encima del 1,20 está feminizado por encima del 60%. Responde a la fórmula: IPRHM= [(M-H)/(M+H)]+1, donde M y H son el número de mujeres y de hombres.



4. DPD por Cuerpos y niveles de personal funcionario (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

Tal como se puede apreciar no existe un criterio homogéneo a la hora de asignar a la persona que ejerce como DPD.

En cuanto al ejercicio de la actividad solamente 2, el 5%, la ejercen de forma exclusiva. El 95% restante compatibiliza su labor como DPD con otras actividades sin una pauta específica (unas personas tienen perfil jurídico, otras son personal TIC, otras ejercen sus competencias en el ámbito de recursos humanos, de contratación, etc.).



5. DPD por Cuerpos y niveles de personal funcionario (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

También se ha constatado que el 97% del personal designado tiene resolución administrativa de su nombramiento, sólo el 3% restante (una persona) no tiene un acto jurídico formal de nombramiento.

Entre el personal designado, un 90% ha comunicado su nombramiento a la autoridad de control, frente a un 10% que no lo ha hecho. Sólo un 69% ha comunicado su nombramiento al resto del personal del organismo, lo cual puede tener especial incidencia en aquellas personas que son responsables de tratamiento que podrían tener dificultades para poder acceder al/a la DPD para soporte o asesoramiento y desconocen sus datos.

No existe un criterio homogéneo para designar a la persona que ejerce como DPD.

Existe gran heterogeneidad entre las funciones con las que los/as DPD compatibilizan su función.

No se comunican los datos de la persona designada a la organización.

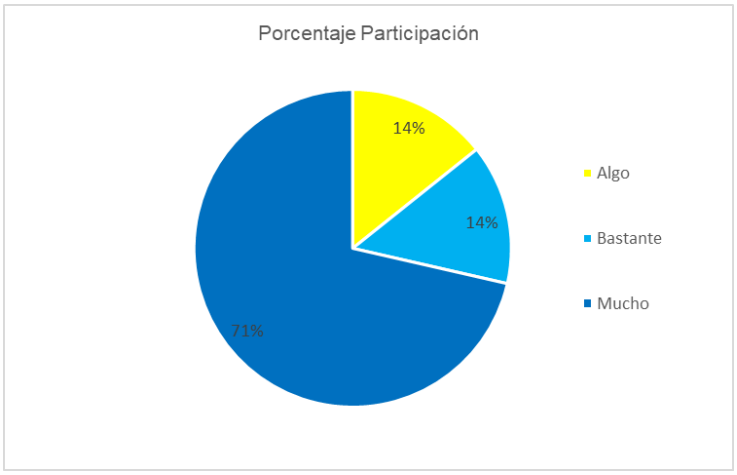
5.2. Política de seguridad de los datos de carácter personal

Mediante el Decreto 70/2017, de 6 de junio, por el que se modifica el Decreto 1/2011, de 11 de enero, se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía[6].

En el 90% de los organismos encuestados existe una política de seguridad, cuyo ámbito se circunscribe al TIC y en algunos casos a la seguridad interior. No es, por lo tanto, una política específica de seguridad de los datos de carácter personal.

El 87% de DPD se coordina con la persona responsable de seguridad TIC de su organismo, a este respecto.

Asimismo, un 54% de los organismos tienen procedimientos específicos de protección de datos definidos en los que ha participado la persona responsable de seguridad TIC, con un porcentaje de participación muy elevado, tal como puede verse a continuación:



6. Porcentaje de participación de la persona responsable de seguridad TIC en los procedimientos de protección de datos (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

No existe una política de seguridad específica para la protección de datos personales

[6] https://juntadeandalucia.es/boja/2017/110/

5.3. Registro de Actividades de Tratamiento

Una de las herramientas que el RGPD exige a los responsables para demostrar su conformidad con él mismo, es el mantenimiento de los Registros de Actividades de Tratamientos de datos (RAT) que tienen bajo su responsabilidad y control, teniendo en cuenta la obligada colaboración con la Autoridad de Control que exige poner a su disposición dichos registros para facilitar sus actividades de supervisión.

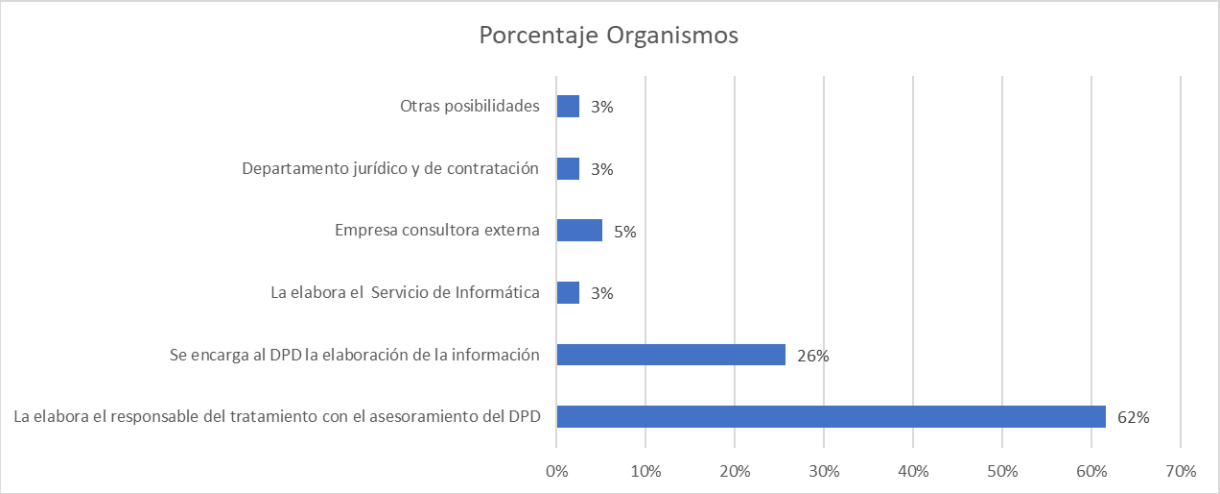
El contenido del Registro de Actividades de Tratamiento constituye una información mínima exigible. Este registro podría integrarse y formar parte de los catálogos de procesos que ya existiesen en la entidad, incluyendo toda la información que el responsable considere necesaria para proteger los derechos y libertades de las personas físicas y poder demostrar cumplimiento atendiendo a la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los posibles orígenes de los riesgos que dicho tratamiento pudiera suponer para los interesados.

El registro podría incluir aspectos que faciliten la aplicación efectiva de la responsabilidad proactiva como: análisis de riesgos para los derechos y libertades realizados, la descripción sistemática del tratamiento, los sistemas de información sobre los que se apoya, la descripción de la identidad de los encargados del tratamiento, las garantías previstas para llevar a cabo transferencias internacionales de datos, información de contacto de las personas o los departamentos de la organización que se encuentran implicados en las operaciones de tratamiento, etc.

En la Junta de Andalucía, las actividades de tratamiento se definieron con una estructura de plantilla común a todas, proporcionando por tanto una estructura de información homogénea a la ciudadanía, si bien, al comparar los datos que aparecen en el Registro de Procedimientos y Servicios (RPS), con el RAT, se ha podido observar que, en algún caso, un tratamiento se corresponde con un procedimiento administrativo, pero en otras ocasiones son varios los procedimientos administrativos; otras veces, puede existir correspondencia entre los tratamientos y trámites dentro de un procedimiento o servicio, en algún caso, o con un sistema de información en otro, etc.

En definitiva, no existe una homogeneidad sobre dónde colocar el foco de cara a definir un tratamiento, ya que no hay criterios comunes. Esta información, no obstante, contrasta con el 77% de organismos que declaró que sí tenía definidos criterios homogéneos en el tratamiento de datos.

Por otra parte, en función de cómo se elabora el RAT se dan varias posibilidades tal como se refleja en la siguiente gráfica, siendo la opción más frecuente que la elabore el responsable del tratamiento con el asesoramiento del DPD en un 62% de los casos.



7. Porcentaje de participación en la elaboración del RAT en función de quién lo elabora (abril-2023))

No existe una homogeneidad de criterios para definir un tratamiento, ni sobre las personas que intervienen en su elaboración.

5.3.1. RAT / Responsables de los tratamientos

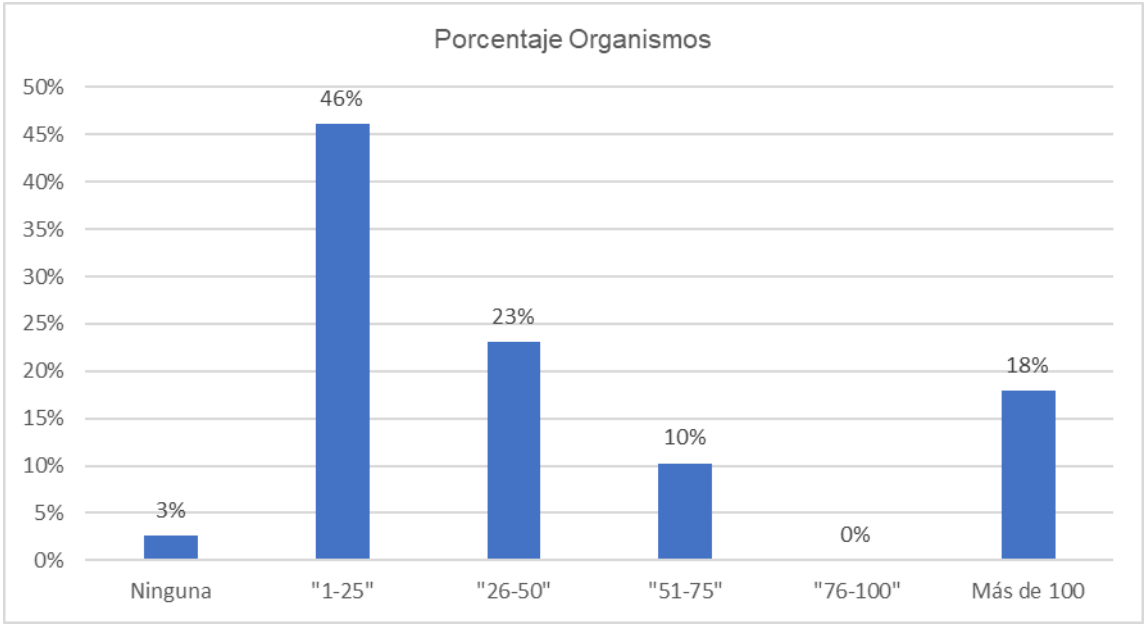
El Responsable del tratamiento (RT) de datos es aquella persona física o jurídica, o autoridad pública, encargada de decidir sobre el tratamiento de datos personales de los individuos. Se encarga de determinar los fines y medios para el tratamiento, así como de establecer las medidas técnicas y organizativas que garanticen la seguridad de los mismos.

Además, debe ser capaz de demostrar el cumplimiento del RGPD y la LOPDGDD ante las autoridades de control.

El Responsable del tratamiento es quien decide si quiere contar con la ayuda de un Encargado del tratamiento, o si decide realizar el tratamiento de datos por sí mismo.

En la Junta de Andalucía, sólo un organismo declaró no tener actividades de tratamiento en las que actúa como responsable, lo que representa un 3%.

El 46% de organismos declararon tener menos de 25 tratamientos, seguido del 23% que declararon tener entre 51 y 75, el 10% entre 51 y 75 y un 18% que declaró tener más de 100.



8. Porcentaje de organismos en función del número de tratamientos declarados por tramos (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

Asimismo, un 44% de organismos declaró que no tienen ninguna actividad totalmente automatizada, eso implica tener tratamientos de datos manuales lo cual conlleva unas medidas de seguridad diferentes a las medidas de seguridad TIC.

Sólo un 3% (1 organismo) declaró tener todos sus tratamientos totalmente automatizados. Este dato pone en evidencia cierto déficit de telematización en la Junta de Andalucía.

¿Cuántas actividades de tratamiento completamente automatizadas tiene su organismo?	Total	%Total
Ninguna	17	44%
"1-25"	16	41%
"26-50"	2	5%
"51-75"	0	0%
"76-100"	0	0%
Más de 100	1	3%
NS/NC	3	8%
	39	

9. Porcentaje de organismos con tratamientos totalmente automatizados por franjas (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

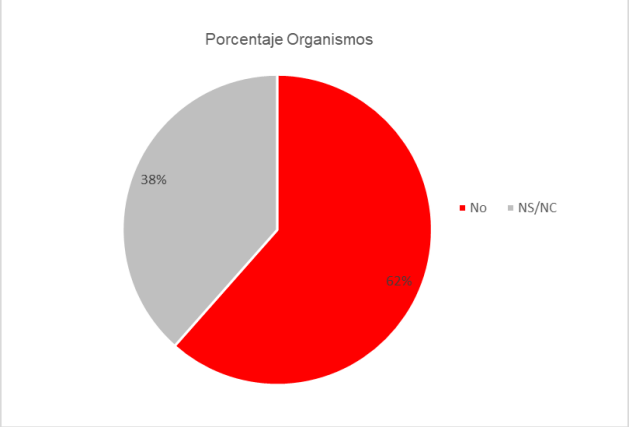
El 46% de organismos declararon tener menos de 25 tratamientos.

La mayoría de los organismos no tienen los tratamientos de datos automatizados.

En cuanto a actividades de tratamiento con categorías especiales de datos, un 5% de los y las DPD respondió desconocer su existencia, un 21% respondió que no se manejan y un 74% declaró que sí.

Respecto a las actividades de tratamiento con decisiones automatizadas o de perfilado sólo un 8% declaró tener alguna, frente a un 82% que declaró no tener ninguna y un 10% que no sabe o no contesta. El 62% declaró no haber recibido ningún ejercicio de derechos de oposición a ser objeto de decisiones individuales automatizadas por parte de las personas interesadas frente al 38% que no sabe o no contesta.

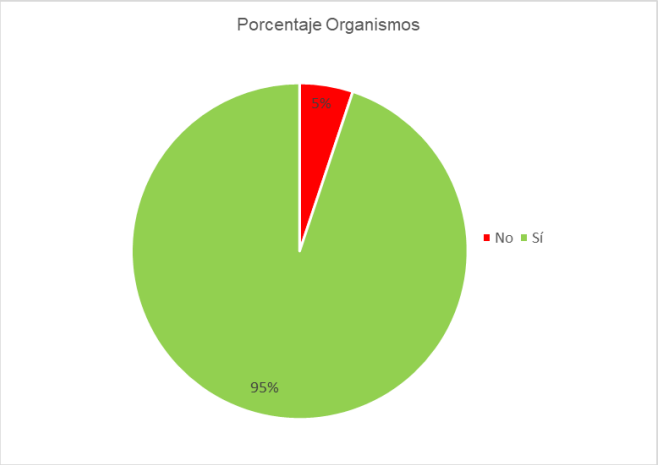
¿Cuántas actividades de tratamiento con decisiones individuales automatizadas o de perfilado tiene su organismo?	Total	%Total
Ninguna	32	82%
1	2	5%
15	1	3%
NS/NC	4	10%
Total general	39	



10. Porcentaje de organismos con tratamientos con decisiones automatizadas o de perfilado (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

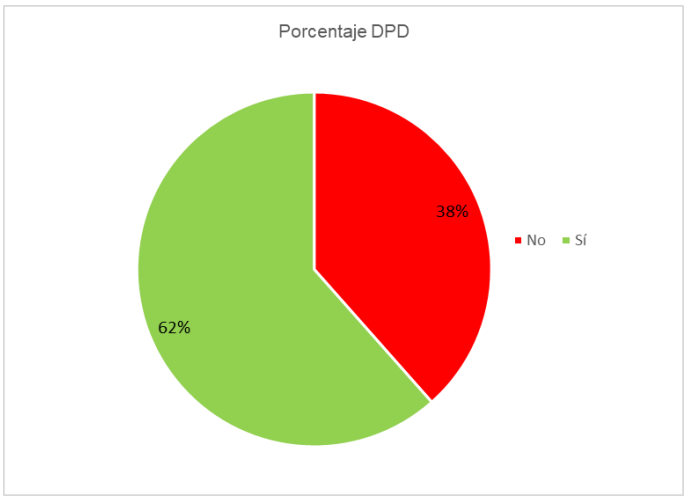
Las entidades señaladas en la LOPDGDD en su artículo 77.1, con fines de transparencia (art. 6.bis Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno), deberán hacer público el inventario de sus actividades de tratamiento de manera que sea accesible por medios electrónicos (art. 31.2 LOPDGDD), esta es una obligación que deben cumplir todas las Administraciones Públicas.

Tal como puede observarse en el siguiente gráfico, un 5% de los organismos encuestados (dos) han incumplido esta obligación frente al 95% que sí la han cumplido.



11. Organismos de la Junta de Andalucía con RAT publicado en la web de transparencia (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

Por otro lado, hay que indicar que el 38% de personas que ejercen como DPD, considera que su organismo no tiene todas las actividades de tratamiento incluidas en el RAT, frente a un 62% que sí consideran que tienen un inventario completo. Un 54%, además, declararon no tener un procedimiento definido de altas y bajas en el RAT frente a un 46% que sí manifestó disponer del mismo.



12. Porcentaje de DPD que consideran que tienen el RAT completo (Fuente: elaboración propia a partir de información de la encuesta (abril-2023)

Un 38% de DPD considera que su organismo no tiene todas las actividades de tratamiento incluidas en el RAT

Un 54% declararon no tener un procedimiento definido de altas y bajas.

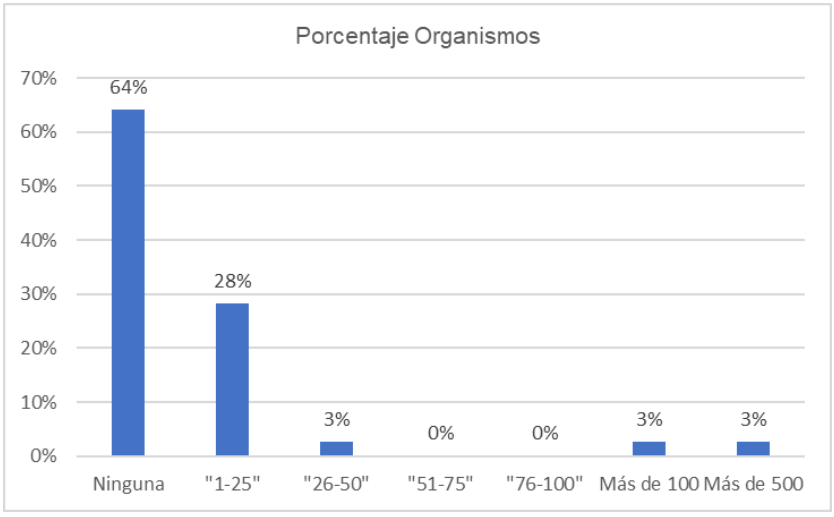
5.3.2. RAT / Encargados del Tratamiento

El Encargado del tratamiento de datos se define como aquella persona física o jurídica, autoridad pública u organismo que brinda un servicio que conlleva el tratamiento de datos personales por cuenta del responsable, siguiendo las directrices del mismo.

La ADA es quien actúa como Encargado de la mayor parte de los tratamientos de la Junta de Andalucía. En los Estatutos de creación[7] de esta Agencia se hace referencia a la normativa de protección de datos, pero no existe un contrato específico de encargado de tratamiento como tal, que regule sus obligaciones.

Según el artículo 33.5 de la LOPDGDD podrán atribuirse las competencias propias de encargado a un organismo vinculado o dependiente mediante la adopción de una norma reguladora de dichas competencias que deberá incorporar el contenido exigido por el artículo 28.3 del RGPD, según el cual: "el tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable".

A este respecto, según los datos obtenidos el 64% de los organismos declaró no actuar como encargados de tratamiento, frente al 36% restante que sí. Destacan dos organismos uno con más de 100 actividades de tratamiento en las que actúa como encargado y un segundo con más de 500, este último es la ADA, ambos suponen un 3% cada uno, según se muestra en el siguiente gráfico:



13. Porcentaje de organismos de la Junta de Andalucía que actúan como encargados de tratamiento (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

El 64% de los organismos declaró no actuar como encargados de tratamiento

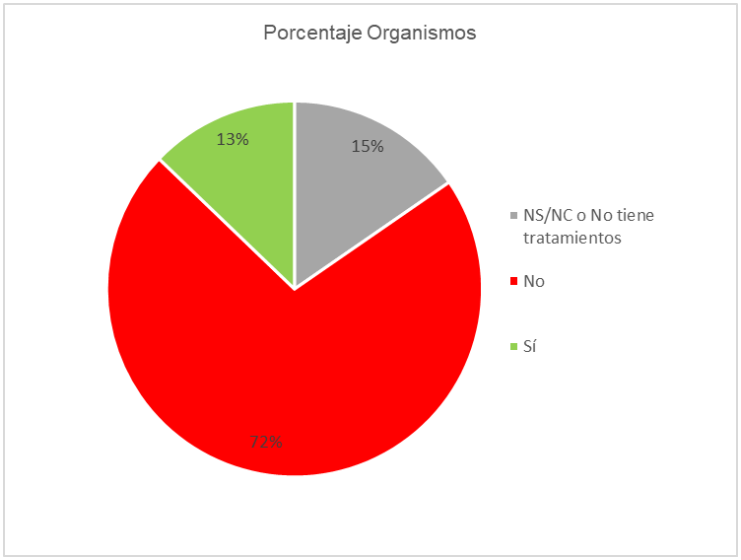
[7] Decreto 128/2021, de 30 de marzo, por el que se aprueban los Estatutos de la Agencia Digital de Andalucía.

El artículo 31 de la LOPDGDD, establece que "*Los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento ...*

Los sujetos enumerados en el artículo 77.1 de esta ley orgánica harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos..."

En la normativa no se hace distinción entre una figura y otra, por lo que se podría interpretar que la obligación de publicar el inventario de actividades recae en cualquiera de ellos.

En este sentido un 72% de los organismos encuestados declararon no tener publicados los inventarios de tratamientos en los que actúan como encargado. Sólo un 13% declaró cumplir con esta obligación.



