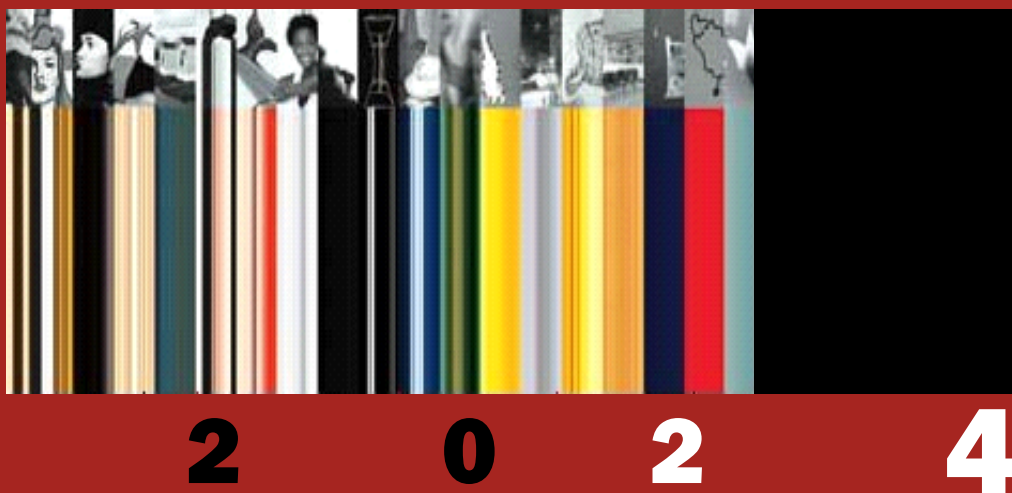
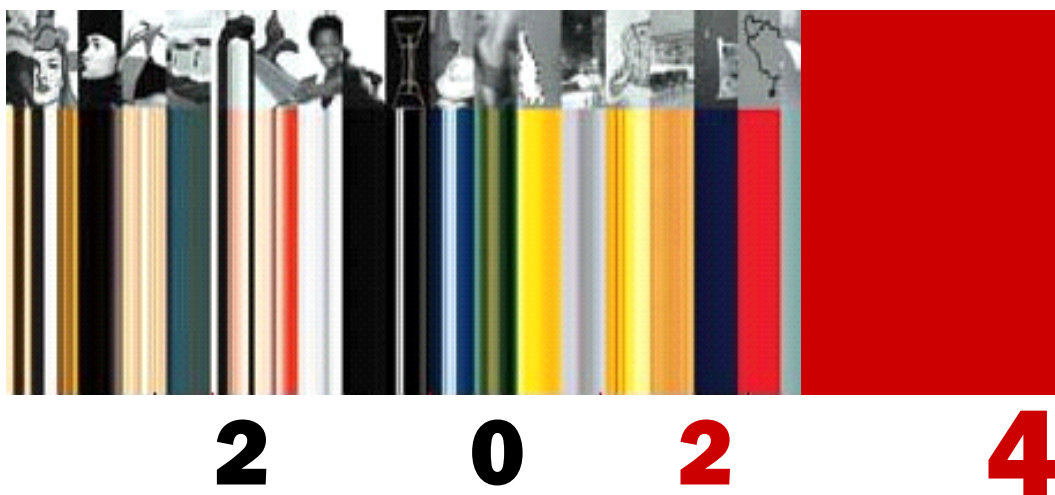


INFORME ANUAL DE ACTIVIDADES



Datuak Babesteko
Euskal Agintaritza
Autoridad Vasca de
Protección de Datos

INFORME ANUAL DE ACTIVIDADES



**Datuak Babesteko
Euskal Agintaritza**
Autoridad Vasca de
Protección de Datos



Autoridad Vasca de Protección de Datos – Datuak Babesteko Euskal Agintaritza
Beato Tomás de Zumárraga, 71 – 3ª planta.

01008 VITORIA-GASTEIZ

avpd@avpd.eus

www.avpd.eus

INFORME ANUAL DE ACTIVIDADES 2024

ISSN: 2253-9506

Periodicidad: anual

D.L. VI 312-2006

Esta obra está bajo Licencia Creative Commons



Reconocimiento (by)

Usted es libre de:

- Copiar, distribuir y comunicar públicamente la obra
- Remezclar — transformar la obra
- Hacer un uso comercial de esta obra

Bajo las condiciones siguientes:

- **Reconocimiento** — Debe reconocer los créditos de la obra de la manera especificada por el autor o el licenciador (pero no de una manera que sugiera que tiene su apoyo o apoyan el uso que hace de su obra).

Más información: <http://creativecommons.org/licenses/by/3.0/es/legalcode.es>



INDICE

PAGINA

1	PRESENTACION.....	4
2	EL CONSEJO CONSULTIVO.....	7
2.1	Personas Miembros del Consejo Consultivo	7
2.2	Sesiones celebradas	8
3	ACTIVIDAD CONSULTIVA	10
3.1	Atención telefónica, presencial y telemática.....	11
3.2	Consultas.....	11
3.3	Dictámenes	12
3.4	Informes	17
3.5	Reuniones.....	18
4	ACTIVIDAD DE CONTROL	20
4.1	Tutela de derechos.....	20
4.2	Denuncias.....	30
4.3	Procedimientos de infracción de las administraciones públicas	36
4.4	Autos y Sentencias.....	47
5	EL REGISTRO DE PERSONAS DELEGADAS DE PROTECCIÓN DE DATOS	49
5.1	Administración Local	50
5.2	Vinculación de los Responsables de Tratamiento con sus DPD-DBO.....	50
6	LA NOTIFICACIÓN DE BRECHAS DE SEGURIDAD	52
7	FORMACION IMPARTIDA POR EL PERSONAL DE LA AVPD	55
8	CENTRO DOCUMENTACION	57
8.1	Principales acciones en el área de documentación	57
8.2	Gestión documental	58
8.3	Comunicación.....	59
8.4	Herramientas de trabajo.....	59
8.5	Otros proyectos	59
8.6	Medios de comunicación	60
9	GESTIÓN INTERNA	64
9.1	Estructura y plantilla de personal	64
9.2	Presupuestos	66
9.3	Recursos materiales.....	68
9.4	Política de Prevención de Riesgos Laborales.....	69
9.5	Gestión sostenible e impacto ambiental	69
10	DATOS RELATIVOS A LA ACTIVIDAD CONSULTIVA	70
11	DATOS RELATIVOS A LA ACTIVIDAD DE CONTROL.....	71
12	DATOS RELATIVOS A LA GESTION INTERNA	72
12.1	Datos relativos a la plantilla presupuestaria	72
12.2	Datos relativos a la ejecución presupuestaria	73



1 PRESENTACION

En cumplimiento de lo dispuesto en el artículo 8.8 de la Ley 16/2023, de 21 de diciembre, de la Autoridad Vasca de Protección de Datos, y de conformidad con lo regulado en el artículo 59 del Reglamento General de Protección de Datos de la UE, se elabora el informe anual de actividades de la Autoridad Vasca de Protección de Datos/Datuak Babesteko Euskal Agintaritza (AVPD) relativo al año 2024, que debe comunicarse al Parlamento Vasco, Gobierno Vasco y demás autoridades de protección de datos del Estado. La finalidad del documento es trasladar a la sociedad vasca el conocimiento sobre la labor desarrollada por la Autoridad durante el año 2024, en la salvaguarda del derecho fundamental a la protección de datos. Se trata de rendir cuentas ante la sociedad vasca y, a su vez, aportar orientación, esencialmente a los entes que componen el sector público vasco, en las mejores prácticas en protección de datos, de acuerdo con los criterios que la propia Autoridad ha ido definiendo a lo largo del año.

Son varios los hitos que han marcado la actividad de la AVPD durante 2024. Estos hitos se corresponden con los objetivos fijados en el Plan Estratégico de la Autoridad, presentado ante el Parlamento Vasco por la actual Presidencia al inicio de su mandato. En primer lugar, en lo que corresponde a la labor de sensibilización y comunicación de los entes que componen el sector público vasco caben destacar cuatro aspectos. Por un lado, el aumento de la presencia de la AVPD en los medios de comunicación y redes sociales, a fin de impulsar campañas de concienciación de la ciudadanía vasca sobre la importancia del derecho a la privacidad. Por otro, la creación de una red de delegadas y delegados de protección de datos denominada HEDATU, a fin de articular un espacio en el que puedan compartir experiencias, conocimiento, dudas y documentación, para facilitar el trabajo conjunto, la formación y la colaboración. Además, se ha trabajado en la elaboración de materiales que aportan criterios específicos sobre cómo proteger los datos de carácter personal en determinados ámbitos, que puedan servir a los principales agentes implicados en la protección de datos. Por último, se han impartido numerosos cursos formativos, así como organizado diversos eventos dirigidos a transferir el conocimiento de la Autoridad a la sociedad.

En segundo lugar, en lo que afecta a la modernización de la Autoridad, se está llevando a cabo un proceso de transformación tanto de la sede electrónica como de la página web, para que sean más intuitivas y accesibles, y más fáciles de usar. Se trata de hacer que la AVPD sea más visible, accesible y transparente ante la sociedad vasca y ante los entes que la Administración independiente fiscaliza. Este proceso de modernización fortalece, a su vez, la necesaria independencia de la Autoridad, exigida por la normativa europea de protección de datos, en la medida en que se dirige a crear herramientas cuya gestión dependa de la propia AVPD y no de otras administraciones.

En tercer lugar, tras la aprobación de la nueva Ley de la Autoridad Vasca de Protección de Datos a finales de 2023, ha sido fundamental replantear la organización y funcionamiento del ente, con el objetivo de adaptarse a las necesidades que plantea la nueva norma, teniendo en cuenta, sobre todo, que se



amplía el ámbito de actuación de la AVPD. Se ha aprobado el Plan de Ordenación de Recursos Humanos a fin de hacer frente a las nuevas necesidades de personal y se han impulsado diferentes medidas dirigidas a estabilizar y ampliar la plantilla. Asimismo, se ha impulsado la acción exterior de la Autoridad con su incorporación a foros de trabajo internacionales, como son la Red Iberoamericana de Protección de Datos, la *Spring Conference 2024* *32nd European Conference of Data Protection Authorities* o la *European Case Handling Workshop ECHW 2024*, eventos en los que se trabaja con las distintas autoridades de control internacionales sobre cuestiones de alcance global. Por otro lado, se está colaborando con la Delegación de Euskadi para la Unión Europea, en Bruselas, a fin de abrir canales de comunicación directos con las instituciones europeas. Se trata de situar a la AVPD en el actual escenario internacional, cada vez más complejo e incierto, y trabajar para que la Autoridad tenga más peso en las instituciones europeas dedicadas a la materia de la protección de datos.