14. Porcentaje de organismos de la Junta de Andalucía que publican el RAT de encargados (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

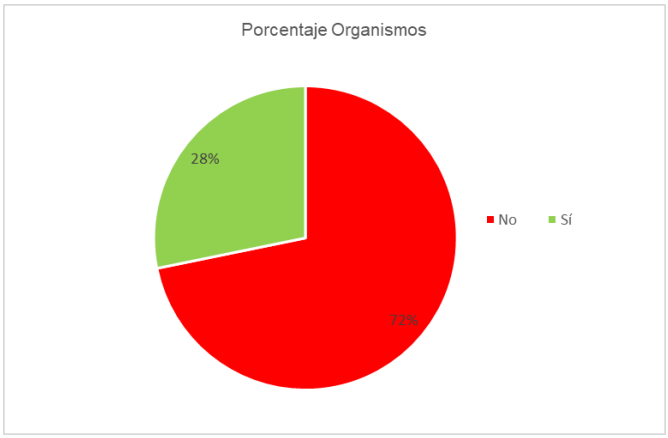
En cuanto a la pregunta de si tienen una relación de los encargados asociados a cada tratamiento, un 72% contesta que no frente a un 28% que declaró sí tenerlos.

Hay que destacar que, si no se tiene dicha relación, se desconoce cómo comprueban el cumplimiento de la normativa por parte de los encargados del tratamiento, habría que valorar si tienen contratos de encargado del tratamiento adecuados o son encargados con alguna certificación, esta cuestión no se ha sondeado.

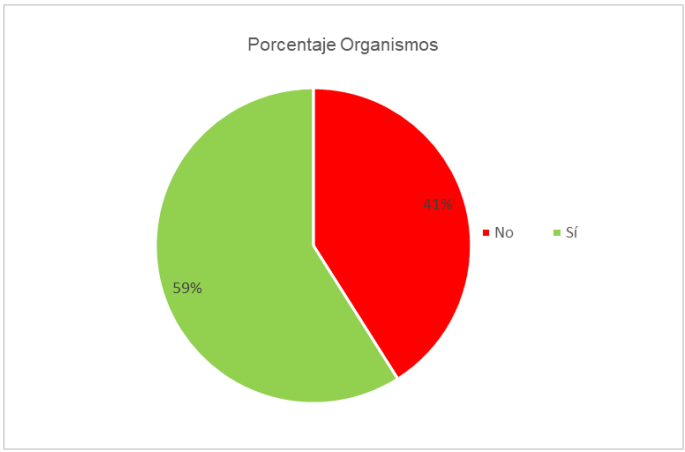
De manera similar un 41% declaró no tener un inventario de los sistemas de información con los que se gestionan los tratamientos frente a un 59% que sí.

En este caso, hay que indicar que las Administraciones Públicas deben tener catalogados todos los sistemas de información de que dispongan, conforme a los niveles básico, medio o alto, tal como establece el Esquema Nacional de Seguridad (ENS), de obligado cumplimiento en el ámbito público. La falta de un mapeo entre sistemas de información y tratamientos puede ocasionar una dificultad a la hora de declarar que un sistema es de un nivel u otro.

El 72% de los organismos encuestados declararon no tener publicados los inventarios de tratamientos en los que actúan como encargado, ni tienen una relación de los encargados asociados a cada tratamiento.

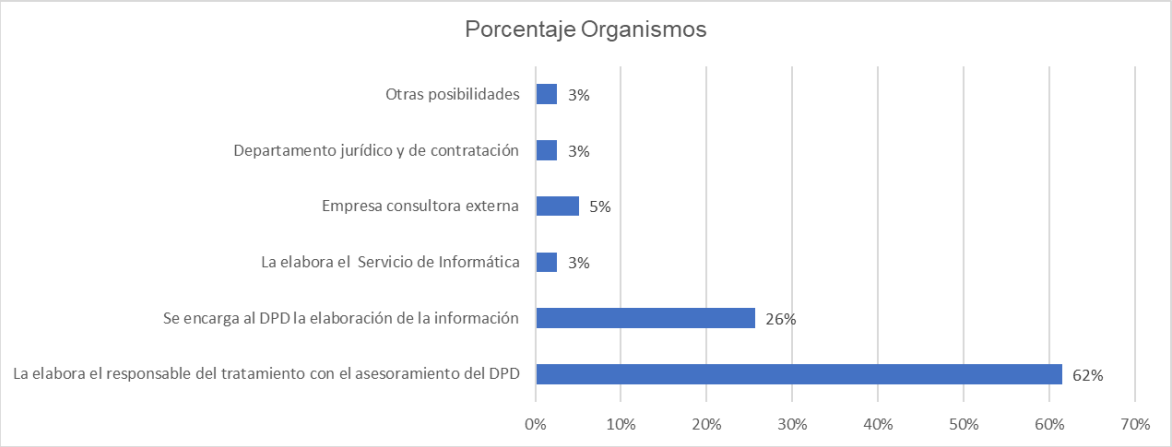


15. Porcentaje de organismos que tienen inventariados los encargos de tratamiento (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))



16. Porcentaje de organismos que tienen un inventario de los sistemas de información con los que gestionan los tratamientos (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

La elaboración del RAT, debería corresponder a la persona responsable del tratamiento, lo cual se da en un 62% de los organismos, en un 26% lo elabora el DPD, en un 5% lo hace una empresa externa, en un 3% el servicio jurídico, 3% el servicio de informática y 3% otras posibilidades, tal como se muestra en la siguiente tabla:



17. Porcentaje de organismos con relación a quién elabora el RAT (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

5.4. Responsabilidad proactiva

El RGPD describe este principio como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento.

En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo.

A partir de este conocimiento deben determinar de forma explícita la forma en que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con él mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión.

En síntesis, este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo.

El análisis de riesgos y la evaluación de impacto son de las principales obligaciones que establece el RGPD en sus artículos 24 y 35, su omisión se considera infracción grave.

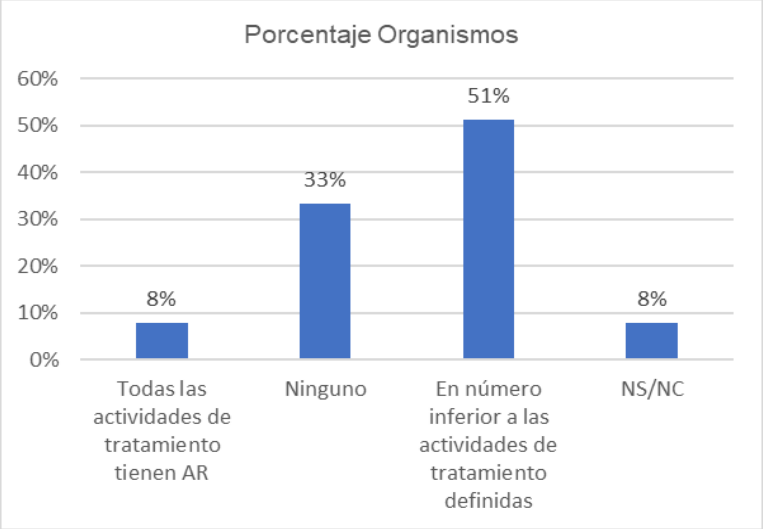
5.4.1. Análisis de riesgos

El RGPD prevé que las medidas de cumplimiento deben aplicarse, en función del riesgo que suponga para los derechos y libertades de las personas interesadas, los tratamientos que realizan.

Por ello, responsables y encargados deben llevar a cabo una valoración del riesgo de sus tratamientos, con el fin de determinar qué medidas aplicar y cómo hacerlo. Este análisis del riesgo variará en función de:

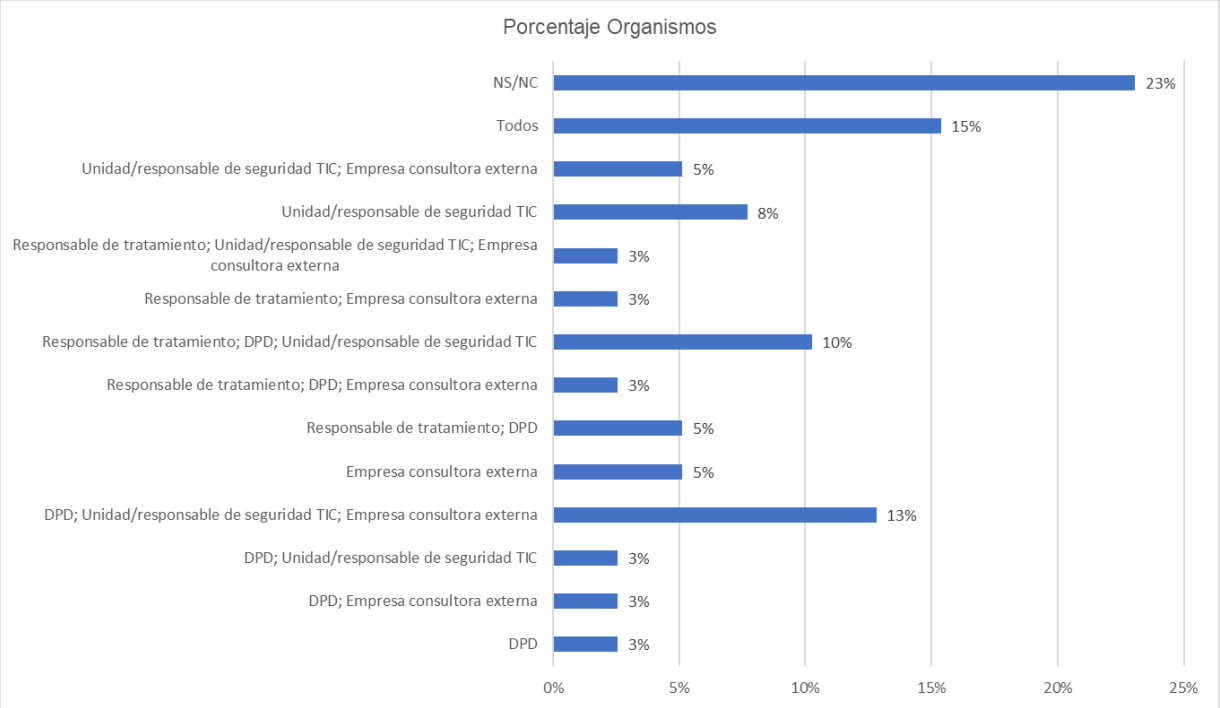
- Los tipos de tratamiento.
- La naturaleza de los datos.
- El número de interesados afectados.
- La cantidad y variedad de tratamientos que realice una misma organización.

En la Junta de Andalucía sólo un 8% de organismos declaró tener todas las actividades de tratamiento con su correspondiente análisis de riesgos, un 33% declaró no tener ninguno, un 51% declaró tener menos de los necesarios y un 8% no sabe o no contesta.



18. Porcentaje de organismos con relación al análisis de riesgos (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

Si se analiza quién intervino en su elaboración no hubo un criterio común tal como se puede observar en el siguiente gráfico, la normativa indica que son responsables y encargados quiénes deben llevar a cabo una valoración del riesgo de sus tratamientos.



19. Porcentaje de organismos con relación a quién elabora el análisis de riesgos (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

La mayoría de los organismos no ha realizado el análisis de riesgo de sus tratamientos de datos.

No hay criterios comunes para realizar su elaboración.

5.4.2. Evaluaciones de impacto

A este respecto, ocurre algo similar, si bien dado que no se conoce cuántas debe haber, se podría comparar con el 8% de los organismos que declararon tener tratamientos con decisiones individuales automatizadas, o bien con el 74% que declaró tener tratamientos con categorías especiales de datos.

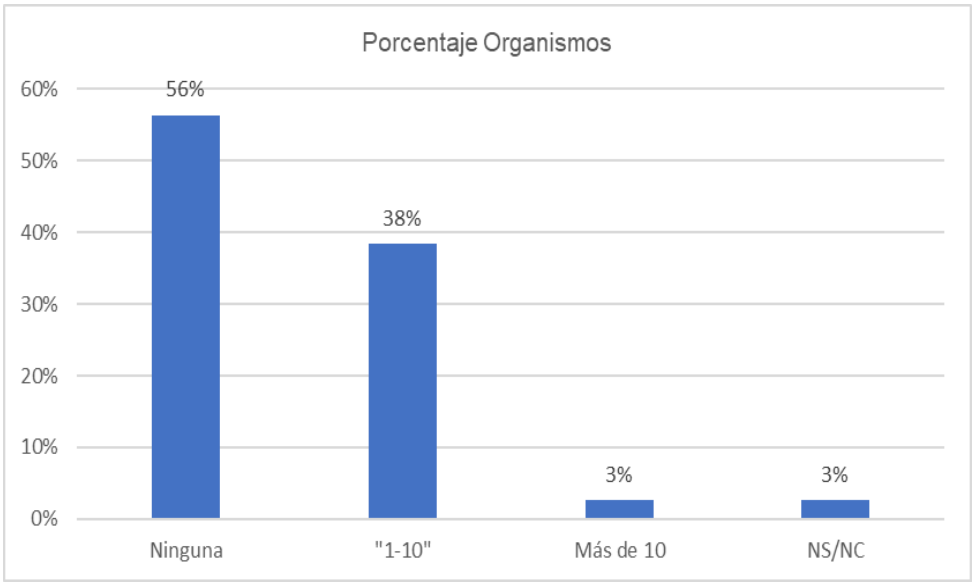
Todos esos tratamientos deberían tener evaluación de impacto tal como establece la autoridad de control en su listado de tratamientos que deben tener evaluación de impacto[8].

[8] Listado de tratamientos que requieren evaluación de impacto publicado por el Consejo de Transparencia y Protección de datos de Andalucía tal como establece el artículo 35.4 del RGPD: https://www.ctpdandalucia.es/area-de-proteccion-de-datos/listado-tratamientos-que-exigen-evaluacion-impacto-o-pueden-estar-exentos-la-misma

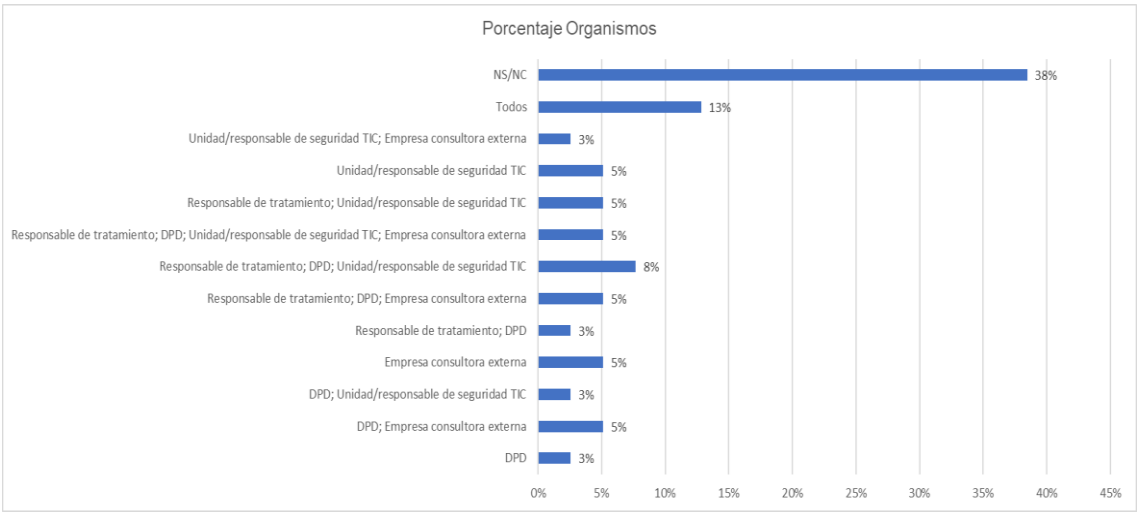
A este respecto, se observa en el gráfico siguiente que el 56% de organismos no ha realizado ninguna. Tampoco existió un criterio común acerca de quién la realiza.

Por otra parte, indicar que un 51% de los organismos considera que hay tratamientos que requieren evaluación de impacto en su organismo y no se ha realizado.

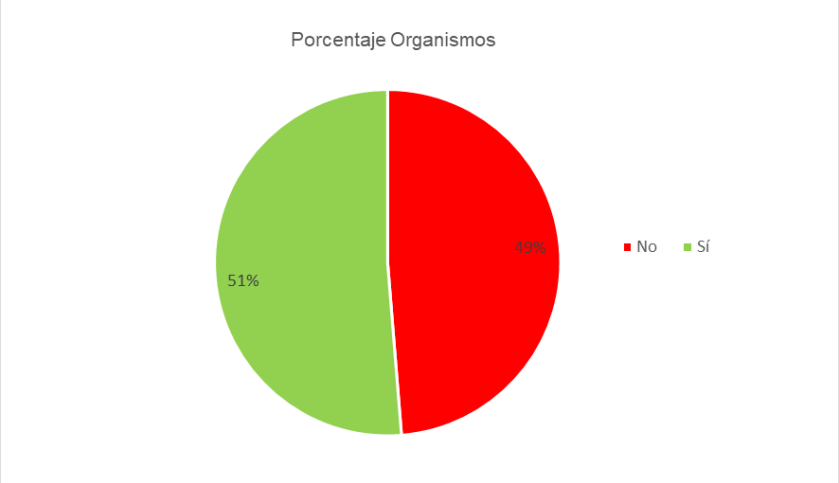
Todo ello se muestra en los gráficos a continuación:



20. Porcentaje de organismos con relación a la evaluación de impacto (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))



21. Porcentaje de organismos con relación a quién realiza la evaluación de impacto y su necesidad (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))



22. Porcentaje de organismos con relación a la necesidad de realizar evaluación de impacto (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

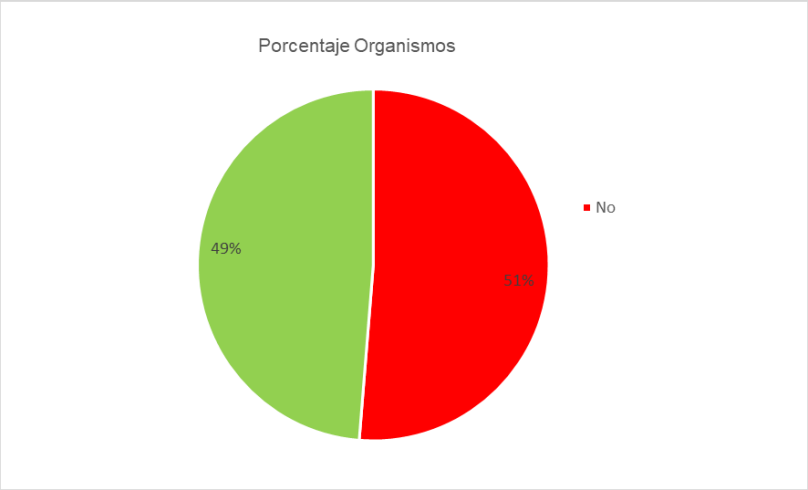
La mayoría de los organismos no ha realizado evaluaciones de impacto en sus tratamientos de datos.

No hay criterios comunes para realizar su elaboración.

En general, en un 56% de los casos no existe un procedimiento definido para la realización de los análisis de riesgos y en un 77% no lo hay para las evaluaciones de impacto.

El hecho de disponer de una herramienta para realizar los análisis de riesgo y/o, en su caso, las evaluaciones de impacto que correspondan, no es una obligación, si bien puede ser un instrumento facilitador del cumplimiento normativo.

Un 51% de los organismos declaró no tener ningún tipo de herramienta, frente a un 49% que sí declaró tenerla.

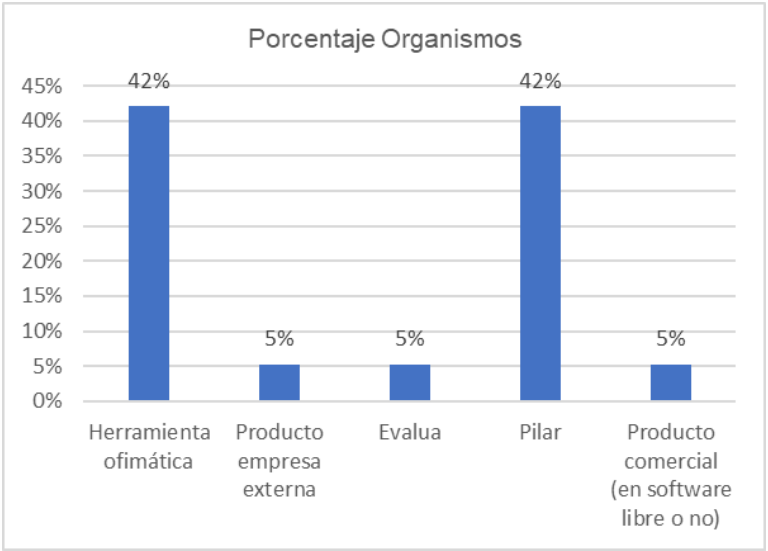


23. Porcentaje de organismos que no disponen de herramienta para gestionar el riesgo (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

El 51% de los organismos no dispone de una herramienta para realizar los análisis de riesgo y/o, en su caso, las evaluaciones de impacto que correspondan

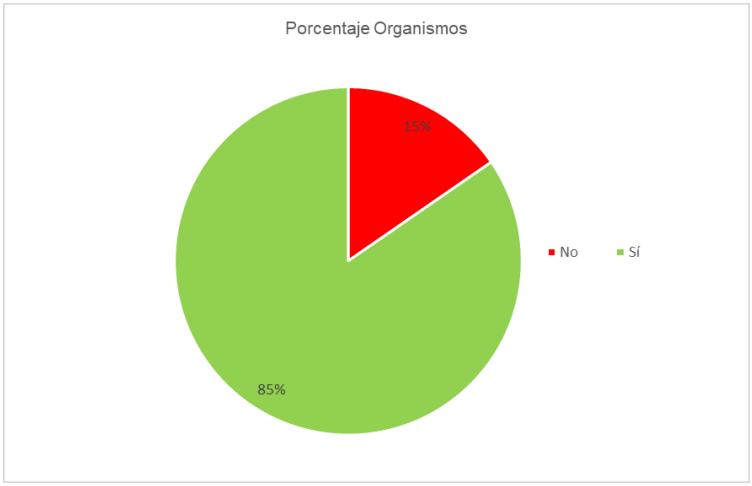
Conforme se muestra en el gráfico a continuación, un 42% de los organismos utilizan herramientas de tipo ofimático, otro 42% utilizan la herramienta Pilar del Centro Nacional de Inteligencia (CCN), un 5% usa Evalúa, herramienta de la AEPD y sólo un 5% declaró tener un producto comercial.