En cuarto lugar, se han articulado líneas de trabajo específicas en materias sensibles como la educación, sanidad o la Inteligencia Artificial. En el ámbito de la educación, se ha abierto un canal de cooperación con la administración educativa a fin de afrontar los retos que plantea la digitalización de los centros de enseñanza. En el ámbito de la sanidad, se ha impulsado un espacio de colaboración con la nueva Dirección de Osakidetza a fin de trabajar sobre aspectos esenciales como el nuevo Reglamento sobre Espacio Europeo de Datos Sanitarios, así como en la elaboración de una instrucción sobre accesos a las historias clínicas. En relación con la Inteligencia Artificial, siendo conscientes de que actualmente el proceso de digitalización del sector público vasco pasa por el uso de herramientas que emplean IA en el procesamiento de datos, y que en la UE se está articulando un nuevo marco normativo dirigido a regular esta tecnología, se ha creado un grupo de trabajo a nivel interno, para afrontar los retos que plantea la IA.

En quinto lugar, se ha realizado un esfuerzo desde la Autoridad para fortalecer su compromiso con el euskera. Por un lado, impulsando la elaboración del primer plan de normalización del uso del euskera para la AVPD. Por otro, participando en la edición de 2024 de la Korrika. Por último, dando, por primera vez, presencia al euskera en los Cursos de Verano de UIK de 2024, “Digitalización de la enseñanza: una visión desde la protección de datos”, organizados por la Autoridad.

Más allá de estos hitos la actividad de la AVPD ha seguido siendo prolija. Por un lado, desarrollando una importante función consultiva, resolviendo posibles dudas sobre cómo aplicar la normativa de protección de datos en casos específicos. Por otro, realizando su actividad ordinaria de control, concretada en la tramitación de los expedientes correspondientes a los procedimientos de tutela de derechos, de infracciones y otros, teniendo en cuenta que el número de expedientes tramitados este año ha aumentado considerablemente con respecto al año anterior. Por último, llevando a cabo una importante labor de colaboración y cooperación con otros entes, caso de las demás autoridades de control que operan en el Estado, así como con otras administraciones que desarrollan su actividad en sectores estratégicos como la sanidad, la educación o la seguridad, o la Inteligencia Artificial, caso del Ararteko o del Basque Artificial Intelligence Center (BAIC) en los que la protección de datos adquiere una relevancia especial.



Este Informe Anual de Actividades constituye un ejercicio de transparencia, para que los diferentes agentes que componen la sociedad vasca puedan fiscalizar la actividad de la AVPD durante el año 2024, y un documento que pueda ayudar a los sujetos responsables de tratamientos de datos de carácter personal, fundamentalmente a los entes que componen el sector público vasco, a interpretar de manera adecuada la normativa de protección de datos.

Unai Aberasturi Gorriño

Presidente de la Autoridad Vasca de Protección de Datos



2 EL CONSEJO CONSULTIVO

El Consejo Consultivo de la Autoridad Vasca de Protección de Datos (AVPD), previsto en la Ley 16/2024, de 21 de diciembre, de la Autoridad Vasca de Protección de Datos, es un órgano colegiado de asesoramiento a la Presidencia de la AVPD, cuya composición es la que determina el artículo 9 de dicha Ley y en la que están representados el Parlamento Vasco, el Gobierno Vasco, las Diputaciones Forales, las entidades locales de Euskadi y dos representantes de la Universidad del País Vasco, uno del ámbito de la informática y el otro del campo de los derechos fundamentales.

2.1 PERSONAS MIEMBROS DEL CONSEJO CONSULTIVO

A 31 de diciembre de 2024 forman parte del Consejo Consultivo las personas siguientes:

- **D. Raúl García Ezquerro.** Alcalde de Laguardia. Representante de las entidades locales de Euskadi.
- **Dña. Montserrat Auzmendi del Solar.** Letrada del Parlamento Vasco.
- **D. Agustín Zubillaga Rego.** Viceconsejero de administración digital y servicios generales. Lehendakaritza.
- **D. Javier Bikandi Irazabal.** Director General de Coordinación y Estrategia Digital de la Diputación Foral de Bizkaia, en representación de las Diputaciones Forales.
- **D. Eduardo Jacob Taquet.** Catedrático de Ingeniería Telemática. Universidad del País Vasco/Euskal Herriko Unibertsitatea.
- **D. Iñaki Esparza Leibar.** Presidente. Catedrático de Derecho Procesal. Universidad del País Vasco/ Euskal Herriko Unibertsitatea.

De conformidad con lo establecido en el artículo 6 de las NORMAS DE ORGANIZACIÓN Y FUNCIONAMIENTO DEL CONSEJO CONSULTIVO DE LA AUTORIDAD VASCA DE PROTECCIÓN DE DATOS, **D^a. Ainara Ugalde López**, Secretaria General de la AVPD, desempeña la función de Secretaria del Consejo Consultivo.

De conformidad con lo establecido en el punto 8 del artículo 7 de las NORMAS DE ORGANIZACIÓN Y FUNCIONAMIENTO DEL CONSEJO CONSULTIVO DE LA AUTORIDAD VASCA DE PROTECCIÓN DE DATOS, **D. Unai Aberasturi Gorriño**, Presidente de la AVPD, asiste, con voz y sin voto, a las sesiones del Consejo Consultivo.

La presidencia del Consejo Consultivo es rotativa, por período de un año y en el orden establecido en el artículo 4.1 de las NORMAS DE ORGANIZACIÓN Y FUNCIONAMIENTO DEL CONSEJO CONSULTIVO.



2.2 SESIONES CELEBRADAS

El Consejo Consultivo celebró en el año 2024 las siguientes reuniones:

- **Sesión ordinaria de 27 de junio de 2024** en la cual, tras la aprobación unánime del acta anterior, la Secretaría General presentó el Plan Estratégico de Recursos Humanos de la AVPD, orientado a reforzar la independencia institucional y la capacidad de autoorganización. El plan detalla la situación actual de la plantilla (15 puestos ocupados y 4 vacantes), los 9 puestos adicionales aún por incorporar a la RPT y la previsión de próximas jubilaciones. Se definieron acciones inmediatas como la aprobación de OPEs, el desarrollo de procesos selectivos, y la planificación del relevo generacional. Asimismo, se anunciaron medidas para revisar la estructura organizativa, actualizar la RPT y las monografías, dimensionar adecuadamente los recursos humanos y fomentar la promoción interna.

Además, se contemplan acciones dirigidas a fortalecer el vínculo interno y el entorno laboral: mejoras en la comunicación interna, difusión de contenidos, elaboración de protocolos sobre salud laboral, acoso en el trabajo y agresiones de terceros. Estas medidas buscan reforzar el compromiso del personal con la organización y garantizar un entorno seguro, igualitario y saludable.

Por otro lado, se expusieron los proyectos estratégicos impulsados por la Presidencia conforme al Plan Estratégico vigente, centrados en aumentar la visibilidad y proyección externa de la AVPD, mejorar el conocimiento ciudadano en protección de datos y fortalecer la colaboración interinstitucional. Finalmente, el asesor de modernización presentó los avances en administración electrónica, tras detectar debilidades en las herramientas actuales. Se están analizando soluciones del Gobierno Vasco y de mercado, en colaboración con EJE y otras entidades, para mejorar la eficacia administrativa de la Agencia. La reunión concluyó sin ruegos ni preguntas, cerrándose a las 13:30 horas.

- **Sesión ordinaria de 19 de diciembre de 2024** en la que se aprobó por unanimidad el acta de la reunión anterior. El primer punto de la jornada trató sobre la propuesta de resolución del presidente de la Autoridad Vasca de Protección de Datos (AVPD), mediante la cual se aprobaba la oferta de empleo público para el año 2024. En este contexto, la secretaria general presentó el marco normativo que regula este tipo de ofertas, haciendo referencia tanto al Estatuto Básico del Empleado Público (EBEP) como a la Ley 11/2022, de Empleo Público Vasco, destacando la importancia de convocar procesos selectivos para cubrir vacantes presupuestadas. Se explicó además que, aunque la OPE no se enmarca dentro de los procesos de estabilización de empleo, sí incluye la cobertura de plazas ocupadas por personal interino debido a situaciones excepcionales, como la crisis sanitaria por la pandemia de COVID-19.

En cuanto a las plazas a cubrir, se detallaron cinco vacantes estructurales que debían ser cubiertas mediante oferta pública. Estas plazas, correspondientes a áreas clave como la Asesoría Jurídica y la Inspección, así como la Secretaría General, eran consideradas fundamentales para asegurar el funcionamiento de la AVPD. El presupuesto asignado para la cobertura de estas plazas fue aprobado dentro del marco presupuestario del País Vasco para el año 2024. Además, se



cumplió con el proceso de negociación con la representación del personal, que tuvo la oportunidad de hacer observaciones y aportaciones.

A continuación, se procedió a la presentación de la relación de plazas que conformaban la oferta de empleo público para 2024. Las plazas incluidas eran las siguientes: tres vacantes de Letrado/a Instructor/a Inspector/a para el área de Asesoría Jurídica e Inspección, y dos plazas para la Secretaría General, una de Técnico/a Traductor/a y otra de Técnico/a de Documentación e Información. Se destacó que la oferta fue aprobada por resolución del presidente de la AVPD en diciembre de 2024, y que las convocatorias para estas plazas se realizarían dentro de los tres años siguientes a su publicación en el Boletín Oficial del País Vasco.

Uno de los puntos más importantes de la reunión fue la creación de una nueva plaza en la AVPD, específicamente para un/a Gestor/a de Administración y Recursos Humanos. Esta nueva plaza tiene como objetivo asegurar una correcta transferencia de conocimientos dentro de la organización, algo que fue aprobado favorablemente por los miembros de la junta. Además, se acordó modificar los requisitos lingüísticos de dos puestos dentro de la Unidad de Evaluación de Impactos Tecnológicos, con el fin de cumplir con los porcentajes legales exigidos de conocimiento del euskera, lo cual era esencial para garantizar la adaptación a las normativas lingüísticas vigentes.