Únicamente 1 organismo declaró haber realizado inversión en una herramienta con coste económico.



24. Porcentaje de organismos en función de la herramienta de gestión del riesgo (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

Por último, indicar que el 85% de los organismos declaró interactuar con la unidad o responsable de seguridad TIC.

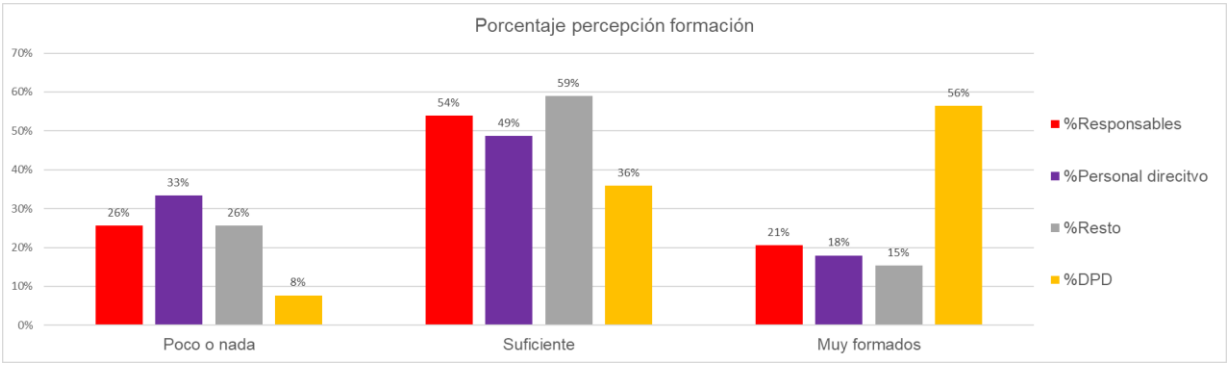


25. Porcentaje de organismos que declara interactuar con su unidad o responsable de seguridad TIC (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

5.5. Formación y concienciación

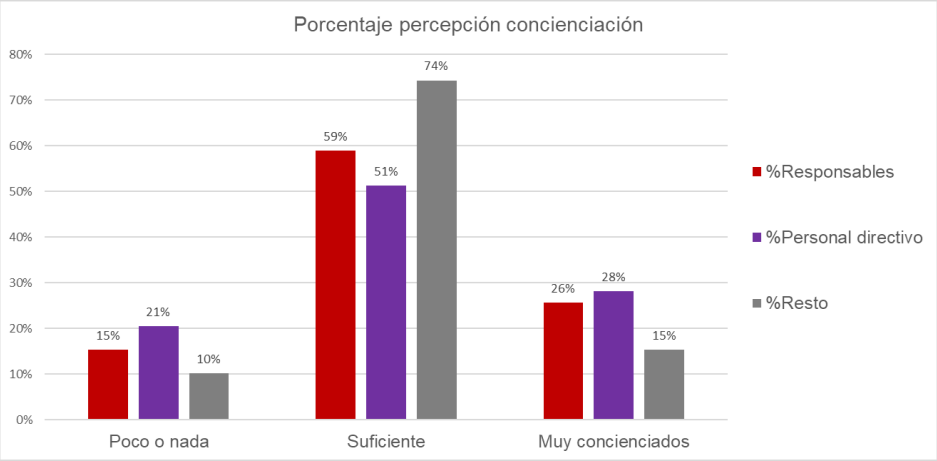
En materia de formación, según el punto de vista del/de la DPD, un 26% del personal responsable del tratamiento, un 33% del personal directivo y un 26% del resto del personal está poco o nada formado.

Según el RGPD el/la DPD, debe nombrarse atendiendo a sus cualidades profesionales y en particular debe contar con conocimientos especializados del Derecho y práctica en protección de datos; a este respecto, es de destacar que un 8% de las personas encuestadas se consideran poco formadas.



26. % Organismos con relación a su percepción de la formación (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

En cuanto a concienciación, según la perspectiva del/de la DPD, un 15% del personal responsable del tratamiento, un 21% del personal directivo y un 10% del resto del personal está poco o nada concienciados con la materia.



27. % Organismos con relación a su percepción de la concienciación (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

5.6. Violaciones de seguridad

El RGPD define las violaciones de seguridad de los datos, más comúnmente conocidas como "brechas de datos personales", de una forma muy amplia, e incluye todo incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

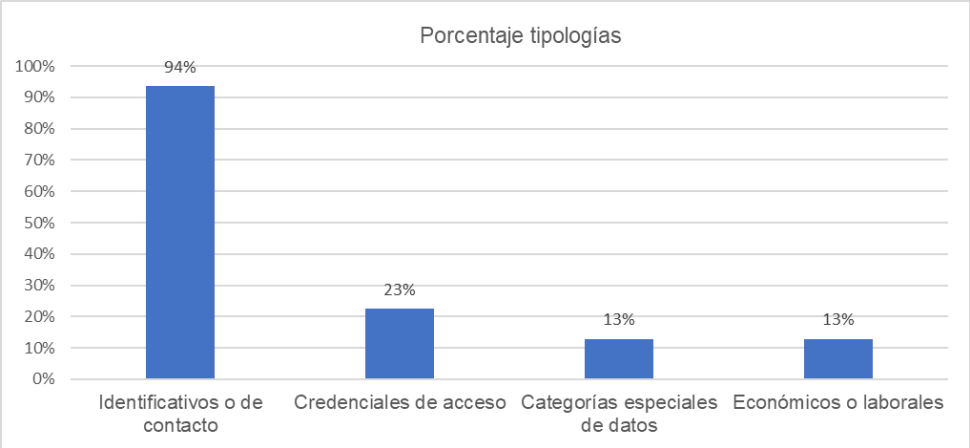
Una brecha de datos personales puede tener una serie de efectos adversos considerables en las personas, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales; por lo que hay que intentar evitarlas y en caso de que sucedan gestionarlas adecuadamente, especialmente cuando puedan poner en riesgo los derechos y libertades de las personas físicas.

El artículo 33 del RGPD impone a los responsables de un tratamiento de datos personales la obligación de notificar a la autoridad de control competente las brechas de datos personales cuando sea probable que constituyan un riesgo para los derechos y libertades de las personas y, además, cuando el riesgo sea alto, el responsable también deberá comunicar la brecha a las personas afectadas conforme al artículo 34 del RGPD.

A este respecto indicar que un 30% de los organismos, no tiene definido un procedimiento de comunicación de las mismas, en su ámbito competencial, un 41% no lo tenía definido para notificar a la autoridad de control y un 44% no lo tenía para comunicar a las personas interesadas.

Asimismo, un 67% de los organismos declaró no tener procedimientos de revisión del tratamiento tras producirse una violación de la seguridad.

Por otra parte, indicar que del 79% que declaró haber tenido alguna violación de la seguridad desde la entrada en vigor del RGPD, un 94% de las mismas afectó a datos identificativos o de contacto, un 23% a las credenciales de acceso, un 13% a categorías especiales de datos y un 13% a datos económicos o laborales, tal como se muestra en el gráfico a continuación:



28. % Tipologías de violaciones de seguridad (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

No existen criterios homogéneos para realizar las comunicaciones de violaciones de seguridad.

No hay procedimientos de revisión del tratamiento, tras producirse una brecha, en la mayoría de los organismos.

Las causas por las cuales se han producido estas brechas han sido las siguientes, expresadas en porcentajes:

- 62% factor humano
- 21% intervención de terceros
- 21% fallo informático
- 3% pérdida o sustracción de portátil

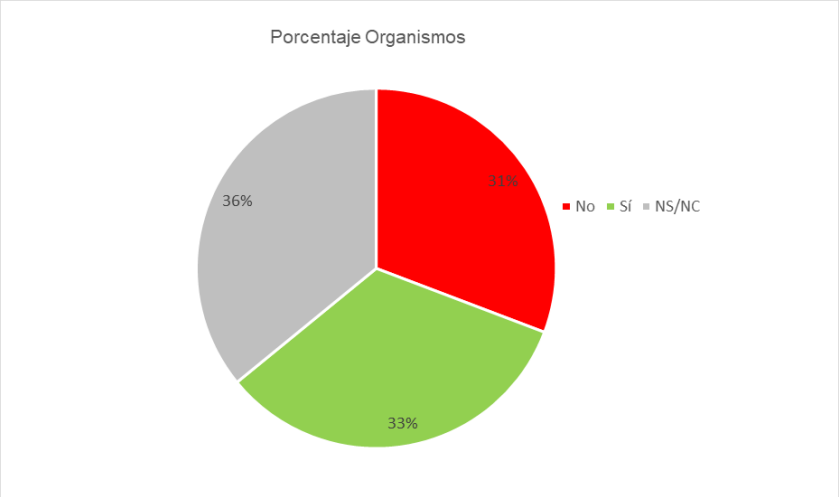
Por otro lado, respecto a las formas de detección de las mismas, se trata de los siguientes supuestos:

- 41% a través del personal TIC
- 38% a través de las reclamaciones de las personas afectadas
- 28% por las personas responsables del tratamiento
- 3% por la autoridad de control
- 3% por parte de otro personal del organismo

5.7. Medidas de seguridad y auditoría

Con el fin de mantener la seguridad de los datos, los responsables o los encargados de los tratamientos, deben evaluar los riesgos inherentes a los mismos y aplicar medidas para mitigarlos.

Entre las medidas que contempla el RGPD a este respecto, se encuentra el cifrado de los datos. Esta medida se aplica en un 33% de los organismos encuestados, tal como recoge la imagen a continuación:

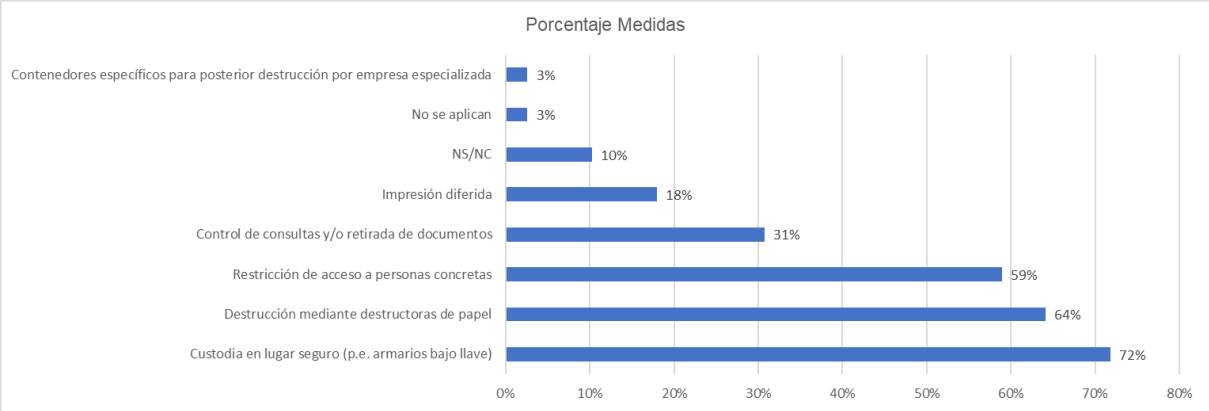


29. % Organismos que aplican el cifrado de datos como medida de seguridad (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

La mayoría de los organismos no utiliza el cifrado de datos.

En lo que se refiere al tratamiento de datos no automatizados, los organismos encuestados declararon aplicar diferentes medidas específicas, entre las que se destacan:

- Custodia en lugar seguro, un 72%.
- Utilización de destructoras de papel, un 64%.
- Restricción de acceso a personas concretas, un 59%



30. % Organismos en función de las medidas de seguridad que aplican (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

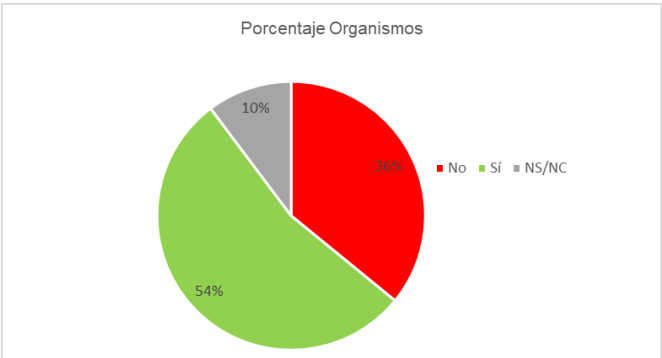
Cabe destacar la respuesta de un organismo que indicó que no se aplican medidas específicas.

Las medidas de seguridad de los datos no automatizados son diferentes en cada organismo.

En lo que respecta a la auditoría de protección de datos, también llamada auditoría LOPD o auditoría RGPD, indicar que éste es un proceso de verificación que hace la empresa u organización, tanto de los tratamientos de datos personales, como de las medidas de seguridad técnicas y organizativas implementadas por el responsable del tratamiento, así como su eficacia, de los encargados del tratamiento y de la finalidad para la que se destinan los datos recabados.

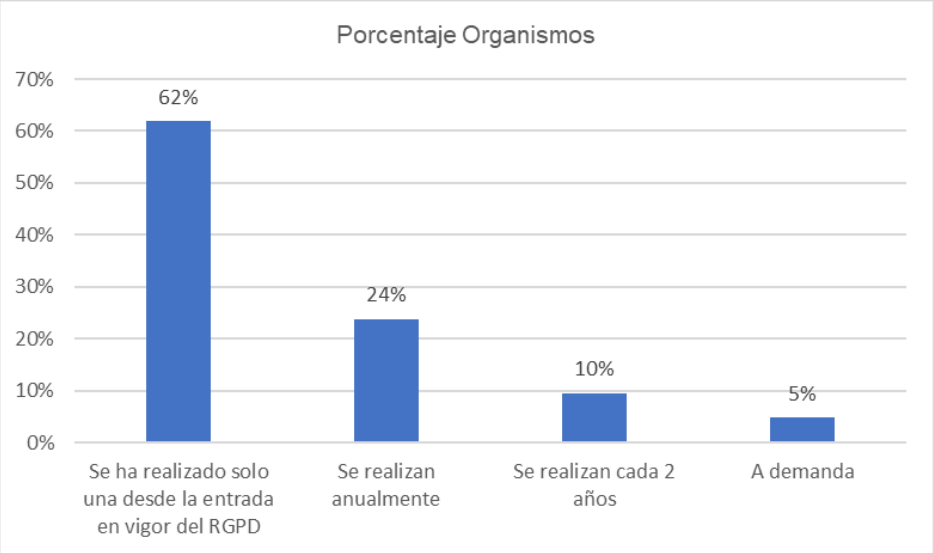
El artículo 96.1 del R.D. 1720/2007, de 21 de diciembre, establecía la realización de auditorías cada dos años.

A este respecto, según se desprende de la encuesta realizada, un 36% de los organismos declaró no realizar ninguna, frente a un 54% que sí lo ha hecho y un 10% que no sabe o no contesta.



31. % Organismos con relación a la realización de auditorías (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

Aquellos organismos que sí las realizan, preguntados sobre la periodicidad de las mismas, declararon en un 62% que habían hecho una desde la entrada en vigor del RGPD.

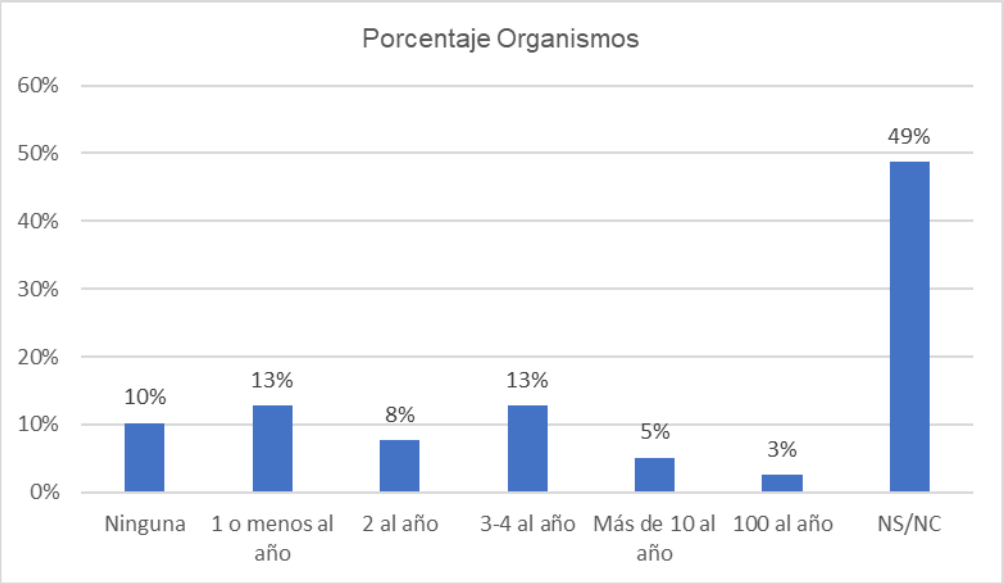


32. % Organismos con relación a la periodicidad de las auditorías (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

5.8. Consulta y ejercicio de los derechos

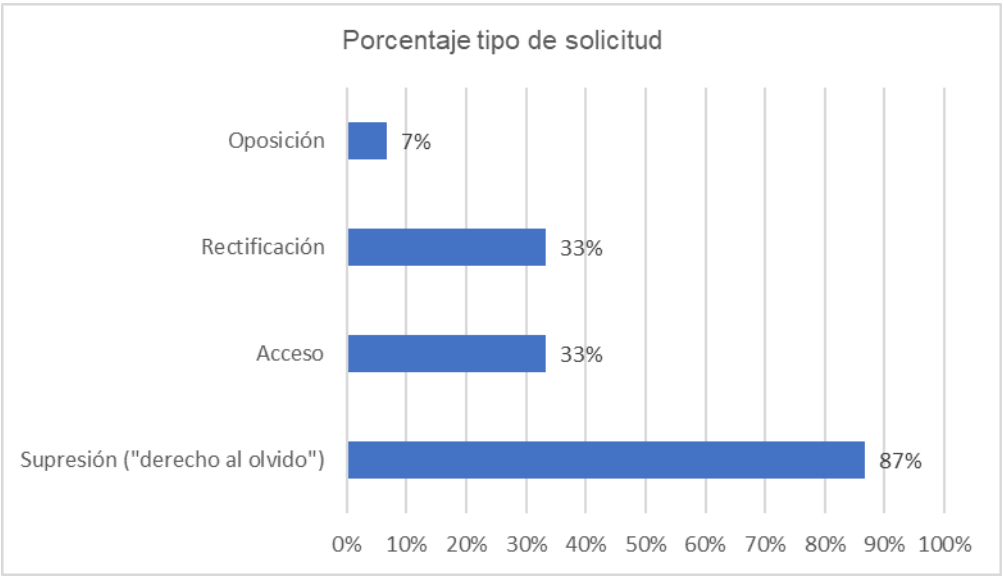
La normativa de protección de datos permite que se pueda ejercer ante el responsable del tratamiento, el derecho de acceso, rectificación, oposición, supresión ("derecho al olvido"), limitación del tratamiento, portabilidad y a no ser objeto de decisiones individualizadas.

En este sentido, un 49% de los y las DPD declaró no saber nada al respecto y un 10% declaró que no se había recibido ninguna consulta. Realmente este ejercicio se realiza ante las personas responsables de los tratamientos, por eso los datos que se muestran a continuación:



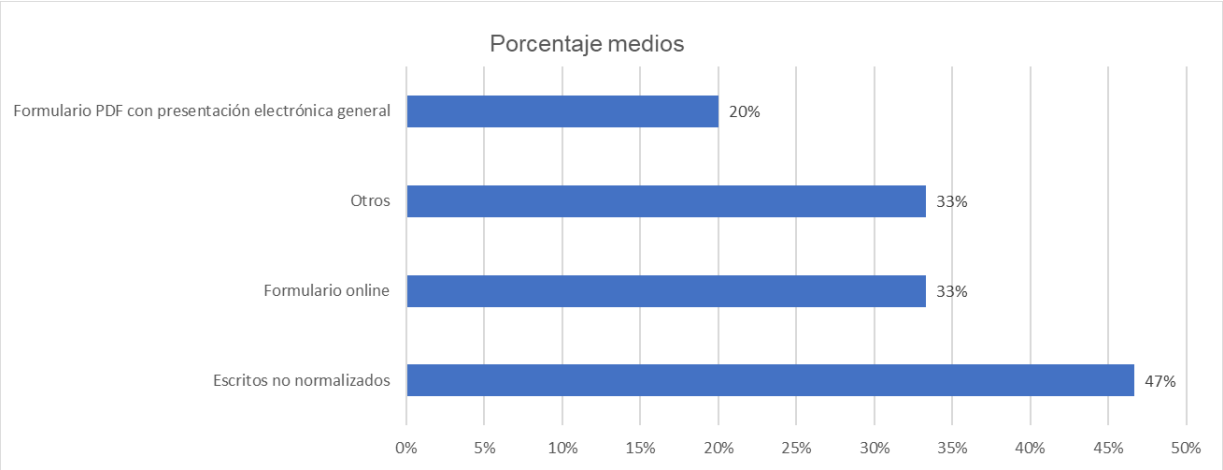
33. % Organismos con relación al ejercicio de los derechos de acceso (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

En cuanto a los organismos que respondieron que sí habían recibido solicitudes en este sentido, indicar que el derecho más ejercido ha sido el de supresión o derecho al olvido con un 87% de frecuencia, les siguen de lejos los derechos de rectificación y de acceso con un 33% de frecuencia cada uno y el de oposición con un 7%.



34. % Organismos con relación al tipo de solicitud de ejercicio de los derechos (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

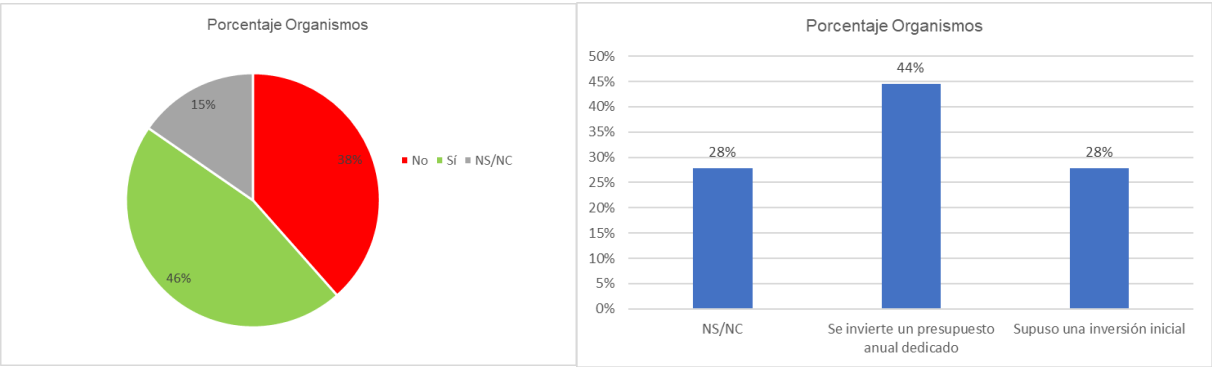
Todas las solicitudes presentadas, según manifiesta el 100% de los organismos encuestados, se respondieron dentro del plazo de un mes que está establecido por la normativa y un 47% de las mismas se recibieron a través de documentos no normalizados, tal como se indica a continuación:



35. % Organismos con relación al medio por el que se reciben las solicitudes de ejercicio de los derechos (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

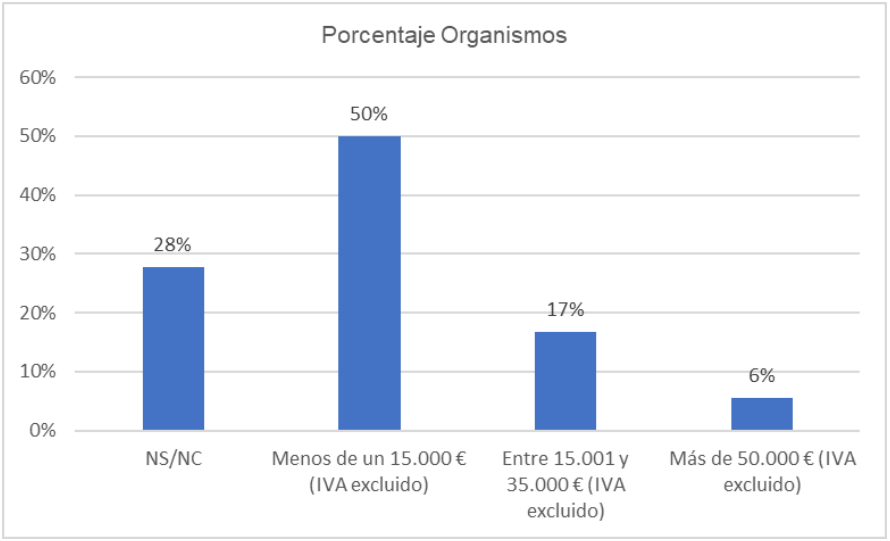
5.9. Costes de implantación del RGPD y normativa asociada

Un 38% de los organismos encuestados declararon que no ha supuesto ningún coste económico la adaptación a la normativa, frente a un 46% que declararon que sí. De estos últimos un 28% manifestaron que supuso una inversión inicial y un 44% que se invierte un presupuesto anual dedicado expresamente a estos efectos.



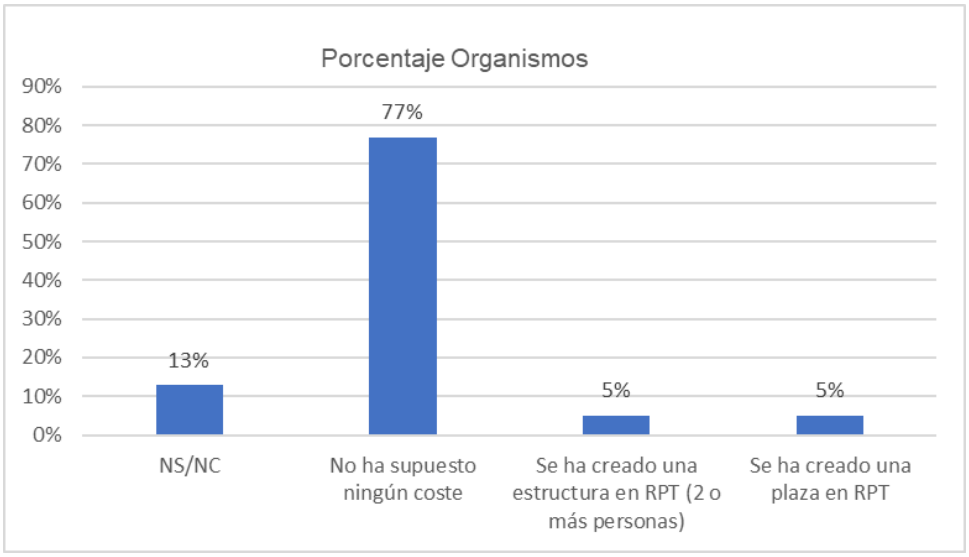
36. % Organismos con relación al presupuesto invertido para la adaptación a la normativa de protección de datos (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

El presupuesto invertido a esos efectos, en un 50% de los organismos ha sido un contrato menor (15.000 euros), un 17%, el importe ha oscilado entre 15.001 y 35.000 euros y sólo un 6% considera que se ha invertido más de 50.000 euros.



37. % Organismos con relación a la cuantía invertida (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

Respecto a la pregunta relativa al posible cambio de tipo organizativo en la organización, para adaptar la normativa en materia de protección de datos, un 77% de los organismos encuestados consideran que no ha supuesto ningún coste, un 5% (2 organismos) manifiestan que se ha creado una estructura de RPT con 2 o más personas y otro 5% especifica la creación de una plaza de RPT.



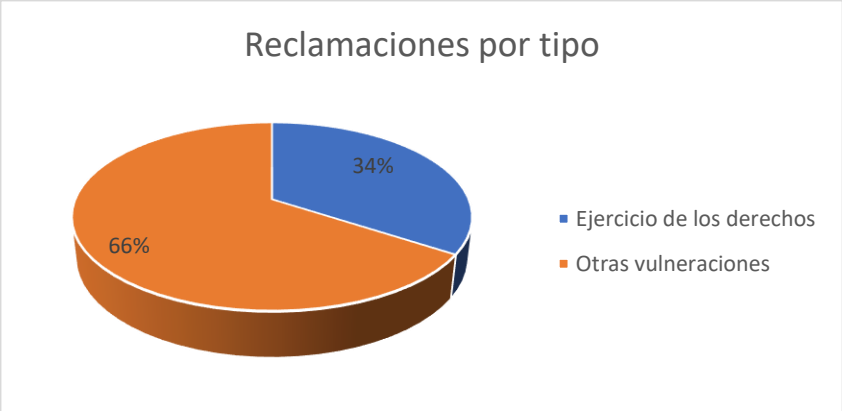
38. % Organismos con relación a los costes organizativos (Fuente: elaboración propia a partir de información de la encuesta (abril-2023))

Por último, cabe indicar que la Junta de Andalucía no ha dictado ninguna norma específica de obligado cumplimiento en esta materia. En la pasada legislatura se redactó un borrador de Decreto que finalmente no fue aprobado.

5.10. Consejo de Transparencia y Protección de Datos de Andalucía: Reclamaciones y apercibimiento

El Consejo de Transparencia y Protección de Datos de Andalucía (CTPDA), creado por el artículo 43 de la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía, es la autoridad independiente de control en materia de transparencia y protección de datos en la Comunidad Autónoma de Andalucía. Tiene la consideración de Administración Institucional, lo que significa que posee personalidad jurídica propia y plena autonomía e independencia en el ejercicio de sus funciones.

Las reclamaciones realizadas a la Junta de Andalucía ante el CTPDA, extraídas de su memoria anual[9] de 2022 han sido 84 de las 238 reclamaciones totales recibidas en 2022 en materia de protección de datos (114 si incluimos las entidades dependientes de la administración autonómica). Estas cifras representan el 35,3% del total (47,9% incluyendo las entidades dependientes). En cuanto a los motivos de las reclamaciones, el 34% de las relativas a la administración autonómica y sus entidades dependientes han sido relativas al ejercicio de derechos, y el 66% han sido relativas a otras vulneraciones.



39. % Reclamaciones por tipo (Fuente: elaboración propia a partir de información del CTPDA - 2022))

En base a la redacción original del artículo 77.2 de la LOPDGDD, vigente hasta el 9 de mayo de 2023, cuando las Administraciones Publicas cometan cualquier tipo de infracción del RGPD o LOPDGDD, "[…] la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento".

Las reclamaciones interpuestas ante el CTPDA que han dado lugar a la sanción de apercibimiento a la Junta de Andalucía han sido un total de 13 desde el año 2019, el 54% de las mismas estaban relacionadas con el artículo 32.1 del RGPD, es decir "Falta de aplicación de adecuadas medidas técnicas y organizativas".

Este dato, siendo correcto, no parece significativo a la vista de los incumplimientos reales, por lo que se podría decir que se reclama poco por parte de la ciudadanía, tal vez porque la privacidad de los datos en sus relaciones con la Administración Pública no se percibe como un problema, o bien porque la ciudadanía no esté formada suficientemente en esta materia y desconoce sus derechos.

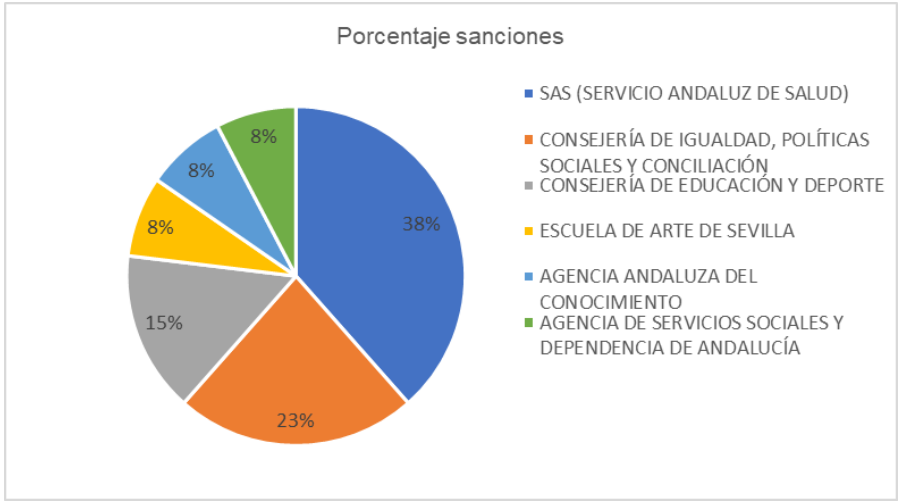
[9] Informes anuales de actuación del CTPDA: https://www.ctpdandalucia.es/transparencia-del-consejo/planificacion-evaluacion-estadistica/informes-anuales-de-actuaci%C3%B3n

Artículo RGPD	Descripción	Tota	%Total
Art. 32.1	Falta de aplicación de adecuadas medidas técnicas y organizativas	7	54%
Art. 28	Vulneración en relación a la obligación de establecer un vínculo jurídico entre responsable y encargado del tratamiento	1	8%
Art. 5.1.c), 35	Vulneración del principio de "minimización de datos" y Evaluación de impacto relativa a la protección de datos	1	8%
Art. 29, 32.1	Vulneración en relación al "Tratamiento bajo la autoridad del responsable o del encargado del tratamiento" y Falta de aplicación de adecuadas medidas técnicas y organizativas	1	8%
Art. 5.1.f)	Vulneración del principio de "integridad y confidencialidad"	1	8%
Art. 29, 32.1	Vulneración en relación al "Tratamiento bajo la autoridad del responsable o del encargado del tratamiento"	1	8%
Art. 5.1.c), 5.1.f)	Vulneración del principio de "minimización de datos" y Vulneración del principio de "integridad y confidencialidad"	1	8%
		13	

40. % Reclamaciones con relación a la vulneración infringida (Fuente: elaboración propia a partir de información del CTPDA (mayo-2023))

Los organismos que han sido sancionados son los siguientes, según se muestra en el gráfico a continuación:

- SAS (cinco apercibimientos): 38%
- Consejería de Igualdad, Políticas Sociales y Conciliación (tres apercibimientos): 23%
- Agencia de Servicios Sociales y Dependencia y la Consejería de Educación y Deporte (dos cada una): 8%
- Escuela de Arte y la Agencia Andaluza del Conocimiento (un apercibimiento cada una): 8%



41. % Sanciones por Organismo (Fuente: elaboración propia a partir de información del CTPDA (mayo-2023))

5.11. Conclusiones generales

5.11.1. Encuesta a Delegados/as Protección de Datos

- Un 37% de organismos no tienen publicado el RAT ni el inventario de DPD en el portal de transparencia.
- En la Junta de Andalucía no existen criterios homogéneos para nombrar al / a la DPD (distintos Cuerpos de procedencia, distintos niveles retributivos, distintas titulaciones académicas y relaciones jurídicas con la Administración).
- Sólo 2 organismos, el 5% ha creado una plaza específica y otros 2 una estructura de dos o más plazas.
- Un 64% de los DPD ha declarado no haber recibido ninguna consulta, en materia de protección de datos, lo cual contrasta con el hecho de que sus funciones principales son las de asesoramiento y consulta.[10]
- No se comunica quién es el/la DPD al resto de la organización, cuando debe ser un punto de contacto con la autoridad de control.[11]
- **Marco organizativo de la seguridad en P.D.:**
    - Un 10% de organismos declaran no tener política de seguridad y un 13% de DPD declaran que no se coordinan con la persona responsable de seguridad.
    - Un 44% no tienen definidos procedimientos de seguridad específicos en materia de protección de datos.
- **Registro de Actividades de Tratamiento:**
    - No existen criterios homogéneos a la hora de definir las actividades de tratamiento ni quiénes son las personas encargadas de hacerlo, en un 38% de los organismos.
    - Un 38% de DPD declara que su organismo no tiene completo el RAT.
    - Un 54% declara que no tiene procedimientos definidos de altas, bajas y modificaciones del RAT en el portal de transparencia.
    - Un 72% de los organismos encuestados declararon no tener publicados los inventarios de tratamientos en los que actúan como encargado.
    - Sólo un 28% tiene una relación de contratos de encargo asociados a los tratamientos.
    - La ADA es quien actúa como Encargado de la mayor parte de los tratamientos de la Junta de Andalucía, pero no existe un contrato específico de encargado de tratamiento como tal, que regule sus obligaciones.

[10] Informar y asesorar al responsable o encargado y a los empleados que se ocupen del tratamiento de las obligaciones que le incumben en virtud de las disposiciones en materia de protección de datos (art. 39.1 a) RGPD)
[11] Recibir las reclamaciones que las personas interesado puedan presentar previamente a reclamar ante la autoridad de control y comunicar una decisión en plazo de dos meses. (art. 37.1 LOPDPGDD). Responder a las reclamaciones que le sean remitidas por la autoridad de control. (art 37.2 LOPDPGDD).

- Sólo un 8% declara tener sus tratamientos completamente automatizados.
- Un 10% han declarado no saber si se aplican medidas de seguridad a los tratamientos no automatizados y un 3% han declarado que no se aplica ninguna medida. Los tratamientos de datos sin automatizar no tienen medidas específicas asociadas a la seguridad de los mismos.

- **Responsabilidad proactiva:**
  - No existen criterios homogéneos para la realización de análisis de riesgo y de evaluaciones de impacto, tampoco con respecto a quién los realiza.
  - Un 51% de organismos no dispone de herramientas que faciliten el cumplimiento de la responsabilidad proactiva.
  - El resto (49%) dispone de herramientas ofimáticas o sin coste, sólo el 5% (1 organismo) dispone de una herramienta de mercado con coste asociado.
- **Formación/Concienciación:**
  - Hay entre un 10% y un 20% de perfiles poco o nada formados ni concienciados en materia de protección de datos.
  - Un 8% de lo/as DPD se declaran poco o nada formados.
  - Hay numerosas respuestas a lo largo del cuestionario en las que aparece NS/NC. Entre las funciones está la supervisión en esta materia[12].
- **Violaciones de seguridad:**
  - Entre un 30 y un 40% de los organismos declara no tener establecidos criterios homogéneos de comunicación de la violación, de comunicación a la autoridad de control, ni de comunicación a las personas afectadas.
  - Un 67% declara no tener procedimientos de revisión tras una violación, lo cual podría provocar que, al no tomarse medidas correctoras, se repitan las mismas circunstancias que dieron lugar a la violación de seguridad.
  - Las más frecuentes están relacionadas con datos identificativos o de contacto, seguida de las credenciales de acceso. Solo un 13% afectan a categorías especiales de datos y otro 13% a datos económicos o laborales.
  - La principal causa es el factor humano, seguida del fallo informático.
  - La forma de detección más usual es a través del personal TIC.
  - En un 41% de organismos (38% + 3%) se detectaron a través de fuentes externas, por ejemplo, por los propios interesados o por el CTPDA.
- **Medidas de seguridad y auditoría:**
  - La mayoría de los organismos no utiliza el cifrado de datos.

[12] Supervisar el cumplimiento de lo dispuesto en las disposiciones en la materia y de las políticas del responsable o encargado. (art. 39.1 b) RGPD).

- Las medidas de seguridad de los datos no automatizados son diferentes en cada organismo.
- El artículo 96.1 del Reglamento de la LOPD (Real Decreto 1720/2007, de 21 diciembre) establece la realización de auditorías cada dos años. La mayoría de los organismos que las han realizado dicen haber hecho sólo una desde la entrada en vigor de RGPD.
- No es frecuente que se consulte a la autoridad de control, sólo dos organismos han realizado una consulta cada uno y el 64% de lo/as DPD declara no haber recibido ninguna solicitud de asesoramiento.

- **Consulta y ejercicio de los derechos:**
  - Todos los organismos declaran contestar en plazo y las solicitudes más frecuentes son supresión o derecho al olvido en un 87% de los casos, seguido de acceso y rectificación en un 33%.
  - El derecho de oposición se ha ejercido de forma residual y el resto de los derechos no ha sido ejercido nunca.
- **Costes de implantación del RGPD y normativa asociada:**
  - Un 38% de los organismos encuestados declararon que no ha supuesto ningún coste económico la adaptación a la normativa, frente a un 46% que declararon que sí.
  - Un 77% indica que no ha tenido tampoco costes organizativos, ya que la persona que ejerce como DPD simultanea sus tareas con otras actividades sin que haya una pauta específica a la hora de que puedan ser homogéneas o relacionadas. Tampoco ha supuesto coste normativo.
  - De los que han contestado que sí ha habido coste económico, un 28% dicen que supuso sólo una inversión inicial, en la mayoría de los casos un contrato menor. Sólo un organismo afirma haber realizado una inversión superior a 50.000€.

5.11.2. Grupo focal con personas expertas

Celebrado en el mes de junio de 2023, estaba compuesto por los siguientes perfiles:

- 1 persona Responsable de tratamiento
- 1 persona Encargado/a de tratamiento
- 1 persona responsable de seguridad TIC
- 1 DPD ADA
- 1 Inspector/a General de Servicios
- 1 persona responsable de la coordinación en materia de protección de datos dependiente del Gabinete de Planificación Estratégica que no hubiera intervenido en la realización del presente diagnóstico
- 1 DPD de Consejería
- 1 DPD de Agencia

- 1 persona responsable de Informática

A estas personas se les realizaron las siguientes preguntas:

- ¿Cree que los datos de la ciudadanía están realmente protegidos en la Junta de Andalucía? Sí/No. Argumente su respuesta.
- ¿Considera que hay alguna dimensión esencial que no se haya analizado? Sí/No. ¿Cuál?
- A la vista de los incumplimientos que considere más relevantes, señale las causas que en su opinión son origen de los mismos.
- ¿Qué medidas a corto, medio plazo considera esenciales para solucionar los problemas más graves?

Las principales conclusiones obtenidas tras la realización del grupo focal son las siguientes:

Desde el punto de vista de la seguridad TIC, los datos de la ciudadanía andaluza están suficientemente protegidos de ciberataques con el riesgo residual que la Administración asume, hay normativa y una estructura organizativa específica, así como dotación económica. Desde la ADA existe un fuerte compromiso con el cumplimento del ENS así como en el resto de los organismos afectados.

En cuanto a la protección de los derechos y libertades fundamentales en materia de protección de datos consideran que faltan recursos en las tres dimensiones analizadas normativa, organizativa y económica. **Las carencias son más acusadas en los tratamientos no automatizados.**

También se destacan la **falta de evidencias para demostrar la responsabilidad proactiva**, la **poca implantación de la seguridad** desde el diseño y por defecto, y la **falta de formación y concienciación** en la materia.

La protección de datos desde el diseño y por defecto viene regulada en el artº 25 del RGPD, en el siguiente sentido: "*Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento...*" .

En opinión de las personas expertas consultadas, no basta con crear un puesto específico para la persona que ejerza como DPD, se precisa mayor formación en todos los ámbitos y en especial en los relacionados con el desarrollo e implantación de los sistemas de información para que se aplique correctamente el principio de protección de datos desde el diseño y por defecto. No se debe considerar la seguridad como una capa adicional que se añade "a posteriori", cuando el producto está acabado, y no desde el diseño y por defecto, tal como define la normativa.

De cara a aprovechar sinergias con la seguridad TIC, que se encuentra más consolidada, las personas expertas echan en falta en este diagnóstico el análisis de la seguridad interior, los servicios esenciales y las infraestructuras críticas que permitirían realizar un diagnóstico más certero de la situación, para poder planificar la puesta en marcha de un **sistema de gestión de la seguridad con todas sus facetas: interior, TIC y la protección de datos de carácter personal**. La ausencia de una herramienta que facilite e integre todas estas perspectivas, impacta en una correcta y completa adecuación normativa.

La **elaboración de instrucciones y recomendaciones de buenas prácticas**, así como la implantación de procedimientos comunes en materia de protección de datos, se considera esencial para dar un impulso positivo a la implantación del RGPD-LOPDGDD en la Comunidad Autónoma de Andalucía.