Finalmente, se presentó un informe sobre el presupuesto de la AVPD para el ejercicio 2025. La secretaria general detalló las principales partidas presupuestarias y justificó el incremento en el presupuesto respecto al año anterior, explicando que este aumento era necesario para cubrir nuevas necesidades operativas y de personal. A pesar de que no se plantearon otros temas relevantes, la reunión concluyó sin nuevos puntos a tratar, y la sesión fue levantada a las 13:30 horas.





3 ACTIVIDAD CONSULTIVA

El año 2024 ha sido el primer año de la autoridad de control en Euskadi como Autoridad Vasca de Protección de Datos, tras la aprobación por el Parlamento Vasco de la Ley 16/2023, de 21 de diciembre, de la Autoridad Vasca de Protección de Datos.

En el plano legislativo, el hecho más relevante, sin lugar a dudas, ha sido la aprobación del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, por el que se establecen normas armonizadas en materia de inteligencia artificial, cuya entrada en vigor se produjo el 1 de agosto de 2024.

Se trata de un texto que, al igual que ha ocurrido con el Reglamento General de Protección de Datos, pretende constituirse en una norma de referencia más allá de las fronteras de la Unión. La inteligencia artificial se configura como una de las tecnologías clave dentro de la llamada cuarta revolución industrial, tecnología transversal por su afectación a todos los ámbitos de actividad, que, no obstante, genera grandes incertidumbres en lo tocante al respeto a los derechos fundamentales, y que exigirá una importante labor ponderativa por parte de los responsables de despliegue de estos sistemas, así como de las instituciones de gobernanza de estos sistemas.

Además de la omnipresente inteligencia artificial, otros desarrollos tecnológicos han exigido la atención de la Autoridad. Así, las tecnologías de seguimiento por redes inalámbricas (wifi tracking) también han sido objeto de análisis por la autoridad vasca de protección de datos, que junto a las otras tres autoridades ha publicado una guía para su utilización compatible con el derecho fundamental.

Además, la utilización en los centros educativos de la CAE de plataformas ofrecidas por grandes corporaciones tecnológicas ha sido objeto de un profundo análisis conjunto con los responsables de la Administración educativa. El empleo de estas plataformas ha sido también objeto de la actividad de control mediante la tramitación de un procedimiento de declaración de infracción, como más adelante se reseñará.

Asimismo, la Autoridad Vasca de Protección de Datos también advirtió de los peligros y de los requisitos exigibles a una iniciativa privada consistente en el tratamiento de datos biométricos (escaneo del iris) realizado a cambio de criptomonedas.

A estas cuestiones de relevancia general se suman otras preocupaciones ciudadanas que se expresan en las reclamaciones recibidas en la Autoridad. Así, el análisis de los procedimientos tramitados en la Autoridad durante 2024 permite extraer algunas conclusiones:

En primer lugar, debemos destacar la preocupación sobre el acceso a la historia clínica que expresa la ciudadanía a través de sus reclamaciones. Año a año se hace cada vez más evidente que el tratamiento de los datos de salud constituye uno de los aspectos del derecho fundamental que los ciudadanos más valoran y con mayor celo desean proteger.



El tratamiento de los datos biométricos bien sea como sistema de acceso a instalaciones, oficinas, etc. o con fines policiales o puramente comerciales como antes hemos mencionado, continúa exigiendo una importante labor tuitiva por parte de la Autoridad Vasca de Protección de Datos.

En lo referente a los principios más vulnerados, en los procedimientos de infracción tramitados, abundan las vulneraciones del principio de integridad y confidencialidad, en muchos casos debidas a errores o desconocimientos que a indiscreciones deliberadas.

3.1 ATENCIÓN TELEFÓNICA, PRESENCIAL Y TELEMÁTICA

La AVPD es una institución joven que trata de llegar a la ciudadanía a través del mayor número posible de canales. Si bien los procedimientos reglados (sancionadores, de declaración de infracción o de tutela de derechos) requieren el cumplimiento de requisitos formales, la prestación de asesoramiento por parte de la Autoridad sobre cuestiones que preocupan o interesan a las personas, se realiza de una manera más acorde con el principio informalista.

Así, muchas personas son atendidas presencialmente en la sede de la Autoridad y otras reciben asesoramiento tras formular consultas telefónicas o por correo electrónico.

Durante el 2024, las cuestiones que más han preocupado a Administraciones y ciudadanía han estado vinculadas a tratamientos de datos relacionados con el servicio público educativo, con el tratamiento de datos vinculados a la prevención, represión e investigación de delitos e infracciones penales, con la permanencia injustificada de información obsoleta en páginas web institucionales, o con la demanda de control sobre los tratamientos realizados sobre los datos de salud de las personas.

3.2 CONSULTAS

Las consultas de mayor complejidad que en materia de protección de datos se formulan a la AVPD, se resuelven vía dictamen. Esta labor de asesoramiento que presta la Autoridad en cumplimiento del artículo 6 de la Ley 16/2023, de 21 de diciembre, se ofrece tanto a Administraciones como a personas, físicas o jurídicas, siempre que se cumplan las siguientes premisas:

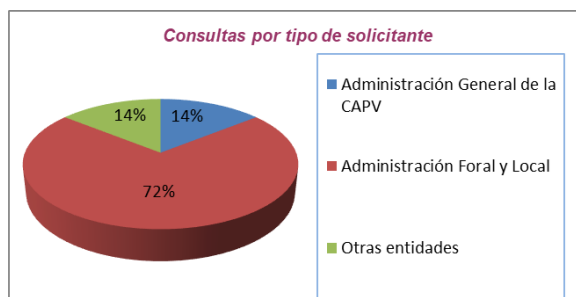
- que la consulta verse sobre el tratamiento de datos personales cuyos responsables sean las Administraciones Públicas y Entidades incluidas en nuestro ámbito de aplicación.
- que la cuestión planteada sea concreta, lo que exige, al menos, la descripción del tratamiento que plantea dudas y la aportación de cuanta información pueda ser relevante para que la Autoridad forme su criterio con garantías de acierto.