Ante la posible falta de motivación de los organismos, a la hora de cumplir la normativa en materia de protección de datos, podría ser interesante plantear compromisos, medidas y responsabilidades, elaborando un código de buen gobierno y ética en la Junta de Andalucía en esta materia.

Se habló de la necesidad de protocolizar la relación entre DPD y Responsables de los tratamientos, así como de la posibilidad de crear la figura de un enlace, interlocutor o responsable delegado entre DPD y el personal técnico, sin necesidad de crear una estructura específica en la RPT, dado que muchas veces coincide con el responsable de transparencia, el cual podría hacer también de interlocutor en materia de protección de datos.

Por otro lado, no hay que olvidar los aspectos positivos existentes en nuestra Comunidad Autónoma, dado que somos referentes en la Junta de Andalucía, frente a toda España, por ejemplo, en la realización de certificaciones del ENS, asimismo hay que resaltar las inversiones realizadas en ciber seguridad y la creación de una estructura organizativa en la Relación de Puestos de Trabajo, en materia de seguridad TIC, lo cual representa un avance importante.

5.11.3. Encuesta a la ciudadanía

El Instituto de Estadística y Cartografía de Andalucía (IECA), realizó una Encuesta Social en el año 2021, entre cuyos apartados se encontraba el tema de la Digitalización y uso de datos personales.

La información se recogió entre el 18 de octubre y el 31 de diciembre de 2021, con una muestra efectiva de 4.675 personas, residentes en Andalucía de 16 a 75 años. Se analizó la percepción que se tiene individualmente sobre qué se hace con sus datos personales y la protección de los mismos.

El resumen de los resultados se muestra a continuación:

Un 10,2% de la población andaluza se siente muy informada de los riesgos que puede conllevar proporcionar datos personales, mientras que **más de la mitad de las personas encuestadas (54,5%) se considera poco o nada informada**.

Observando perfiles más específicos, existe también una brecha en la percepción de desinformación que aumenta con la edad: el 13,3% de las personas encuestadas de 66 a 75 años se considera nada informado sobre los riesgos que puede conllevar proporcionar datos personales, frente al 5,5% de la población de 26 a 35 años.

En general las personas que menos informadas se consideran son aquellas con estudios primarios, un 20,3%.

A la hora de dar el consentimiento para disponer de los datos personales, una de cada cuatro personas en Andalucía nunca lo hace. El perfil demográfico que es más reticente a ceder sus datos personales, son las mujeres de 66 a 75 años con un 46,8% de su población, frente al 7,4% de las mujeres de entre 16 y 25 años.

Respecto a la percepción del riesgo al proporcionar datos personales, **el 78,6% de la población andaluza piensa que es muy o bastante probable que sus datos puedan ser usados sin su consentimiento**.

El **riesgo de suplantación de identidad** lo perciben en alto grado el 66,7%.

La respuesta a la pregunta: ¿En quién confía la población andaluza?, es la siguiente:

En cuanto a la cesión de datos personales, se confía mayoritariamente en las entidades públicas. Los Servicios de Salud Pública son los que mayor confianza generan, el 92,8% confía en ellos a la hora de ceder sus datos, seguidos por la Administración Pública con un 86,5%.

Las entidades privadas generan menor confianza a la hora de ceder datos personales, salvo los bancos en los que confía un 71,9% de la población.

6. Diagnóstico

6.1. Problemas, Necesidades y Retos

Este diagnóstico de situación pone en evidencia que en la Junta de Andalucía no se han empleado todos los recursos necesarios para un correcto cumplimiento de la normativa y que se requiere un plan de actuación inminente para mejorar y/o corregir las carencias detectadas.

Es de destacar la diligencia con la que ha actuado la organización en relación con el registro de actividades de tratamiento a la fecha de difusión del diagnóstico entre el personal DPD a finales de 2023 pasando de 2.022 actividades de tratamiento a 2.176 y de 51 DPD a 68 registrados en el portal de transparencia de la Junta de Andalucía a fecha de septiembre de 2024[13]. Adicionalmente, queremos poner en valor la decisión de realizar este Plan Estratégico con actuaciones a corto plazo, así como el establecimiento de esas actuaciones a futuro y la estructura de gobernanza que se ha creado en torno a la CICRA que confiamos en que conducirán a la Junta de Andalucía a ser un referente en esta materia.

A continuación, se recogen los problemas, necesidades y retos (PNR), identificados en el análisis de la situación de partida de la Protección de Datos en la Junta de Andalucía, elaborado por la Oficina Técnica del Plan, su priorización se llevó a cabo en la Comisión Interdepartamental de Coordinación y Racionalización Administrativa (CICRA) dado que dicho órgano es el Comité Directivo del mismo.

PROBLEMAS	P1. No existen criterios homogéneos, a la hora de definir las actividades de tratamiento, ni quienes son las personas encargadas de hacerlo.
	P2. No hay una relación de contratos de encargo asociados a los tratamientos.
	P3. La mayoría de los tratamientos de datos no están automatizados y no cuentan con medidas de seguridad específicas.
	P4. El RAT no está publicado en la totalidad de los organismos, ni el inventario de los/as DPD.
	P5. No hay definidos procedimientos de seguridad específicos en materia de protección de datos.
	P6. En la Junta de Andalucía no existen criterios homogéneos para nombrar al / a la DPD, ni existe una estructura homogénea en la RPT de las diferentes Consejerías o Agencias de la Junta de Andalucía.
	P7. No se comunica al resto de la organización los datos de la persona que ejerce como DPD.
	P8. La realización de análisis de riesgo y de evaluaciones de impacto no tiene un procedimiento normalizado.

[13] Datos obtenidos de los registros de tratamientos y DPD publicitados en: https://juntadeandalucia.es/protecciondedatos.html

	P9. Ausencia de criterios homogéneos a la hora de comunicar las brechas de datos a los diferentes entes implicados.
	P10.La falta de procedimientos de revisión, tras una violación de seguridad, puede provocar que se vuelva a repetir.
NECESIDADES	N1. Crear una herramienta informática que facilite la gestión del riesgo, el cumplimento de la normativa y que dé soporte a la responsabilidad proactiva.
	N2. Dotar la RPT de un puesto de trabajo en exclusiva para ejercer como DPD y comunicar los datos de la persona nombrada a la organización
	N3. Impartir más formación en protección de datos para los y las responsables de los tratamientos.
	N4. Mejorar la concienciación en esta materia para los y las responsables de los tratamientos.
	N5. Realizar una formación especializada obligatoria para los y las DPD, con carácter periódico.
	N6. Crear una normativa específica para regular esta materia en la Administración de la Junta de Andalucía.
	N7. Implantar más medidas de concienciación y formación en protección de datos para todo el personal.
	N8. Desarrollar e implementar procedimientos comunes y homogéneos en los diferentes ámbitos de aplicación: metodología simplificada.
	N9. Impulsar medidas de coordinación entre los diferentes gestores.
	N10. Implantar mecanismos de motivación en el cumplimiento normativo, mediante la creación de un código de buen gobierno y ética en la protección de datos en la Junta de Andalucía: manual de buenas prácticas.
	N11. Mejorar la gestión del RAT: diseño de altas, bajas y modificaciones.
	N12.Mejorar las actuaciones internas para la detección de violaciones de seguridad.
	N13. Realizar campañas de información a la ciudadanía.
RETOS	R1. Ser una Administración referente en la ejecución y adaptación normativa de la protección de datos personales en Andalucía.
	R2. Construir un sistema de gestión de la información, con un sistema de gobernanza del dato que permita la toma de decisiones tanto operacionales como estratégicas, en materia de protección de datos en la Junta de Andalucía.

	R3. Implantar medidas de seguridad de los datos desde el diseño y por defecto, integrando todas las perspectivas: interior, TIC y protección de datos personales.

6.2. DAFO

Debilidades	Amenazas
Recursos Limitados: Presupuesto y recursos humanos limitados para implementar todas las medidas de seguridad necesarias. **Actualización Continua:** Necesidad constante de actualizar sistemas y procedimientos para mantenerse al día con las nuevas amenazas. **Concienciación:** Falta de concienciación y formación continua entre todos los empleados sobre la importancia de la protección de datos.	**Ciberataques:** Incremento en la frecuencia y sofisticación de los ciberataques. **Cumplimiento Normativo:** Riesgo de sanciones por incumplimiento de las normativas de protección de datos. **Fugas de Información:** Posibilidad de fugas de datos debido a errores humanos o fallos en los sistemas.
Fortalezas	**Oportunidades**
Marco Legal Sólido: Cumplimiento con el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos (LOPD). **Infraestructura Tecnológica:** Sistemas y tecnologías avanzadas para la gestión y protección de datos. **Personal Capacitado:** Equipos de trabajo con formación específica en protección de datos.	**Innovación Tecnológica:** Implementación de nuevas tecnologías como la inteligencia artificial para mejorar la seguridad de los datos. **Colaboración:** Posibilidad de colaborar con otras instituciones y empresas para compartir conocimientos y recursos. **Regulación:** Nuevas regulaciones que pueden fortalecer aún más la protección de datos.

7. Objetivos

Partiendo de los problemas, necesidades y retos enunciados arriba, se han determinado las líneas estratégicas y los objetivos mediante los cuales se pretende dar respuesta a los primeros.

Objetivo	Descripción
OE01.- Mejorar las actuaciones de prevención para un cumplimiento más eficaz del derecho a la protección de datos de carácter personal.	Este objetivo estratégico pretende garantizar un cumplimiento adecuado de la normativa y prevenir brechas de datos personales. Da cobertura a los siguientes PNR: P1, P2, P9, N3, R1, R2, R3.
OE02.- Mejorar la gestión de las brechas de datos personales.	Este objetivo estratégico está orientado a realizar una gestión homogénea de las brechas de datos personales, así como para el seguimiento de las mismas, que permita que no vuelvan a producirse. Da cobertura a los siguientes PNR: P7, P8, N13, R1.
OE03.- Impulsar la protección de datos desde el diseño y por defecto.	Este objetivo estratégico va encaminado a facilitar la implantación de las medidas desde el diseño y por defecto en la organización que mitiguen los riesgos asociados al tratamiento de datos personales. Da cobertura a los siguientes PNR: N3, R2, R3.
OE04.- Garantizar la privacidad en los contratos de servicios.	Este objetivo estratégico va encaminado a mejorar la gestión de los contratos o actos jurídicos equivalentes que vinculan a los responsables con los encargados de tratamiento. Da cobertura a los siguientes PNR: P6, R2.
0E05.- Garantizar la privacidad y facilitar el ejercicio de los derechos de la ciudadanía.	Este objetivo estratégico va encaminado a mejorar la gestión del registro de actividades de tratamiento y su publicidad de modo que siempre ofrezca información actualizada y presentada con formato homogéneo, lo que contribuye a facilitar el ejercicio de los derechos en materia de protección de datos por parte de la ciudadanía. Da cobertura a los siguientes PNR: P3, P5, N8, R1, R2, R3.
OE06.- Reforzar la figura de DPD en la organización.	Este objetivo estratégico va encaminado a situar la figura del DPD en el contexto de la organización administrativa de la Junta de Andalucía definiendo tanto su estatuto personal (grupo de clasificación, nivel, procedimiento de nombramiento y cese, etc.) como funcional (adscripción orgánica, dedicación exclusiva, oficina de apoyo, etc.) Igualmente se pretende potenciar el conocimiento de la figura del DPD en el seno de la organización. Da cobertura a los siguientes PNR: P4, P10, N4, N11, N12, R2, R3.

Objetivo	Descripción
OE07.- Proporcionar recursos que mejoren el desempeño de la figura de DPD.	Este objetivo estratégico pretende dotar a los y las DPD de herramientas (normativas, informáticas, etc.) que faciliten y permitan ganar efectividad en el desempeño de sus funciones. Se incluye la realización de formación especializada para las personas que ostentan el rol de DPD con el objeto de que adquieran competencias especializadas en esta materia y se facilite su reciclaje y formación continua. Da cobertura a los siguientes PNR: N1, N2, N7, R2, R3.
OE08.- Mejorar la adquisición de competencias en materia de protección de datos	Con este objetivo estratégico se pretende formar y concienciar a todas las personas responsables de tratamiento y al personal empleado público en general, en materia de protección de datos para la adquisición de estas competencias específicas. Asimismo, incluye la realización de formación o campañas de sensibilización entre el personal directivo para que adquieran mayor concienciación en esta materia y se involucren en la gestión de la protección de datos en su organización. Da cobertura a los siguientes PNR: N5, N6, N9, R2.
OE9.- Mejorar la información y la visibilidad de la información en materia de protección de datos que se ofrece a la ciudadanía.	Con este objetivo estratégico se pretende sensibilizar a la ciudadanía en esta materia de cara al ejercicio de sus derechos, facilitándole de manera clara y accesible la información al respecto. Da cobertura a los siguientes PNR: N10, R2
OE10.- Mejorar los servicios a la ciudadanía optimizando la gestión de datos personales con pleno cumplimiento de la normativa.	Con este objetivo estratégico se pretende que la protección de datos no sea vista como un obstáculo sino como un habilitador para la mejora de los servicios, aumentando la eficiencia y efectividad de los procesos, reduciendo errores, fomentando la innovación al desarrollar soluciones novedosas y a facilitar la mejora continua y la adaptabilidad a los cambios. Da cobertura a las necesidades de protección de datos puestas de manifiesto durante la elaboración de la Estrategia para una Administración Pública Innovadora.

8. Líneas estratégicas y programas de actuación

8.1. Línea estratégica: Gobernanza de protección de datos y responsabilidad proactiva

8.1.1. Programa 1.1: Normativa y estructura organizativa de protección de datos

En la Junta de Andalucía es práctica habitual designar a personas para ejercer como DPD en el ámbito de las diversas Consejerías y entes instrumentales, si bien existe una amplia dispersión en las características de los puestos asociados a esta labor y en los perfiles de las personas que los ocupan. Asimismo existe dispersión de criterios y modelos de gestión de la protección de datos. Este programa pretende reestructurar la gestión de la protección de datos, definiendo una estructura organizativa adecuada, estableciendo los roles y perfiles de las diversas figuras implicadas en la protección de datos personales, y aprobando una normativa organizativa que proporcione confianza, fiabilidad y estabilidad al modelo definido.

Este programa contribuye a los objetivos estratégicos OE01, OE03 y OE06 y tiene los siguientes objetivos específicos:

1. Profundizar en el marco jurídico de actuación de los distintos sujetos que intervienen en el tratamiento de datos de carácter personal.
2. Garantizar la aplicación del principio de la protección de datos desde el diseño y por defecto en todas las fases y desde la creación de la norma.
3. Asegurar que las personas que ejercen como DPD tengan la relevancia necesaria en la organización y el perfil profesional adecuado.

Se han definido los siguientes indicadores de resultado:

1. % de responsables del tratamiento que aplican el principio de protección de datos desde el diseño y por defecto.
2. % de organismos que aplican los criterios establecidos en el modelo organizativo de protección de datos.
3. % de normas que pasan una revisión de protección de datos con carácter previo a su aprobación.

Este programa se desarrolla a través de los siguientes proyectos:

Proyecto	Descripción	Indicadores de realización
Realizar un análisis del grado de cooperación entre autoridad de control, CICRA, unidad de coordinación, personas DPD, responsables de tratamiento y responsables de seguridad TIC y elaborar un catálogo de deficiencias y acciones de mejora.	Reforzamiento de la cooperación entre todos los actores involucrados en la protección de datos: autoridad de control, Comisión Interdepartamental de Coordinación y Racionalización Administrativa, unidad de coordinación, personas DPD, personas responsables del tratamiento y personas responsables de seguridad TIC, así como con el futuro Centro de Inteligencia Artificial de Andalucía.	Número y desglose de las acciones de mejora identificadas en materia de cooperación entre autoridad de control, CICRA, unidad de coordinación, personas DPD, responsables de tratamiento y responsables de seguridad TIC.
Diseño de una estructura organizativa para la protección de datos que incluya la existencia de una coordinación nivel 30 con estructura de apoyo y unos criterios y procedimiento homogéneos de nombramiento de personas DPD.	Definir una estructura organizativa para la gestión de la protección de datos, incluyendo una coordinación de protección de datos con dedicación exclusiva y personal a cargo, una red de unidades de protección de datos en Consejerías y entidades instrumentales y la creación de plazas en RPT para las personas DPD, con dedicación exclusiva y/o equipos de apoyo cuando se requiera, y con la garantía de evitar conflictos de intereses cuando la dedicación no sea exclusiva.	Existencia de documento de propuesta de nueva estructura organizativa para la protección de datos (S/N). Existencia de coordinación de protección de datos nivel 30 con estructura de apoyo (S/N). Existencia de criterios y procedimiento homogéneos de nombramiento / cese motivado de personas DPD (S/N).
Diseño de un comité asesor en protección de datos para tecnologías disruptivas para la Junta de Andalucía.	Este comité tendrá funciones de evaluación tecnológica y actualización normativa continua, y permitirá articular la colaboración con Universidades y grupos de investigación, autoridades de control, etc. Facilitará el seguimiento de los cambios en las normativas nacionales e internacionales sobre protección de datos para adaptarlos rápidamente a las políticas internas. Este comité estará estrechamente relacionado con el grupo de trabajo creado por la CICRA para la colaboración de las personas DPD.	Existencia de documento de propuesta de diseño de comité asesor (S/N). Existencia de comité asesor (S/N).
Revisión de protección de datos en la elaboración normativa.	Modificación del proceso de elaboración normativa para garantizar que todas las normas sean revisadas desde el punto de vista de la protección de datos.	Inclusión en la MAIN del impacto de la protección de datos en la normativa (S/N)

Proyecto	Descripción	Indicadores de realización
Aprobación de un Decreto en materia de protección de datos.	Este Decreto establecerá la estructura organizativa para la coordinación de protección de datos, incluyendo un comité de protección de datos, las características de la unidad de coordinación, las unidades de protección de datos de Consejerías y entidades instrumentales, la necesidad de plazas en RPT para las personas DPD con dedicación exclusiva, los equipos de apoyo a las personas DPD, el comité asesor en protección de datos, ... Deberá tener una visión multidisciplinar, integrando la seguridad TIC e interior para proporcionar una protección integral.	Existencia de un Decreto en materia de protección de datos (S/N).

8.1.2. Programa 1.2: Procedimientos y guías

El modelo de protección de datos anterior al RGPD ponía el acento en el establecimiento de reglas y estándares mínimos en la gestión de la información y contemplaba vías de reparación a posteriori, por el contrario, bajo el enfoque proactivo se trata de prevenir y evitar por anticipado que aparezcan quiebras en la privacidad y el correspondiente daño para los afectados, en lugar de ofrecer únicamente mecanismos para la reparación de los perjuicios causados.

Se ha detectado que la implantación a coste cero de la normativa de protección de datos desde 2018 en la mayoría de los centros directivos ha ocasionado dificultades para garantizar su cumplimiento tanto para los centros directivos responsables de tratamiento como para la persona que ejerce como DPD. Con este programa se pretenden generar recursos a la organización que faciliten el cumplimiento de la normativa, así como el ejercicio de las funciones de DPD. Así, este programa responde a la necesidad de impulsar una labor más proactiva por parte de las personas responsables de los tratamientos mediante la creación de procedimientos de seguridad específicos, comunes y homogéneos, adicionales a los que proporciona la seguridad TIC e interior.

Mención especial merece la aplicación de medidas de detección y minimización de violaciones de seguridad de datos personales (brechas) y por otro lado establecer criterios comunes de gestión de las mismas y comunicación tanto a los responsables implicados en su resolución como, en su caso, a las personas interesadas y las autoridades de control.

Este programa contribuye a los objetivos estratégicos OE01, OE02, OE03, OE04, OE07 y OE08 y tiene los siguientes objetivos específicos:

1. Crear procedimientos de seguridad específicos de protección de datos de carácter personal.
2. Establecer criterios homogéneos de gestión y comunicación de las brechas de seguridad.
3. Aplicar medidas de detección y minimización de brechas de seguridad.
4. Desarrollar criterios homogéneos para la realización de análisis de riesgos y evaluaciones de impacto de los tratamientos de datos de carácter personal.

5. Establecer en los contratos, convenios u otros instrumentos las garantías adecuadas en materia de protección de datos.
6. Proporcionar recursos que mejoren el desempeño de la figura de DPD en la organización.
7. Producir criterios, guías de actuación, buenas prácticas, etc. que favorezcan la unificación de las actuaciones de los DPD.
8. Desarrollar contenidos que promuevan un mejor cumplimiento del derecho a la protección de datos de carácter personal.

Se han definido los siguientes indicadores de resultado:

1. % de organismos que aplican la política de protección de datos personales.
2. Nº de análisis de riesgos realizados en relación con el número de tratamientos.
3. Nº de evaluaciones de impacto realizados en relación con el número de tratamientos.
4. Nº de brechas de seguridad gestionadas con el procedimiento definido
5. % de responsables del tratamiento que utilizan el procedimiento de gestión de brechas definido.
6. N' de instrumentos jurídicos de encargo de tratamiento que usan las cláusulas tipo establecidas.

Este programa se desarrolla a través de los siguientes proyectos:

Proyecto	Descripción	Indicadores de realización
Elaboración de una política de protección de datos de la Junta de Andalucía.	Esta política realizará una definición clara de roles y responsabilidades (responsables, encargados, usuarios), directrices claras y uniformes para todo el personal (procedimientos estandarizados, …), establecerá los mecanismos de evaluación de riesgos y evidencia del cumplimiento, sistematizará el proceso de obtención de consentimiento, facilitará la realización de auditorías, ... Dado que en la Junta de Andalucía tiene competencias sectoriales que requieren políticas muy específicas de protección de datos, esta política establecerá las bases comunes y podrá ser completada o puntualizada por las políticas de protección de datos específicas de cada Consejería, para aquellas Consejerías que las necesiten.	Existencia de una política de protección de datos de la Junta de Andalucía (S/N).
Creación de un código de conducta en protección de datos para la Junta de Andalucía y sus entidades instrumentales.	Este código de conducta establecerá reglas específicas para contribuir a la correcta aplicación del RGPD y la LOPDGDD, en el ámbito de la Junta de Andalucía y sus entidades instrumentales.	Existencia de un código de conducta en protección de datos (S/N).
Elaboración de una metodología de análisis de riesgos y evaluaciones de impacto de protección de datos.	Esta metodología facilitará el cumplimiento, por parte de los responsables del tratamiento, de la obligación de realizar análisis de riesgos de protección de datos, así como evaluaciones de impacto en los tratamientos que las requieren.	Existencia de una metodología normalizada de análisis de riesgos y evaluaciones de impacto de protección de datos (S/N).