Durante el año 2024, al igual que en ejercicios anteriores, la mayoría de las consultas recibidas en la Autoridad las formulan los Ayuntamientos y las Diputaciones Forales, seguido de la Administración General de la CAPV.

Entre las consultas formuladas, merece destacarse la referida a la implantación de sistemas biométricos para acceso a instalaciones municipales.



3.3 DICTÁMENES

Los dictámenes más representativos están disponibles en la página web de la Autoridad (www.avpd.eus).

- **Contenido de las publicaciones de las listas de electores y de candidatos en las elecciones a los órganos de representación del personal al servicio de una administración local (CN24-001)**

La publicación por las mesas electorales de las listas de electores, elegibles, y la proclamación de las candidaturas es un tratamiento amparado por el cumplimiento de una obligación legal (art. 6.1 c RGPD), como figura en la Ley del Estatuto Básico del funcionario Público, en Ley del Estatuto de los Trabajadores, y en los reglamentos de desarrollo vigentes. Dichas listas las elabora la propia Mesa Electoral a partir del censo que le debe facilitar la Administración Pública implicada, y la publicación tiene como finalidad dar a conocer a las personas partícipes en el proceso electoral: quién ostenta la condición de elector, de elegible y quiénes son los candidatos presentados.

Y siendo esa la finalidad, y en aplicación del principio de minimización de datos, sólo se deben publicar aquellos datos personales del censo que sean imprescindibles para esa finalidad. Bastaría con el nombre, apellidos y el número del DNI en la forma que indica la Disposición Adicional 7ª de la LOPDGDD. La publicación en el tablón no deberá ser colocada en lugares accesibles a personas ajenas al proceso electoral, y no más allá de la fecha límite fijada para el ejercicio de los derechos a cuya efectividad coadyuva.

- **Uso de la huella dactilar como mecanismo de autenticación para el acceso a ciertas instalaciones de un ayuntamiento (CN24-002)**

El tratamiento de datos biométricos, específicamente la huella dactiloscópica, para el control de acceso a determinadas instalaciones municipales no es conforme con la normativa reguladora de protección de datos.

Teniendo en cuenta que los datos biométricos se incluyen en la actualidad en las categorías especiales de datos a que se refiere el artículo 9 del RGPD, con carácter previo al tratamiento de este tipo de datos, debería analizarse la proporcionalidad, necesidad e idoneidad para la finalidad pretendida.



Históricamente, las interpretaciones doctrinales han estado orientadas a subrayar la diferencia entre identificación y autenticación, y considerar solamente la técnica de la identificación como un tratamiento de datos de categorías especiales, como un tratamiento de datos biométricos.

No obstante, teniendo en cuenta el contexto y la evolución social, tecnológica y jurídica en este ámbito, estas consideraciones parecen superadas. Así, es necesario destacar las aportaciones realizadas por las Directrices 05/2022 del Comité Europeo de protección de Datos (CEPD), sobre el uso de la tecnología de reconocimiento facial, que determinan en su apartado 12 que el concepto de dato biométrico abarca tanto la autenticación como la identificación, y que ambos se incluyen en las categorías especiales de datos.

Teniendo en consideración estas interpretaciones, se puede afirmar que, en el caso del uso de la huella dactilar como mecanismo de autenticación para el acceso a ciertas instalaciones de un ayuntamiento, los datos objeto de tratamiento serían datos de categorías especiales, y por tanto se debería realizar un análisis sobre la legitimación del tratamiento de este tipo de datos para conseguir la finalidad pretendida, el control de los accesos a determinadas instalaciones.

En el caso objeto de consulta, el tratamiento pretendido deberá ampararse en una norma con rango legal que habilite el mismo. En este sentido, debemos analizar la STC 76/2019, de 22 de mayo, en la que el Tribunal Constitucional afirma que no es suficiente la mera existencia de norma con rango legal, sino que esta deberá determinar las circunstancias de las limitaciones del derecho fundamental.

En la actualidad, en el ordenamiento jurídico aplicable, no existe ninguna norma con rango de ley que reúna estos requisitos. Es decir, no existe ninguna norma legal que autorice el tratamiento de datos biométricos para el control de presencia, precisando además sus límites y garantías, aportando previsibilidad y la seguridad jurídica. Además, se debe tener en cuenta que cualquier excepción a la prohibición habrá de ser objeto de interpretación restrictiva.

Por ello, otra posible base legitimadora para el tratamiento pudiera ser el consentimiento, con base en el apartado 9.2.a) del RGPD, siempre y cuando se garantice que el mismo es obtenido libremente.