Proyecto	Descripción	Indicadores de realización
Revisión de las experiencias de uso de la metodología de análisis de riesgos y evaluaciones de impacto de protección de datos y elaboración de una nueva versión.	La experiencia de uso de las primeras versiones de las metodologías de análisis de riesgos y evaluación de impacto han puesto de manifiesto la existencia de aspectos mejorables para facilitar su aplicación a un conjunto más amplio de actividades de tratamiento, por lo que se ha incluido este proyecto para analizar en detalle esos aspectos mejorables y poder elaborar una nueva versión más completa de la metodología.	Existencia de una nueva versión de la metodología normalizada de análisis de riesgos y evaluaciones de impacto de protección de datos (S/N).
Elaborar un procedimiento integrado de gestión de incidentes de seguridad TIC y de violaciones de seguridad de datos personales (brechas).	Este proyecto agrupa a los cuatro proyectos preexistentes dedicados al diseño de un manual de gestión de brechas de datos personales con directrices comunes, a la definición del procedimiento de comunicación de brechas de seguridad a la autoridad de control, a la definición del procedimiento de comunicación de brechas de seguridad a las personas interesadas y a la coordinación en materia de gestión de incidentes de seguridad y brechas de seguridad de datos personales.	Existencia de un procedimiento integrado de gestión de incidentes de seguridad TIC y de violaciones de seguridad de datos personales (brechas) (S/N).
Revisión y actualización del clausulado de protección de datos en los modelos de pliegos y contratos.	La Junta de Andalucía dispone de modelos de pliegos para la licitación de contratos, publicados en https://juntadeandalucia.es/temas/contratacion-publica/gestion/comision-consultiva/paginas/pliegos.html. Estos modelos ya incorporan cláusulas relativas al tratamiento de datos personales y a los encargos de tratamiento, si bien resulta necesario revisar, actualizar y completar dichas cláusulas.	Número de modelos de pliegos y contratos revisados. Número de modelos de pliegos y contratos actualizados.
Creación de modelos de anexos de encargados de tratamiento para aquellos tipos de contratos, encargos, convenios, subvenciones u otros instrumentos que no lleven pliegos de cláusulas administrativas particulares.	Para aquellos instrumentos jurídicos de encargo de tratamiento que no tienen un pliego publicado entre los modelos de pliegos mencionados en el proyecto anterior, se hace necesario elaborar modelos de encargo de tratamiento adaptados específicamente a las necesidades de estos instrumentos.	Número de modelos de anexos de encargado de tratamiento creados.
Definición de directrices comunes y un procedimiento común para la elaboración, aprobación y publicación del RAT.	Con este proyecto se pretende homogeneizar la forma en que los responsables del tratamiento publican información en el RAT, para garantizar que la información proporcionada a la ciudadanía sea completa a la vez que sencilla de interpretar, y que la organización pueda hacer un uso eficaz del RAT para su gestión interna.	Existencia de guía de directrices comunes y procedimiento común para la publicación y aprobación del RAT (S/N).

Proyecto	Descripción	Indicadores de realización
Elaboración de otros procedimientos y guías de protección de datos.	Dado que las necesidades de elaboración de procedimientos y guías de protección de datos son muy amplias y cambiantes, y no resulta razonable hacer un desglose exhaustivo de todas ellas, se incluye este proyecto en cuyo marco se irán elaborando procedimientos y guías que no han sido priorizados en esta iteración, pero cuya prioridad puede aumentar durante la ejecución de la estrategia. Entre ellos pueden encontrarse los siguientes: - Procedimientos de seguridad específicos para la protección de datos con directrices comunes para la gestión de tratamientos en papel y automatizados - Guía para la protección de datos en actuaciones administrativas automatizadas. - Protocolo de actuación sobre la obligación de informar cuando los datos no se obtengan directamente del interesado. - Normativa de Protección de Datos en sistemas que usen IA: Crear una política de uso de servicios basados en IA, asegurando que los sistemas utilizados para entrenarse, aprender, almacenar o procesar datos personales cumplan con las medidas de seguridad y privacidad necesarias. - Guía de recomendaciones para la protección de datos desde el diseño y por defecto - Manual de buenas prácticas en materia de protección de datos - Normativa de Protección de Datos en la Nube: Crear una política de uso de servicios en la nube, asegurando que las plataformas externas utilizadas para almacenar o procesar datos personales cumplan con las medidas de seguridad y privacidad necesarias.	Número de procedimientos y guías específicos generados.

8.1.3. Programa 1.3: Mejora del registro de actividades de tratamiento (RAT) y su gestión

El registro de actividades de tratamiento es una de las herramientas que el RGPD exige a los responsables para demostrar la conformidad con el mismo, mediante el mantenimiento de un inventario de las actividades de tratamiento de datos que tienen bajo su responsabilidad y control, teniendo en cuenta la obligada colaboración con la Autoridad de Control que exige poner a su disposición dichos registros de operaciones de tratamiento para facilitar las actividades de supervisión realizadas en el ámbito de los poderes que el RGPD le otorga. Asimismo, se configura como una herramienta básica para proporcionar transparencia de cara a la ciudadanía y el ejercicio de sus derechos en esta materia. Con este programa se pretende mejorar la información del registro y facilitar su uso y su gestión a las personas responsables de los tratamientos.

Este programa contribuye a los objetivos estratégicos OE01, OE03 y OE09 y tiene los siguientes objetivos específicos:

1. Mejorar la gestión del registro de actividades de tratamiento.
2. Consolidar la información que los responsables de tratamiento necesitan gestionar en relación a sus actividades de tratamiento.
3. Mejorar la transparencia en materia de protección de datos.

Se han definido los siguientes indicadores de resultado:

1. % de centros directivos que publican sus tratamientos en el RAT.

Este programa se desarrolla a través de los siguientes proyectos:

Proyecto	Descripción	Indicadores de realización
Extensión de la información a registrar en el RAT.	Ampliar conceptualmente el RAT, incorporando información sobre los encargados de tratamiento y sus contratos, los sistemas de información en los que se gestiona la actividad de tratamiento, la realización de análisis de riesgos y evaluaciones de impacto de protección de datos, las brechas de seguridad, …	Número de datos publicados añadidos a la plantilla del RAT. Número de datos no publicados añadidos a la plantilla del RAT.
Adquisición/construcción de herramienta informática para la gestión automatizada del RAT y del riesgo.	La herramienta actual para la gestión del RAT no facilita su utilización para la gestión de la información ampliada objeto del proyecto anterior, ni para la gestión de los riesgos. Por tanto, se hace necesario dotar a la Junta de Andalucía de una nueva herramienta más potente y adecuada.	Existencia de una herramienta para RAT y gestión del riesgo (S/N).
Creación de un banco de tratamientos comunes para incorporar al RAT de cada organismo y/o consolidar como tratamientos horizontales / corporativos.	Existen diversas actividades de tratamiento que son comunes a la mayoría de organismos, como la gestión de eventos y la captura de imágenes, la vigilancia de edificios, el control horario, …. Mediante este proyecto se pretende homogeneizar la gestión y publicación en el RAT de estas actividades de tratamiento.	Nº tratamientos comunes definidos.

Proyecto	Descripción	Indicadores de realización
Enlazar el Registro de Actividades de Tratamiento con el Registro de Procedimientos y Servicios.	Incorporar relaciones entre el Registro de Actividades de Tratamiento y el Registro de Procedimientos y Servicios, para garantizar la trazabilidad entre cada procedimiento o servicio gestionado en la Junta de Andalucía y la actividad o las actividades de tratamiento que se realizan para tramitar ese procedimiento o proporcionar ese servicio.	Nº de procedimientos del RPS que incluyen información sobre las actividades de tratamiento asociadas.

8.2. Línea estratégica: Coordinación y apoyo a personas DPD y órganos directivos

8.2.1. Programa 2.1: Apoyo a personas DPD

A las personas Delegadas de Protección de Datos, cuya designación es obligatoria en la Administración, incumben funciones de asesoramiento a los responsables o encargados de los tratamientos, supervisar su adecuación a la legislación vigente y cooperar con la Autoridad de Control. Por otra parte, las personas DPD se relacionan con la ciudadanía en lo referente al ejercicio de sus derechos y con la Autoridad de Control. Con este programa se pretende facilitar a estas personas el ejercicio de sus funciones, proporcionándoles los recursos necesarios, fomentando la colaboración entre ellas, analizando sus cargas de trabajo, la necesidad de personal de apoyo específico y/o la dedicación exclusiva, dando a conocer esta figura en la organización, así como garantizando su publicidad en el portal de transparencia y la autoridad de control.

En el marco de la colaboración entre personas DPD, este programa contempla la creación de un grupo de trabajo sobre protección de datos donde se determinen modelos y criterios homogeneizados de aplicación en toda la Junta de Andalucía en temas de protección de datos y la articulación de un procedimiento que permita de forma eficaz la transferencia de conocimiento en el caso de sucesión en el cargo de DPD.

Este programa contribuye a los objetivos estratégicos OE01, OE06 y OE07 y tiene los siguientes objetivos específicos:

2. Definir el perfil profesional de la persona que ejerce como DPD y su posición dentro de la organización.
3. Difundir y publicitar la figura de DPD y sus funciones dentro de la organización y de cara a la ciudadanía.
4. Reforzar los mecanismos de colaboración entre las personas DPD.
5. Proporcionar asesoramiento y apoyo a las personas DPD.

Se han definido los siguientes indicadores de resultado:

1. % de DPD que responden al perfil profesional deseado.
2. % de DPD inscritos en el portal de transparencia.
3. % de DPD comunicados a la autoridad de control.

Este programa se desarrolla a través de los siguientes proyectos:

Proyecto	Descripción	Indicadores de realización
Mejorar los mecanismos de colaboración entre los DPD.	Este proyecto incluye la creación de un grupo de trabajo formado por todos los DPD, la gestión documental de la información relevante que debe estar a disposición de los DPD y la creación de un espacio en Red Profesional para los DPD, en el que se puedan abrir debates, complementario al espacio intranet de protección de datos. Asimismo incluye el establecimiento de un procedimiento de transferencia del conocimiento del DPD saliente al entrante.	Número de reuniones del grupo de trabajo de los DPD. Número y detalle de actuaciones de mejora de la colaboración realizadas.
Difusión de la figura del DPD.	Impulsar y supervisar el cumplimiento de la obligación de publicitar al DPD en el portal de transparencia e informar a la autoridad de control y al personal en el ámbito de actuación del DPD. Para ello se realizarán actuaciones de difusión de estas obligaciones, así como de campañas de supervisión y aviso a los organismos que no estén cumpliéndolas adecuadamente.	% de DPD publicados en el portal. % de DPD comunicados al CTPDA. % de DPD comunicados al personal en su ámbito de actuación.
Análisis del puesto DPD y sus competencias.	Este proyecto incluye la realización de análisis de cargas de trabajo de DPD, el estudio de las necesidades de personal de apoyo, así como el establecimiento del régimen de incompatibilidades y la clarificación de los casos en que se requiere dedicación exclusiva a esta función.	Existencia de una guía de definición del puesto DPD (S/N).
Creación de manual de bienvenida al nuevo DPD.	Este proyecto pretende agilizar la incorporación de nuevas personas al puesto de DPD, proporcionándoles la información necesaria para conocer sus funciones y los recursos que tienen a su disposición.	Existencia de un manual de bienvenida al nuevo DPD (S/N).
Asesoramiento Legal Permanente.	Contar con un equipo legal especializado en protección de datos que asesore en proyectos novedosos, transversales y/o que utilicen tecnologías disruptivas	Existencia de equipo de asesoramiento legal permanente (S/N).

8.2.2. Programa 2.2: Apoyo a responsables

Los responsables del tratamiento son una figura clave en la aplicación de la normativa de protección de datos, si bien resulta frecuente que consideren esta actividad como un esfuerzo añadido a sus labores principales de ejecución de políticas públicas. Este programa pretende facilitar su labor, impulsando que la protección de datos sirva de apoyo a la ejecución de las políticas públicas y los responsables la incorporen de manera natural en su actividad cotidiana.

Este programa contribuye a los objetivos estratégicos OE01, OE02, OE03 y OE05 y tiene los siguientes objetivos específicos:

1. Facilitar la localización y uso de la documentación, guías y plantillas relevantes para la aplicación de la normativa de protección de datos personales.
2. Impulsar la actualización y mantenimiento permanente del RAT así como de los análisis de riesgos y evaluaciones de impacto de protección de datos.
3. Proporcionar herramientas para gestionar y hacer seguimiento de las brechas de datos personales.
4. Garantizar que los responsables de tratamiento conozcan sus obligaciones en relación al tratamiento de datos personales así como los recursos de que disponen para ayudar al cumplimiento de las mismas.
5. Agilizar la respuesta a las solicitudes de ejercicio de derechos mediante su tramitación electrónica.

Se han definido los siguientes indicadores de resultado:

1. % de responsables del tratamiento que hacen uso de los recursos proporcionados en el marco de este programa.

Este programa se desarrolla a través de los siguientes proyectos:

Proyecto	Descripción	Indicadores de realización
Definición y automatización de procedimiento común para el ejercicio de los derechos de protección de datos por parte de la ciudadanía.	Se implantará un sistema de tramitación electrónica de los expedientes de ejercicio de derechos, que facilite el control de plazos, garantice la información al ciudadano, y permita la obtención de indicadores.	Nº de solicitudes de ejercicio de los derechos tramitadas telemáticamente.
Gestión documental vinculada a la responsabilidad proactiva.	Se incorporarán mecanismos de gestión documental que faciliten el acceso por parte de los responsables a los procedimientos y guías, a las plantillas de documentos, informes y fichas, a los informes de respuestas al ejercicio de derechos, criterios para la realización de cesiones de datos, etc.	Nº documentos compartidos.
Creación de un registro de brechas de datos de carácter personal.	Este registro, mantenido en un sistema de información, facilitará la gestión y el seguimiento de las violaciones de seguridad de datos personales, incluyendo la información a todos los participantes en su resolución así como la notificación a la autoridad de control.	Existencia de un registro de brechas de datos. Nº de brechas registradas.

Proyecto	Descripción	Indicadores de realización
Elaboración de una plantilla de libro blanco sobre protección de datos, para información y capacitación para personas titulares de centros directivos en esta materia.	Se trata de crear un proyecto específico orientado a los momentos en que se producen cambios de titulares de centros directivos (que son los responsables del tratamiento), ya sea de modo puntual o con un carácter más amplio. Mediante este proyecto se facilitará a las nuevas personas titulares de los cargos un "Libro Blanco sobre Protección de Datos", en donde se les informará -al poco de tomar posesión- sobre los tratamientos que son responsabilidad del centro directivo correspondiente y cuáles son las principales obligaciones del responsable de tratamiento, incorporando referencias a la normativa fundamental en la materia y a la organización de la Junta de Andalucía en esta materia. Asimismo se les informará sobre quién o quiénes son las personas DPD competentes, cuáles han sido las principales incidencias en relación con protección de datos en los distintos tratamientos, etc. Este libro blando tendrá el formato de un breve dossier que permitiera a la persona, por una parte, conocer la importancia del tema y por otra facilitar desde el principio su participación en las decisiones que pudieran afectar a los tratamientos del centro.	Nº de responsables del tratamiento a los que se les proporciona el libro blanco.
Campaña de revisión de los análisis de riesgos y evaluaciones de impacto de cada organismo en función de los criterios comunes definidos.	Se verificará la aplicación de los criterios comunes de análisis de riesgos y evaluaciones de impacto de protección de datos sobre una muestra de actividades de tratamiento. Para la realización de este proyecto se podrá contar con el apoyo de la Inspección General de Servicios.	Nº de AR y EI revisados.
Campaña de revisión del RAT de todos los organismos en base a los criterios comunes definidos.	Se verificará la aplicación de los criterios comunes de publicación en el Registro de Actividades de Tratamiento, sobre una muestra de centros directivos. Para la realización de este proyecto se podrá contar con el apoyo de la Inspección General de Servicios.	Nº de organismos que realizan la revisión del RAT.

8.2.3. Programa 2.3: Evaluación y auditoría

Este plan requiere la realización de múltiples cambios en la forma de trabajar de numerosos organismos y afecta a un número muy elevado de personas, por lo que resulta imprescindible verificar su cumplimiento y disponer de mecanismos de seguimiento pormenorizados. Asimismo, los responsables y encargados de los tratamientos deberán estar en condiciones de demostrar las medidas aplicadas mediante un sistema de métricas que permitan medir de manera homogénea el nivel de implantación de las mismas.

Este programa pretende dar respuesta a estas necesidades, incorporando medidas de evaluación y auditoría de cumplimiento, así como implantando un sistema pormenorizado de seguimiento de indicadores y un cuadro de mando que proporcione información a la dirección sobre la situación en materia de protección de datos personales.

Este programa contribuye a los objetivos estratégicos OE01, OE03, OE04 y OE10 y tiene los siguientes objetivos específicos:

1. Establecer un sistema de información a la dirección sobre la situación de cumplimiento de la normativa de protección de datos personales.
2. Supervisar el cumplimiento de las obligaciones de los responsables del tratamiento.
3. Verificar que los encargos de tratamiento de datos personales cumplen adecuadamente las instrucciones de los responsables.
4. Asegurar que la información publicada en el RAT es relevante y está actualizada.

Se han definido los siguientes indicadores de resultado:

1. % de incumplimientos detectados en evaluaciones y auditorías.
2. Nº de consultas al sistema de indicadores de protección de datos.

Este programa se desarrolla a través de los siguientes proyectos:

Proyecto	Descripción	Indicadores de realización
Impulsar y supervisar el cumplimiento de la obligación de publicar el RAT.	Se realizarán campañas de difusión de la obligación de publicar el RAT, entre los órganos directivos de la Junta de Andalucía y sus entidades instrumentales. Asimismo se realizarán campañas de supervisión y aviso a incumplidores.	Nº de órganos directivos que tienen información publicada en el RAT. Nº y detalle de actuaciones de impulso realizadas.

Proyecto	Descripción	Indicadores de realización
Revisión de los instrumentos jurídicos de encargo de tratamiento de los entes instrumentales que actúan como encargados de tratamiento sin disponer de un contrato o encargo de gestión específico.	En la Junta de Andalucía existen entes instrumentales que actúan como encargados del tratamiento por cuenta de otros organismos, sin que medie necesariamente un contrato ni un encargo de gestión. En estos casos el instrumento jurídico que da validez al encargo del tratamiento suelen ser los estatutos del ente, que le asignan determinadas funciones y competencias sin que las mismas incluyan la definición completa de los fines y medios del tratamiento. En este proyecto se revisarán de forma exhaustiva estas situaciones, se verificará si cumplen adecuadamente la normativa, y se propondrán las acciones de mejora que sean necesarias.	Nº de instrumentos jurídicos de encargo de tratamiento revisados.
Realización de auditorías periódicas de protección de datos.	Se realizarán, mediante muestreo, auditorías completas de cumplimiento de la normativa de protección de datos para determinadas actividades de tratamiento y/o determinados órganos directivos. Para la realización de este proyecto se podrá contar con el apoyo de la Inspección General de Servicios.	Nº de auditorías realizadas.
Revisión y Evaluación de Proveedores.	Se realizarán, mediante muestreo, auditorías y evaluaciones de los proveedores que manejen datos personales, asegurando que cumplan con los requisitos del RGPD y de la Junta de Andalucía. Para la realización de este proyecto se podrá contar con el apoyo de la Inspección General de Servicios.	Nº de auditorías y evaluaciones de proveedores realizadas.
Construir un sistema de indicadores de protección de datos.	Se definirán los indicadores de medición más relevantes para facilite la coordinación y el seguimiento del cumplimiento de la normativa de protección de datos.	Nº de indicadores definidos.
Implantación de una herramienta de seguimiento de indicadores y cuadro de mando de protección de datos.	Se implantará una herramienta que facilite el seguimiento pormenorizado y agregado de los indicadores establecidos en materia de protección de datos, incluyendo un cuadro de mando para proporcionar información a la dirección, a los responsables del tratamiento y a las personas DPD.	Existencia de herramienta de seguimiento de indicadores y cuadro de mando de protección de datos (S/N).

8.3. Línea estratégica: Capacitación, concienciación y sensibilización a personas empleadas públicas

8.3.1. Programa 3.1: Capacitación, concienciación y sensibilización a personas empleadas públicos

Con este programa se quiere conseguir aumentar el número de personas empleadas públicas formadas en materia de protección de datos, en especial aquellas implicadas en el ciclo de vida del dato de carácter personal.

A través de este programa se quiere introducir una cultura de protección de datos entre el personal empleado que presta sus servicios en la Junta de Andalucía para que incorpore hábitos de protección de datos personales en su trabajo diario principalmente entre las personas responsables y encargadas de los tratamientos, así como sensibilizar al personal directivo en la necesidad de cumplimiento de esta normativa y de destinar recursos humanos y materiales para este fin.

Este programa contribuye a los objetivos estratégicos OE03, OE07 y OE08 y tiene los siguientes objetivos específicos:

1. Fomentar una cultura de protección de datos.
2. Concienciar al personal alto cargo y al personal empleado público en general de la importancia de la protección de datos de carácter personal
3. Sensibilizar al personal directivo en la necesidad de cumplimiento de esta normativa y de destinar recursos humanos y materiales para este fin.
4. Garantizar la formación especializada y de reciclaje de la figura de DPD.
5. Formar al personal alto cargo y al personal empleado público en general en materia de protección de datos de carácter personal.

Se han definido los siguientes indicadores de resultado:

1. % de incremento del personal formado en protección de datos (desagregado por sexo y colectivo).
2. Número de reclamaciones a las autoridades de control en protección de datos (minimizar).
3. % de DPD con formación especializada.
4. % de incremento del personal sensibilizado (desagregado por sexo y colectivo).
5. Presupuesto destinado a la protección de datos.