Por tanto, podríamos afirmar que, desde el punto de vista del requisito de libertad del consentimiento, para poder cumplirlo, el empleador, en este caso el ayuntamiento, debería ofrecerles a los empleados otra opción equivalente, menos intrusiva, que no trate datos personales biométricos, dado que no se puede olvidar el hecho de que el tratamiento de datos biométricos en este caso es un medio para conseguir el control de accesos a determinadas instalaciones, y no una finalidad por sí misma.

Aun así, en el presente supuesto se debe también tener en consideración que, si existe otra opción equivalente para la consecución del fin pretendido con este tratamiento, la obtención de los datos biométricos sería un tratamiento excesivo, ya que no cumpliría con el principio de minimización y la proporcionalidad, así como necesidad para conseguir el fin perseguido.





- **Comunicación a las personas inscritas en Lanbide de la identidad del personal profesional de referencia asignado por dicho organismo autónomo (CN24-003)**

La comunicación prevista por Lanbide de la identidad del profesional asignado (nombre y primer apellido) a las personas previamente inscritas en dicho organismo como demandantes de servicios de empleo y residentes en la CAE es un tratamiento de datos personales y como tal está sujeto a la normativa de protección de datos.

La Ley 15/2023, de 21 de diciembre, de Empleo, recoge los principios rectores de las políticas públicas de empleo y reconoce una serie de derechos que se centran en dar un servicio personalizado (asistencia personalizada, diagnóstico personal sobre la empleabilidad, elaboración de un plan integrado y personalizado de empleo participado por la persona usuaria), y será Lanbide el organismo que deberá garantizar tales derechos. La ley indica que tendrá que asignar a tales personas inscritas un profesional de referencia que llevará a cabo las funciones que tal ley determina. Asimismo, indica cuándo debe realizarse la asignación y que la misma ha de comunicarse a las personas interesadas.

La identificación del profesional de referencia mediante su nombre y primer apellido no vulnera el principio de minimización de datos, ya que de esta forma se puede cumplir con la finalidad de que Lanbide preste, a través de estos profesionales de referencia, una asistencia personalizada, continuada y adecuada dirigida a que aquéllas puedan encontrar un empleo y mejorar su empleabilidad o las perspectivas de trabajo autónomo.

El responsable deberá cumplir con el deber de transparencia informando a los profesionales de referencia del nuevo tratamiento (comunicación a personas inscritas).

Y entre los derechos reconocidos por el RGDP, destacamos el derecho de oposición, que podrán ejercitar los profesionales de referencia en los propios términos que indica el artículo 21.1.

- **Comunicaciones de datos a través del sistema IMI (CN24-005)**

La consulta realizada por la Diputación Foral de Gipuzkoa plantea diversas cuestiones en torno a la adecuación de la transmisión de información por la DFG a las autoridades rumanas para comprobar la autenticidad de la tarjeta de cualificación de conductor expedida por la DFG a través del sistema de información del mercado interior (en adelante, “Sistema IMI”) a la normativa de protección de datos.

En relación con la cuestión concreta planteada por la DFG sobre la necesidad de recabar el consentimiento del interesado, para poder analizar el encaje del consentimiento como base de legitimación para el tratamiento de datos personales, debemos señalar que, en el caso de las administraciones públicas, por regla general, existe una relación de desequilibrio entre la Administración pública y los ciudadanos, lo que imposibilita la condición de libertad que debe contener el consentimiento para su validez.



Teniendo en cuenta que el tratamiento indicado tiene que venir amparado por alguna de las bases jurídicas recogidas en el artículo 6.1 del RGPD, en este caso concreto podría encontrar su amparo en la letra c), es decir, “el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento” o también en la letra e), es decir, “el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento”

En este caso, tras el examen de la normativa sectorial aplicable se determina que la DFG es competente en materia de movilidad y transportes mecánicos por carretera dentro de su territorio, siendo el ejercicio de la competencia administrativa la base legitimadora del tratamiento y, además, el tratamiento de datos personales se realiza en cumplimiento de una obligación legal para lograr la cooperación administrativa eficaz en lo que respecta al reconocimiento de cualificaciones profesionales.

Asimismo, se informa sobre las obligaciones que tiene como responsable la DFG en relación con el RAT, con la obligación de respetar los principios del artículo 5 del RGPD, en especial el principio de transparencia.

- **Implantación de un sistema de control de acceso por huella dactilar (CN24-006)**

La consulta realizada por el Instituto Foral de Bienestar Social de la Diputación Foral de Álava plantea diversas cuestiones en torno a la implantación de un sistema de control de acceso por huella dactilar de los empleados en las instalaciones de la dicho Organismo Autónomo. Así, la cuestión sometida al criterio de la Autoridad versa sobre la adecuación del tratamiento de datos biométricos de empleados a la normativa de protección de datos.

En la medida en que los datos biométricos permiten o comprueban la identificación de una persona física, están sometidos a la normativa de protección de datos. Además, el artículo 9.1 del RGPD establece un régimen específico de protección para el tratamiento de lo que se denominan categorías especiales de datos personales, en las que incluye los datos biométricos. En este sentido, queda prohibido el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida a la vida sexual o las orientaciones sexuales de una persona física.

El mismo artículo 9, en su apartado 2, detalla los supuestos de excepción a la prohibición general que habilitan el tratamiento de datos de categorías especiales, levantando la prohibición del tratamiento. Entre los supuestos previstos, se encuentra el consentimiento explícito otorgado por el interesado para el tratamiento de dichos datos.