Este programa se desarrolla a través de los siguientes proyectos:

Proyecto	Descripción	Indicadores de realización
Análisis de necesidades formativas y rediseño del plan de formación en protección de datos.	El plan de formación tendrá en cuenta las necesidades específicas de los responsables del tratamiento y de los DPD, así como las generales de todo el personal de la organización. Se buscará fomentar la participación en la formación, creando un sistema de incentivos que podría estar basado en la gamificación.	Existencia de plan de formación en protección de datos (S/N).

Proyecto	Descripción	Indicadores de realización
Intranet de protección de datos.	Creación de un espacio Intranet de protección de datos para compartir recursos con DPD, responsables del tratamiento y con todo el personal de la Junta de Andalucía.	Existencia de un espacio intranet de protección de datos (S/N).
Formación especializada para DPD.	Impartición de formación especializada para las personas DPD, con cursos y jornadas orientados específicamente a sus necesidades formativas.	Nº cursos realizados. Nº DPD formados anualmente.
Píldoras informativas para DPD.	Realización de píldoras informativas para DPD sobre temas de actualidad (tecnologías disruptivas, protección desde el diseño y por defecto, nuevas guías AEPD, etc.), con el fin de garantizar la actualización permanente.	Nº de píldoras informativas para DPD sobre temas de actualidad.
Intercambio de conocimientos con el CTPDA.	Establecimiento de un espacio de intercomunicación (jornadas, foros, etc.) con el CTPDA que favorezca la puesta en común de conocimientos que afectan al ejercicio de las funciones del DPD.	Número de sesiones de puesta en común con el CTPDA.
Formación para responsables de tratamiento y personal empleado público.	Ampliar la oferta formativa permanente, progresiva y especializada, dirigida a las personas responsables de los tratamientos y al personal empleado público en general	Nº de cursos anuales. Nº personas responsables de tratamiento formadas (desagregado por sexo y colectivo). Nº de personas empleadas públicas formadas (desagregado por sexo y colectivo).
Píldoras formativas para personal empleado público.	Crear píldoras formativas dirigidas a todos los sujetos implicados en el ciclo de vida del dato de carácter personal	Nº píldoras formativas creadas.
Plan de sensibilización.	Diseño de un plan de sensibilización para mejorar el cumplimiento normativo en protección de datos. Podrá incluir la publicación de boletines informativos periódicos, la realización de píldoras informativas y el uso de microlearning. Estará orientado tanto al personal empleado público como al personal directivo.	Existencia de un plan de sensibilización (S/N). Nº y detalle de actuaciones de sensibilización realizadas.
Protección de datos en los temarios de las oposiciones.	Refuerzo del peso de la materia de protección de datos en los temarios de las oposiciones para el ingreso a los distintos grupos de personal funcionario y en los contenidos de los cursos selectivos de acceso.	Nº temarios/cursos de acceso en los que se ha incluido o reforzado la materia de protección de datos.

8.4. Línea estratégica: Ciudadanía y privacidad

8.4.1. Programa 4.1: Ciudadanía y privacidad

La normativa de protección de datos permite que la ciudadanía pueda ejercer ante el responsable del tratamiento sus derechos de acceso, rectificación, oposición, supresión ("derecho al olvido"), limitación del tratamiento, portabilidad y a no ser objeto de decisiones individualizadas. Estas solicitudes deben ser gratuitas y respondidas en el plazo de un mes, aunque en función de su complejidad podrían prorrogarse otros dos meses más. En la actualidad no se dispone de mecanismos homogéneos y fiables de control sobre las solicitudes recibidas, ni sus respuestas ni plazos. Con este programa se pretende facilitar a la ciudadanía el ejercicio de sus derechos a través de un canal único y centralizado, que permita hacer seguimiento de los plazos y facilite a la organización el proceso de respuesta.

Asimismo, este programa pretende crear una cultura de protección de datos en la ciudadanía, con el fin de que ésta conozca de manera clara y sencilla quién trata sus datos personales y con qué finalidad en la Junta de Andalucía, así como de las vías para ejercer sus derechos en esta materia. De esta manera se quiere mejorar en transparencia y concienciar a la ciudadanía acerca de la importancia de salvaguardar su privacidad, de modo la persona administrada tenga confianza en que sus datos están protegidos y su privacidad garantizada, con especial hincapié en colectivos vulnerables en cuanto a protección de datos se refiere o en aquellos datos de especial protección.

Este programa contribuye a los objetivos estratégicos OE03, OE05, OE09 y OE10 y tiene los siguientes objetivos específicos:

1. Fomentar una cultura de protección de datos y salvaguardia de la privacidad en los datos personales de la ciudadanía.
2. Mejorar el proceso de atención al ejercicio de los derechos en materia de protección de datos.
3. Mejorar la transparencia en materia de protección de datos que se ofrece a la ciudadanía, proporcionando a los ciudadanos información clara y accesible sobre cómo se gestionan sus datos, facilitando la comprensión de sus derechos y la forma en que la Junta de Andalucía los protege.
4. Trasladar eficazmente a la ciudadanía las actuaciones que la Junta de Andalucía realiza para garantizar la protección de sus datos personales.

Se han definido los siguientes indicadores de resultado:

1. % solicitudes telemáticas de ejercicio de los derechos tramitadas en el plazo establecido.
2. Número de visualizaciones del área de protección de datos del portal de transparencia.
3. Número de personas impactadas por las campañas de concienciación y divulgación de protección de datos.
4. Número de sugerencias recibidas.

Este programa se desarrolla a través de los siguientes proyectos:

Proyecto	Descripción	Indicadores de realización
Implantar una sección de transparencia en protección de datos para la ciudadanía, en el portal corporativo.	Crear una sección en el portal corporativo de la Junta de Andalucía donde los ciudadanos puedan obtener información detallada sobre el tratamiento de sus datos personales. El portal incluirá:	Nº de recursos informativos creados en la sección de protección de datos del portal corporativo.

Proyecto	Descripción	Indicadores de realización
	- Información clara y accesible sobre las políticas de privacidad. - Preguntas frecuentes (FAQ) sobre protección de datos y derechos. - Instrucciones sobre cómo ejercer derechos como el acceso, rectificación, supresión y portabilidad de datos. Este proyecto está alineado con el proyecto "Explicar el tratamiento de datos personales" de la EAPI, cuyo objetivo es conseguir que las personas confíen plenamente en el tratamiento seguro y confidencial de sus datos personales.	
Mejorar la gestión de cookies en el portal web de la Junta de Andalucía.	Mejorar la accesibilidad y visibilidad de la política de privacidad y sobre el uso de cookies en el portal web de la Junta de Andalucía.	Verificación de que la política de privacidad y sobre el uso de cookies está visible y accesible para la ciudadanía (S/N).
Plataforma digital de trámites de protección de datos: Ventanilla electrónica de ejercicio de los derechos por parte de la ciudadanía.	Crear un sistema en línea, de ventanilla electrónica, para que los ciudadanos puedan ejercer sus derechos (acceso, rectificación, supresión, portabilidad, ...) a través de un formulario sencillo y accesible. El sistema generará un proceso automatizado para que el ciudadano reciba confirmación del estado de su solicitud.	Implantación en la ventanilla electrónica del procedimiento de ejercicio de los derechos (S/N).
Plataforma digital de trámites de protección de datos: Automatizar el ejercicio del derecho de acceso como servicio de respuesta inmediata.	Este proyecto pretende aprovechar las sinergias existentes entre el derecho de acceso a los datos personales y el derecho a la consulta de estado de los expedientes administrativos. Mediante este proyecto se pretende que la ciudadanía pueda consultar de manera inmediata sus datos personales, sin necesidad de tener que solicitarlos y esperar a que la administración los recopile y se los facilite. Para ello se hará uso de las funcionalidades de Carpeta Ciudadana, extendiéndolas en lo que sea necesario, así como del resto de plataformas y sistemas de consulta de estado y/o consulta de información.	Existencia del servicio de respuesta inmediata de ejercicio del derecho de acceso (S/N)

Proyecto	Descripción	Indicadores de realización
Plataforma digital de trámites de protección de datos: Gestión electrónica de consentimientos.	Adoptar plataformas que permitan gestionar electrónicamente los consentimientos de los ciudadanos para el tratamiento de sus datos. Esto incluye una herramienta en línea donde los ciudadanos puedan ver y gestionar sus consentimientos relacionados con el uso de sus datos. Esto permitirá: - Revocar consentimientos previamente otorgados. - Actualizar preferencias de comunicación. - Gestionar cómo la Junta y sus departamentos pueden utilizar sus datos personales. Este proyecto se encuentra incluido en la EAPI.	Nº de trámites cuyo consentimiento se gestiona a través de la plataforma digital de trámites de protección de datos.
Elaboración de un plan de información a la ciudadanía en materia de protección de datos.	Este plan de información contemplará un conjunto diverso de actuaciones orientadas a garantizar que la ciudadanía tenga toda la información que necesita en materia de protección de datos. Entre ellas pueden encontrarse: - Creación y divulgación de píldoras informativas orientadas a la ciudadanía - Boletines Informativos de Protección de Datos: Enviar boletines periódicos por correo electrónico o SMS informando a los ciudadanos de cambios importantes en la política de protección de datos, actualizaciones sobre nuevas normativas y cómo la Junta está protegiendo su información personal. - Guías Prácticas sobre Protección de Datos: Desarrollar y distribuir guías digitales y físicas que expliquen de manera sencilla los derechos de protección de datos de los ciudadanos y cómo ejercitarlos. - Webinars y sesiones Informativas para Ciudadanos: Organizar webinars regulares donde expertos en protección de datos expliquen a la ciudadanía conceptos clave como la privacidad en línea, cómo identificar prácticas fraudulentas (phishing) y cómo proteger su información personal en entornos digitales. Este proyecto se encuentra incluido en la EAPI.	Plan de información a la ciudadanía elaborado (S/N). Nº de actuaciones de información a la ciudadanía realizadas.

Proyecto	Descripción	Indicadores de realización
Campaña de Sensibilización "Tus Datos, Tu Derecho".	Lanzar una campaña de sensibilización pública, tanto en medios digitales como tradicionales (televisión, radio, redes sociales), que eduque a los ciudadanos sobre la importancia de la protección de datos y cómo pueden ejercer sus derechos. Esta campaña puede incluir mensajes como: ¿Qué son los datos personales? Cómo mantener tus datos seguros. Tus derechos según la normativa de protección de datos (RGPD).	Campaña de sensibilización realizada (S/N).
Chatbot de Consulta de Privacidad.	Implementar un asistente virtual o chatbot en el sitio web de la Junta que permita a los ciudadanos hacer preguntas sobre protección de datos y recibir respuestas rápidas sobre cómo se manejan sus datos o cómo ejercer sus derechos.	Existencia de asistente virtual de protección de datos (S/N).
Colaboración con Centros Educativos.	Incluir módulos de concienciación sobre la protección de datos en el currículum educativo de escuelas y universidades. Colaborar con centros de educación para desarrollar contenido pedagógico que fomente desde una edad temprana la importancia de la privacidad y el manejo seguro de la información personal.	Incorporación de módulos de concienciación sobre protección de datos en el curriculum educativo (S/N).
Encuestas Periódicas sobre Protección de Datos.	Enviar encuestas periódicas a los ciudadanos para recabar su opinión sobre cómo la Junta de Andalucía está gestionando sus datos y si perciben mejoras o preocupaciones en la protección de su información. Los resultados se utilizarán para mejorar continuamente las políticas de protección de datos.	Nº de personas encuestadas.
Entorno de Innovación Ciudadana en Protección de Datos.	Establecer un entorno donde los ciudadanos puedan proponer ideas o mejoras para la protección de datos. Las mejores sugerencias podrían ser implementadas por la Junta, fomentando una mayor participación activa en la creación de un entorno de datos más seguro.	Entorno de innovación ciudadana implantado (S/N)

8.5. Línea estratégica: Innovación

8.5.1. Programa 5.1: Innovación en la protección de datos

Este programa pretende aprovechar las capacidades del ecosistema y las nuevas tecnologías para mejorar la protección de datos personales mediante la realización de proyectos altamente innovadores, entendiendo la innovación como la creación de valor público resolviendo problemas de formas novedosas.

Este programa contribuye a los objetivos estratégicos OE01, OE03, OE10 y OE11 y tiene los siguientes objetivos específicos:

1. Impulsar la utilización de tecnologías emergentes para la mejora de la protección de datos.
2. Aumentar el conocimiento de la organización sobre los riesgos de protección de datos a los que está expuesta.
3. Aumentar la capacidad de las personas de gestionar los datos que la Junta de Andalucía tiene sobre ellas.
4. Mejorar los servicios a la ciudadanía optimizando la gestión de datos personales con pleno cumplimiento de la normativa.

Se han definido los siguientes indicadores de resultado:

1. Número de proyectos identificados para la mejora de la protección de datos haciendo uso de tecnologías emergentes.
2. Número de tratamientos incluidos en el mapa de riesgos.
3. Número de actuaciones de mejora realizadas con éxito en el marco de los proyectos de este programa.
4. Número de servicios que hacen uso del mecanismo de gestión de datos de la ciudadanía.

Este programa se desarrolla a través de los siguientes proyectos:

Proyecto	Descripción	Indicadores de realización
Análisis de Nuevas Tecnologías de Protección de Datos.	Investigar tecnologías emergentes como inteligencia artificial, blockchain o técnicas de anonimización y seudonimización de datos para mejorar la protección de la información. Este proyecto se desarrollará a través de grupos de trabajo.	Existencia de informe sobre la adopción de tecnologías emergentes para mejorar la protección de la información (S/N).
Mapa de riesgos de protección de datos en la Junta de Andalucía.	Elaboración de un mapa de riesgos de protección de datos en la Junta de Andalucía, que identifique los procesos más críticos y las áreas de vulnerabilidad en el manejo de datos.	Número de riesgos incluidos en el mapa de riesgos.

Proyecto	Descripción	Indicadores de realización
Entornos seguros para iniciativas de mejora.	Analizar la viabilidad de establecer entornos seguros en los que los equipos que trabajan en iniciativas de mejora puedan acceder a datos personales de manera controlada, y los cambios a realizar en los registros de actividades de tratamiento y en los análisis de riesgos y evaluaciones de impacto de protección de datos para permitirlo. Este proyecto se encuentra incluido en la EAPI.	Número de iniciativas de mejora que hacen uso de entornos seguros de acceso a datos personales.
Analizar las actuaciones a realizar con relación a la protección de datos personales para mejorar los servicios a la ciudadanía compartiendo datos entre administraciones.	Analizar los cambios a realizar en los registros de actividades de tratamiento y en los análisis de riesgos y evaluaciones de impacto de protección de datos para facilitar la compartición de datos con otras administraciones, en la medida en que sea idóneo, necesario y proporcional. Este proyecto se encuentra incluido en la EAPI.	Número de actuaciones identificadas.
Gestión de datos de la ciudadanía.	Crear un mecanismo eficiente de gestión de datos de la ciudadanía, incluyendo sus datos de contacto, su situación, necesidades e intereses, y los servicios proactivos y avisos personalizados que desea recibir, todo ello con pleno cumplimiento de la normativa de protección de datos personales. Este proyecto se encuentra incluido en la EAPI.	Número de conjuntos de datos incorporados y/o integrados con el mecanismo de gestión de datos de la ciudadanía.
ENS y protección de datos personales.	Analizar las mejoras a realizar en organización y procedimientos para facilitar el cumplimiento conjunto de la normativa de protección de datos y el Esquema Nacional de Seguridad.	Número de mejoras identificadas.

9. Seguimiento y evaluación

El seguimiento y evaluación del plan ha de ser coherente con el modelo de Gobernanza empleado para la redacción del mismo, manteniendo los mecanismos de colaboración con aquellos agentes, cuyo compromiso y participación es necesario para garantizar su adecuado cumplimiento.

Los mecanismos para su gestión, en cuanto a coordinación, seguimiento, revisión y evaluación, estarán sujetos a su posible adaptación a las circunstancias, que pueden ser cambiantes a lo largo de su desarrollo, dado que tiene un horizonte amplio que alcanza hasta el año 2030. Asimismo, tal como se expone a lo largo de la misma, habrá medidas cuyo sistema de seguimiento se establecerá de origen y otras, cuyo sistema de indicadores de seguimiento, se irá construyendo conforme se van ejecutando otras medidas relacionadas.

Mediante este seguimiento y evaluación se podrá comprobar el desarrollo de los programas y medidas previstas, e intervenir mediante su revisión siempre que sea necesario para conseguir los objetivos establecidos. Para facilitar esta labor, se han previsto una serie de herramientas y mecanismos que han de permitir conocer periódicamente su nivel de ejecución, a fin de detectar, con antelación suficiente, posibles desviaciones y poder determinar medidas alternativas para superarlas.

Con las finalidades indicadas, se diseñará un panel de indicadores capaces de ofrecer información homogénea, detallada, pero también integrada y sintética sobre la situación de los programas y el nivel de consecución de los objetivos.

La información de seguimiento será mantenida y revisada de forma permanente por los órganos designados a tal fin, con la participación de los distintos centros directivos que están involucrados en la Estrategia. Esta información será compartida, en aras de garantizar la transparencia y promover la participación.

Asimismo, se creará una Comisión de Seguimiento, formada por una Oficina Técnica de Evaluación y Seguimiento, que se encargará de supervisar su correcto desarrollo, de medir la realización y resultados de los programas y medidas, así como de proponer las modificaciones o reprogramaciones que se estimen oportunas y por un Órgano de Dirección, que será responsable de la toma de decisiones que impliquen modificaciones o reprogramaciones, en base a las propuestas realizadas por la Oficina Técnica.

9.1. Comisión de seguimiento

Para llevar a cabo estas tareas, se constituirán dos órganos:

1. Una Oficina Técnica de Evaluación y Seguimiento que será la encargada de supervisar el correcto desarrollo del plan, para ello diseñará e implementará los mecanismos oportunos que aseguren la disponibilidad de los datos, para que se pueda medir la realización y resultados de los programas y medidas.

   Dicha Oficina estará compuesta por personal al servicio de la Secretaría General para la Administración Pública, dando continuidad a los trabajos realizados por la Oficina Técnica de elaboración del plan, tal como se indica en el modelo de Gobernanza.

   En concreto, serán funciones de la Oficina Técnica de Evaluación y Seguimiento las siguientes:

   - Diseñar las herramientas necesarias para la recogida de la información. Como mínimo, se tiene prevista la creación de un cuadro de mandos que permita recogerla de forma automatizada, a través de los indicadores establecidos.

- Establecer un sistema y calendario para la recogida sistemática de la información.
- Recopilación, tratamiento y análisis de la información relativa al sistema de indicadores.
- Realización de memorias anuales de seguimiento del plan, así como de las evaluaciones intermedias y la evaluación final.
- A partir de lo anterior, y dentro del proceso de mejora continua del mismo, elaboración de las propuestas de modificación de los programas y medidas a desarrollar que se consideren necesarios, de acuerdo con los Centros Directivos responsables, o a propuesta de las diferentes Consejerías.
- Proponer las modificaciones o reprogramaciones, que se estimen oportunas, al Órgano de Dirección.

2. Un Órgano de Dirección de la Evaluación y Seguimiento, que se reunirá con carácter anual y donde se tomarán las decisiones que impliquen modificaciones o reprogramaciones en el plan, en base a las propuestas de la Oficina Técnica de Evaluación y Seguimiento. Este Órgano será la CICRA como evolución del Comité Directivo que se detalla en el sistema de Gobernanza.

   Serán funciones de este Órgano:

   - Análisis y valoración de las memorias anuales, así como de las evaluaciones intermedia y final.
   - Modificación y reprogramación, en caso necesario, de los objetivos, programas y medidas del plan, a partir de las propuestas elevadas por la Oficina Técnica de Evaluación y Seguimiento.
   - Valorar y aprobar, si se estima oportuno, las propuestas realizadas la Oficina Técnica de Evaluación y Seguimiento, así como determinar las actuaciones que deban adoptarse para evitar desviaciones de los objetivos perseguidos.
   - Coordinación, en su caso, con otros organismos públicos, así como con las empresas y asociaciones sectoriales, en la ejecución del plan.

9.2. Periodicidad del Seguimiento y la Evaluación

El Seguimiento y Evaluación del plan se realizará durante su ejecución y a la finalización del mismo, con los siguientes informes:

- **Evaluación ex ante**. Este plan se someterá a una evaluación ex ante con la participación de un grupo de personas expertas en el ámbito de la protección de datos que se referenciarán en el Anexo correspondiente. Las principales aportaciones realizadas por las personas expertas se incorporarán en el presente documento.
- **Informes de seguimiento anual**. Cada año se elaborará un informe de seguimiento referido al año anterior, en el que se presentará de forma clara y concisa el grado de avance en las medidas y programas de actuación, así como la evolución de los indicadores correspondientes. Se identificarán los problemas y condicionantes surgidos, identificando las causas que los provocan, sus consecuencias y las soluciones propuestas para resolverlos.

Con esta información se persigue analizar el grado de consecución del plan y sus logros parciales. Tras la revisión de los informes de seguimiento anuales, y previo acuerdo del Órgano de Dirección, podrán derivarse modificaciones, que deberán quedar debidamente formalizadas.

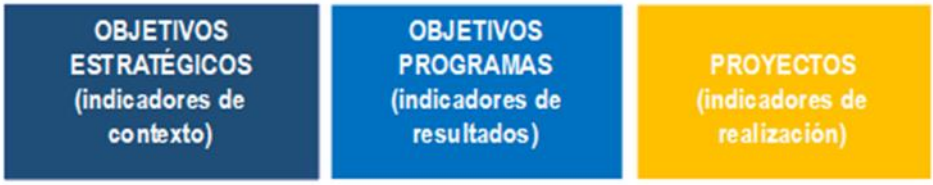
- **Evaluación intermedia**. Referida a la finalización del año 2027, en esta evaluación se analizará el diseño, la implementación y los resultados hasta ese momento, y con ella se perseguirán los siguientes propósitos:
    - Analizar el grado de avance de la ejecución, así como la forma en la que las actuaciones se han ajustado a lo programado.
    - Valorar el progreso en la consecución de los objetivos fijados, mediante la valoración de la evolución de los principales indicadores, estudiándose las causas de los niveles alcanzados.
    - Analizar los cambios en el marco normativo y estratégico, y reajustar las líneas, objetivos y programas para hacerlos coherentes.
    - Proponer cambios en los programas, para ajustarlos a los recursos disponibles, mejorar los resultados y alcanzar los objetivos establecidos para el 2030.
    - En línea con lo anterior, y en caso de existir una desviación importante respecto de los objetivos marcados, se analizará y propondrá un plan de medidas correctoras, cuya aplicación se consensuará con los agentes involucrados.
- **Evaluación final**. Referida al periodo completo de ejecución del plan, hasta el ejercicio 2030; en esta evaluación se valorarán los resultados generados y se determinará si los programas y medidas aplicadas han sido útiles y eficaces contribuyendo a alcanzar los objetivos perseguidos. Esta evaluación actualizará los resultados obtenidos en la evaluación intermedia, siendo su propósito obtener conclusiones para formular el siguiente plan. Se requerirá disponer de los datos necesarios para establecer los valores finales de los indicadores.

9.3. Sistema de Indicadores

Constituyen la principal fuente de información en el seguimiento y evaluación del plan, estos indicadores se estructuran en tres niveles:

- Los indicadores de impacto o de contexto están asociados a los Objetivos Estratégicos, se miden al inicio y se establecen metas a alcanzar a la finalización del plan. En aquellas medidas que se establezcan a más largo plazo se construirán y/o medirán en las sucesivas iteraciones del mismo.
- Los indicadores de resultados están asociados a los Programas, al igual que los anteriores se miden al inicio del plan, siempre que sea posible, o en las sucesivas iteraciones.
- Los indicadores de realización miden la ejecución de los proyectos o medidas, incluidos en cada Programa.

Los indicadores que se han podido recopilar en el análisis de la situación inicial, sirven de medida como punto de partida. En los casos viables se han propuesto metas, en otros se establecerán en las sucesivas iteraciones del plan, ya que se ha considerado más realista establecerlas al inicio de cada proyecto, momento en el que se va a tener un conocimiento más específico que permita definir cada meta. Todos aquellos indicadores que hagan referencia a personas están debidamente desagregados por sexo.



42. Sistema de indicadores del plan (Fuente: Elaboración propia)

Anexo I. Actualización del plan realizada en esta iteración

Como consecuencia del avance en los trabajos, de la elaboración de la Estrategia para una Administración Pública Innovadora 2023-2030, y de la propia evolución de los servicios, la normativa y la actuación de las autoridades de control, se ha hecho necesario realizar una actualización del plan, ajustando los objetivos, líneas, programas y proyectos a las necesidades y situación actuales.

La Estrategia para una Administración Pública Innovadora proporciona un impulso innovador también a este plan, entendiendo la innovación como la creación de valor público resolviendo problemas de formas novedosas. Por este motivo se ha considerado necesario añadir un nuevo objetivo: "**Mejorar los servicios a la ciudadanía optimizando la gestión de datos personales con pleno cumplimiento de la normativa**". De este modo el plan no solo estará orientado al cumplimiento normativo, que es esencial, sino que también irá orientado a que la protección de datos no sea vista como un obstáculo sino como un habilitador para la mejora de los servicios, aumentando la eficiencia y efectividad de los procesos, reduciendo errores, fomentando la innovación al desarrollar soluciones novedosas y a facilitar la mejora continua y la adaptabilidad a los cambios.

Asimismo, el nuevo enfoque requiere incorporar nuevos proyectos a este plan. Teniendo en cuenta que originalmente tenía 63 proyectos, y a fin de facilitar su seguimiento y evaluación, se hace necesario agrupar y simplificar algunos de los proyectos preexistentes, evitando que el número total de proyectos aumente a la vez que se mantiene lo necesario para lograr sus objetivos. Este esfuerzo simplificador se traslada también a los 16 programas que tenía el plan originalmente, y como consecuencia se ha hecho necesario reenfocar también las líneas estratégicas que agrupan los programas.

La línea de responsabilidad proactiva, que contaba con 6 programas, cambia su denominación a "Gobernanza de protección de datos y responsabilidad proactiva" y se simplifica reagrupando sus proyectos en 3 programas:

- Normativa y estructura organizativa de protección de datos. Este programa agrupa todos los proyectos preexistentes relacionados con la creación y modificación de órganos y puestos en RPT, así como con la colaboración entre los diversos órganos, junto con las modificaciones normativas requeridas para realizar esos cambios. Además, los 11 proyectos preexistentes en esta materia se reagrupan en 5 proyectos que dan cobertura conjuntamente a los objetivos de los 11 anteriores.
- Procedimientos y guías. Este programa recoge los 17 proyectos preexistentes relacionados con la elaboración de procedimientos, guías, manuales, documentos tipo, y en general cualquier documento cuya finalidad sea ser utilizado como referencia o plantilla por las personas implicadas en el tratamiento de datos personales, ya sean responsables del tratamiento, DPD, unidades de seguridad TIC o personas empleadas públicas. Entre ellos se incluye la creación de una política de seguridad y de un código de conducta en materia de protección de datos. Los 17 proyectos se han reagrupado y simplificado en 9 proyectos, que ponen el foco en los aspectos prioritarios sin reducir su alcance conjunto.

- Mejora del registro de actividades de tratamiento (RAT) y su gestión. Este programa se mantiene para destacar algunos cambios que es necesario realizar en este registro y que son imprescindibles para una adecuada gobernanza de la protección de datos. No obstante, la mayoría de los proyectos de este programa se han trasladado a los programas de procedimientos y guías, normativa y estructura organizativa, evaluación y auditoría, y apoyo a responsables. Como consecuencia, este programa pasa a tener 3 proyectos, todos ellos de alta importancia estratégica.

La línea "la figura de DPD" contaba con 6 programas. De entre ellos, el programa dedicado a la formación se traslada a la línea de capacitación y concienciación, para dar una visión conjunta a todas las actividades relacionadas con la capacitación, concienciación y sensibilización de todo el personal empleado público. Los proyectos del programa de creación normativa se trasladan a la línea de gobernanza de protección de datos y responsabilidad proactiva, al igual que todos los proyectos relacionados con la cooperación entre órganos y con la elaboración de material de apoyo a la labor de estas personas. Como consecuencia, esta línea se condensa en un único programa, denominado "Apoyo a personas DPD", con 5 proyectos relacionados con la colaboración entre personas DPD, la visibilidad de esta figura en la organización, el análisis de los puestos que desempeñan y deben desempeñar y el asesoramiento legal a las personas que realizan esta importante función.

Por analogía con este programa, se crea un programa de "Apoyo a responsables", con los proyectos cuya utilidad principal es ayudar a las personas responsables del tratamiento a realizar sus funciones. En este programa se incluyen proyectos de implantación de herramientas para el desarrollo de sus funciones (gestión electrónica de los procedimientos de ejercicio de derechos y registro de violaciones de seguridad), así como actuaciones de apoyo al cumplimiento de sus obligaciones.

Los proyectos relacionados con la verificación del cumplimiento de la normativa se han agrupado en un nuevo programa denominado "Evaluación y auditoría". A ellos se han añadido un proyecto de realización de auditorías periódicas de protección de datos y uno de revisión y evaluación de encargados de tratamiento.

Estos tres programas (apoyo a DPD, apoyo a responsables, evaluación y auditoría) se han agrupado en una nueva línea estratégica denominada "Coordinación y apoyo a DPD y órganos directivos".

La línea "Capacitación y concienciación" se mantiene, aunque se amplía su denominación a "Coordinación, concienciación y sensibilización a personas empleadas públicas", para resaltar que incluye actuaciones de sensibilización y que va dirigida a todos los colectivos de personas empleadas públicas, pero no a la ciudadanía. En esta línea, que tiene un único programa, se han reagrupado los proyectos preexistentes en la materia, y se ha añadido un nuevo proyecto orientado a realizar un análisis con visión de conjunto de toda la formación en materia de protección de datos orientado a la elaboración de un plan de formación en esta materia.

La línea "Ciudadanía y privacidad" se mantiene con un único programa, pero aumenta su importancia con la incorporación de nuevos proyectos con un enfoque claramente innovador.

Finalmente, se ha incorporado una nueva línea de “Innovación”, con un único programa denominado “Innovación en la protección de datos”, que incluye proyectos altamente innovadores. Entre ellos destaca el análisis de cómo pueden ayudar las tecnologías emergentes a la protección de datos, la elaboración de un mapa de riesgos de protección de datos que cubra a toda la Junta de Andalucía, y proyectos orientados a facilitar, en la medida de lo posible, el intercambio de datos entre administraciones, el establecimiento de entornos seguros para que los equipos que trabajan en iniciativas de mejora puedan acceder a datos personales de manera controlada, y el cumplimiento conjunto de la normativa de protección de datos y el Esquema Nacional de Seguridad.

Anexo II. Seguimiento de la ejecución

Se detallan a continuación los proyectos en los que se han realizado avances relevantes hasta la finalización del tercer trimestre de 2024, detallando los indicadores de resultados y de realización asociados. No se incluyen los indicadores de contexto, entendiendo que el periodo transcurrido no es suficiente para haber logrado cambios relevantes en estos indicadores.

La información de este anexo está organizada según las líneas estratégicas, programas y proyectos que se definieron en el plan original.

II.1. Línea estratégica de responsabilidad proactiva

Esta línea abarca los siguientes 6 programas:

- P01. Programa de prevención para una protección más eficaz
- P02. Programa de mejora de la gestión de brechas de seguridad
- P03. Programa de fomento de la protección de datos desde el diseño y por defecto
- P04. Programa de revisión de clausulado
- P05. Programa de mejora del Registro de Actividades de Tratamiento y su gestión
- P06. Programa de mejora de la gestión del ejercicio de los derechos en materia de protección de datos

En el marco del programa P01, de prevención para una protección más eficaz, se han completado los proyectos 02 (Procedimiento normalizado de análisis de riesgos), 03 (Procedimiento normalizado de evaluaciones de impacto) y 05 (Creación de una guía práctica con recomendaciones para tratamientos en papel). Con base a los nuevos procedimientos se han realizado al menos 41 análisis de riesgos y 10 evaluaciones de impacto de protección de datos. En cuanto a indicadores destacan los siguientes:

- Indicadores de resultado:
    - Nº de análisis de riesgos realizados en relación con el número de tratamientos: Más de 41 análisis de riesgos realizados.
    - Nº de evaluaciones de impacto realizados en relación con el número de tratamientos: Más de 10 evaluaciones de impacto realizadas.
- Indicadores de realización:
    - Existencia de un procedimiento normalizado AR (S/N): S
    - Existencia de un procedimiento normalizado EI (S/N): S
    - Nº de recomendaciones para tratamientos en papel: 1 (infografía 10/2024: Tratamiento de datos en papel Junta de Andalucía)

En el marco del programa P02, de mejora de la gestión de brechas de seguridad, se han completado los proyectos 01 (Diseño de manual de gestión de brechas de datos personales con directrices comunes), 02 (Definición de procedimiento de comunicación de brechas de seguridad a la autoridad de control), 03 (Definición de procedimiento de comunicación de brechas de seguridad a las personas interesadas) y 04 (Actuación coordinada en materia de gestión de incidentes de seguridad y brechas de seguridad de datos personales), dado que se ha elaborado un procedimiento integrado para la gestión de incidentes de seguridad y brechas de datos personales que incluye la comunicación a la autoridad de control y a las personas interesadas, que se pretende potenciar mediante su aprobación formal como instrucción. En cuanto a indicadores destacan los siguientes:

- Indicadores de resultado:
    - Nº de criterios y/o procedimientos comunes implantados: 1
- Indicadores de realización:
    - Existencia de un manual de gestión de brechas de seguridad (S/N): S
    - Existencia de un procedimiento común de comunicación de brechas de seguridad a la autoridad de control (S/N): S
    - Existencia de un procedimiento común de comunicación de brechas de seguridad a las personas interesadas (S/N): S
    - Existencia de un procedimiento común de comunicación de brechas de seguridad a los agentes implicados (S/N): S

En el marco del programa P03, de fomento de la protección de datos desde el diseño y por defecto, se ha completado el proyecto 02 (Inclusión de una revisión desde el punto de vista de la protección de datos en el ciclo de aprobación de la normativa), dado que se ha incluido un completo apartado de protección de datos en la memoria de análisis de impacto normativo (MAIN), cuyo uso obligatorio se aprobó mediante el Decreto-ley 3/2024, de 6 de febrero, por el que se adoptan medidas de simplificación y racionalización administrativa para la mejora de las relaciones de los ciudadanos con la Administración de la Junta de Andalucía y el impulso de la actividad económica en Andalucía. En cuanto a indicadores destacan los siguientes:

- Indicadores de realización:
    - Inclusión en la MAIN del impacto de la protección de datos en la normativa (S/N): S

En el marco del programa P04, de revisión de clausulado, se han iniciado la ejecución del proyecto 02 (Creación de anexos de contratación para aquellos tipos de contratos, encargos, convenios u otros instrumentos que no lleven pliegos de cláusulas administrativas particulares, p.e. encargos de ejecución, menores, convenios, etc.), dado que se han elaborado las recomendaciones para contratos menores, estando pendiente las recomendaciones para el resto de instrumentos (aunque las de contratos pueden servir de referencia). En cuanto a indicadores destacan los siguientes:

- Indicadores de realización:
    - Nº de anexos creados: 1

En el marco del programa P05, de mejora del Registro de Actividades de Tratamiento y su gestión, se ha completado el proyecto 01 (Definición de directrices comunes para la elaboración del RAT), dado que se ha elaborado una guía de directrices y se ha dado difusión entre las personas DPD. Asimismo, se está trabajando en el proyecto P05 (Realización de campañas de difusión de la obligación de publicar el RAT), dado que se han realizado varios recordatorios de la obligación de actualizar el RAT. En cuanto a indicadores destacan los siguientes:

- Indicadores de resultado:
    - % centros que publican sus tratamientos en el portal de transparencia: 100% considerando Consejerías, Agencias Administrativas, Agencias de Régimen Especial y Agencias Públicas Empresariales. Más del 77% considerando también las fundaciones y sociedades mercantiles.
        - Nota: todas las Consejerías (14), Agencias Administrativas (11), Agencias de Régimen Especial (3) y Agencias Públicas Empresariales (14) tienen actividades de tratamiento registradas en el RAT corporativo de la Junta de Andalucía. De las 17 fundaciones y 16 sociedades mercantiles, al menos 10 fundaciones y 6 sociedades mercantiles tienen actividades registradas en el RAT corporativo (el resto pueden publicarlo por otros medios).
- Indicadores de realización:
    - Existencia de guía con directrices comunes (S/N): S

Resulta interesante resaltar que desde el 1 de octubre de 2023 al 30 de septiembre de 2024 se han actualizado 960 actividades de tratamiento en el RAT corporativo.

En el marco del programa P06, de mejora de la gestión del ejercicio de los derechos en materia de protección de datos, se han hecho avances muy relevantes en los proyectos 01 (Ventanilla electrónica para el ejercicio de los derechos por parte de la ciudadanía) y 02 (Definición y automatización de procedimiento común para el ejercicio de los derechos de protección de datos por parte de la ciudadanía), dado que ya se encuentran implantados en entorno de pruebas tanto el formulario de solicitud de ejercicio de derechos en VEAJA (Ventanilla Electrónica de la Administración de la Junta de Andalucía) como el sistema de tramitación electrónica de estas solicitudes.

II.2. Línea estratégica de la figura del DPD

Esta línea abarca los siguientes programas:

- P07. Programa de sensibilización acerca de la figura de DPD en la organización
- P08. Programa de homogeneización de la figura de DPD en la organización
- P09. Programa de refuerzo de la figura de DPD en la organización
- P10. Programa de formación especializada para DPD
- P11. Programa de creación normativa
- P12. Programa de creación de recursos para facilitar la labor del DPD

En el marco del programa P07, de sensibilización acerca de la figura de DPD en la organización, se han realizado avances muy relevantes en los proyectos 01 (Realización de campañas de difusión de la obligación de publicitar al DPD en el portal de transparencia y al resto de la organización) y 02 (Realización de campañas de difusión de la obligación de comunicar el nombramiento de DPD a la autoridad de control), dado que cada vez que se ha detectado que algún organismo no tenía publicado su DPD se le ha pedido que lo haga y se ha confirmado que lo ha hecho, y también se ha confirmado que han comunicado la designación al CTPDA. En cuanto a indicadores destacan los siguientes:

- Indicadores de resultado:
    - %DPD inscritos en el portal de transparencia: 95% (considerando Consejerías, Agencias Administrativas, Agencias de Régimen Especial y Agencias Públicas Empresariales)
    - %DPD comunicados a la autoridad de control: 95%

En el marco del programa P08, de homogeneización de la figura de DPD en la organización, se ha completado el proyecto 04 (Equiparar la coordinación de protección de datos a otras áreas como por ejemplo transparencia), dado que se ha creado una unidad orgánica con nivel 30, denominada Coordinación para la Transformación e Innovación de la Administración Pública y Protección de Datos, y se le ha dotado de 6 personas a cargo con plazas de diversos niveles, incluyendo una de nivel 29, 2 de nivel 28 y 2 de nivel 26. En cuanto a indicadores destacan los siguientes:

- Indicadores de realización:
    - Existencia coordinación nivel 30 y estructura de apoyo (S/N): S

En el marco del programa P09, de refuerzo de la figura de DPD en la organización, se han hecho avances relevantes en los siguientes proyectos:

- 04. Reforzamiento de la cooperación la autoridad de control (CTPDA) actuando como punto de contacto con la misma: De forma generalizada, las personas DPD tienen asignada la función de punto de contacto con el CTPDA en lo relativo a la gestión de violaciones de protección de datos (brechas).
- 06. Adquisición/construcción de herramienta informática para la gestión automatizada del RAT y del riesgo: Se ha realizado un análisis de mercado de las herramientas existentes para esta función.
- 07. Gestión documental vinculada a la responsabilidad proactiva: plantillas Actividad de tratamiento, categorías de datos, respuestas al ejercicio de derechos, cesiones de datos, etc.: Se ha creado un espacio de almacenamiento compartido entre todas las personas DPD, donde se ubica toda la documentación relevante a estos efectos, incluyendo la utilizada en las reuniones de coordinación.
- 08. Creación de una Intranet de protección de datos para compartir recursos con las personas responsables de tratamientos y con otros DPD: Se ha contratado el desarrollo de la intranet. Se ha iniciado la elaboración del material a publicar.
- 09. Elaboración de manual de buenas prácticas en materia de protección de datos: Se han elaborado 12 píldoras informativas con buenas prácticas en temas concretos.

En el marco del programa P10, de formación especializada para DPD, se está trabajando de manera continua en el proyecto 01 (Impartición de formación especializada para DPD), dado que anualmente se imparten cursos de formación avanzada en protección de datos, y se imparte un curso de especialización para delegados de protección de datos (programa superior DPD/DPO). En cuanto a indicadores destacan los siguientes:

- Indicadores de resultado:
    - %DPD con formación especializada: al menos 7 DPD tienen la certificación en protección de datos, y del resto la mayoría han recibido formación especializada.
- Indicadores de realización:
    - Nº cursos realizados: 1 al año
    - Nº DPD formados anualmente: 15

En el marco del programa P12, de creación de recursos para facilitar la labor del DPD, se ha completado el proyecto 01 (Creación de un grupo de trabajo formado por todos los DPD) y se mantienen reuniones con periodicidad mensual, siempre en el mismo día de cada mes. En cuanto a indicadores destacan los siguientes:

- Indicadores de realización:
    - Número de reuniones del grupo de trabajo de los DPD: 20

II.3. Línea estratégica de capacitación y concienciación

Esta línea abarca los siguientes programas:

- P13. Programa de formación general en protección de datos de carácter personal
- P14. Programa de sensibilización general en protección de datos de carácter personal

En el marco del programa P13, de formación general en protección de datos de carácter personal, se ha avanzado de manera relevante en los proyectos 01 (Ampliar la oferta formativa permanente, progresiva y especializada, dirigida a las personas responsables de los tratamientos) y 02 (Ampliar la oferta formativa permanente, progresiva y especializada, dirigida al personal empleado público en general), dado que se ha elaborado un plan de formación para el año 2025 que tiene en cuenta las necesidades de formación en protección de datos de todos los colectivos y se ha trasladado al IAAP para incorporarlo a su plan de formación integral. Asimismo, se ha avanzado en el proyecto 03 (Crear píldoras formativas dirigidas a todos los sujetos implicados en el ciclo de vida del dato de carácter personal), habiéndose elaborado 12 píldoras formativas. En cuanto a indicadores destacan los siguientes:

- Indicadores de realización:
    - Nº de cursos anuales: 2 (en 2024)
    - Nº de personas empleadas públicas formadas: 1.457 personas (1.283 en la primera edición del curso “Protección de datos personales en la práctica”, y 174 en el curso de perfeccionamiento “Aplicación práctica en materia de protección de datos en la Junta de Andalucía”.

En el marco del programa P14, de sensibilización general en protección de datos de carácter personal, se encuentra casi finalizado el proyecto 02 (Inclusión de la materia de protección de datos en los temarios de las oposiciones para el ingreso a los distintos grupos de personal funcionario y en los contenidos de los cursos selectivos de acceso), dado que se ha incorporado esta materia a los temarios de los procesos selectivos, quedando pendiente incorporarlo en los cursos selectivos de acceso.

II.4. Línea estratégica de ciudadanía y privacidad

Esta línea abarca el programa 15, de transparencia en materia de protección de datos orientado a la ciudadanía.

En el marco de este programa se ha completado el proyecto 03 (Mejorar la accesibilidad y visibilidad de la política de privacidad y sobre el uso de cookies en el portal web de la Junta de Andalucía), dado que se ha publicado un aviso de cookies en el portal, con la posibilidad de aceptarlas, rechazarlas o gestionarlas, así como la política sobre el uso de cookies. En cuanto a indicadores destacan los siguientes:

- Indicadores de realización:
    - Comprobar que la política de privacidad y sobre el uso de cookies está visible y accesible para la ciudadanía: S