Para poder analizar el encaje del consentimiento como condición de levantamiento de la prohibición, debemos comenzar por señalar que el artículo 4.11 del RGPD se refiere al consentimiento del interesado como “toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea





mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen”. Por su parte, el Considerando 43 del RGPD establece que para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibrio claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular.

Es decir, en el caso de las administraciones públicas, por regla general, existe una relación de desequilibrio entre la Administración pública y los ciudadanos, el cual no posibilita la condición de libertad que debe contener el consentimiento para su validez.

Por tanto, podríamos afirmar que, desde el punto de vista del requisito de libertad del consentimiento, para poder cumplirlo, el empleador, en este caso el Instituto Foral de Bienestar Social de la Diputación Foral, debería ofrecer a los empleados otra opción equivalente, menos intrusiva, que no trate datos personales biométricos, dado que no se puede olvidar el hecho de que el tratamiento de datos biométricos en este caso es un medio para conseguir el control de accesos a determinadas instalaciones, y no una finalidad por sí misma.

Aun así, en el presente supuesto se debe también tener en consideración que, si existe otra opción equivalente para la consecución del fin pretendido con este tratamiento, la obtención de los datos biométricos sería un tratamiento excesivo, ya que no cumpliría con el principio de minimización y la proporcionalidad, así como necesidad para conseguir el fin perseguido.

- **Utilización de los datos provenientes de la red wifi municipal externa del Ayuntamiento (CN24-007)**

Un Ayuntamiento pretende utilizar la información sobre el movimiento de los dispositivos móviles conectados a la red WIFI municipal a lo largo del tiempo a fin de identificar las tendencias de movilidad urbana, zonas de aglomeraciones en función de factores externos (festivos, eventos especiales,), zonas comerciales en función de campañas u otros parámetros, y plantea en su consulta si estamos ante un tratamiento de datos personales a los que sea de aplicación la normativa de protección de datos personales.

Los datos transmitidos por las señales Wi-Fi utilizados en este tipo de procesos pueden ser considerados como datos personales en la medida en que están relacionados con personas identificables y son susceptibles de ser utilizados para su identificación directa o indirecta, en concreto estaríamos hablando del identificador de dispositivo o MAC, la fecha/hora y la posición.

La obtención o recogida de información de los dispositivos por la red Wifi municipal, así como el propio proceso de anonimización, y su posterior utilización para los fines indicados en la consulta en el caso de que se llegase a materializar el riesgo de reidentificación, constituyen tratamientos de datos personales.



En la medida que hay tratamiento de datos personales, el responsable tendrá que cumplir los principios consagrados en el RGPD, en concreto el de licitud, limitación de la finalidad y limitación del plazo de conservación. En lo relativo al cumplimiento del principio de licitud, la base legitimadora aplicable a cada tratamiento requiere de un análisis pormenorizado del caso concreto por parte del responsable del tratamiento, en virtud del principio de responsabilidad proactiva (artículo 5.2 RGPD), que tendrá en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento.

De acuerdo con el artículo 35.3 del RGPD, en aquellos tratamientos que incorporen Wi-Fi tracking y que supongan una observación sistemática a gran escala de una zona de acceso público, la EIPD será obligatoria.

En cuanto a las medidas técnicas y organizativas apropiadas el dictamen se remite a las orientaciones publicadas por las autoridades de control, haciendo hincapié en el proceso de anonimización.

3.4 INFORMES

Durante el año 2024 han sido objeto de informe doce proyectos de decreto y cinco convenios:

- Proyecto de Decreto de respuesta a la diversidad en el marco de un sistema educativo inclusivo, para las alumnas y alumnos de los centros docentes no universitarios de la CAE.
- Proyecto de Decreto por el que se aprueba el Programa Estadístico Anual 2024.
- Proyecto de Decreto de la Comisión de Valoración, Selección y Acceso a los Documentos de la Comunidad Autónoma de Euskadi (COVASADE).
- Proyecto de Decreto por el que se crea el Registro de Sociedades Civiles del País Vasco y se aprueba su Reglamento.
- Proyecto de Decreto de regulación de la utilización de las instalaciones del Centro Autorizado Superior de Música del País Vasco-Musikene para actividades no comprendidas en su programación anual.
- Proyecto de Decreto por el que se crea y regula el Registro de Asociaciones de Comerciantes de Euskadi.
- Proyecto de Decreto por el que se crea la Red Vasca de Puntos de Asistencia Comercial MERKASARETZA y se define la Cartera de Servicios de Asistencia Comercial.
- Proyecto de Decreto de creación del Sistema de información sobre adicciones de Euskadi.
- Proyecto de Decreto por el que se regulan los estímulos al empleo de aplicación a las personas beneficiarias de la Renta de Garantía de Ingresos y de las ayudas de emergencia social.





- Proyecto de Orden por la que se regula el Catálogo Corporativo de Servicios y Procedimientos del Sector Público de la CAE en sus procedimientos sujetos al derecho público.
- Proyecto de Orden por la que se aprueba la política de firma electrónica basada en certificados.
- Proyecto de Orden por la que se regula el Registro Electrónico General del sector público de la Comunidad Autónoma de Euskadi en sus procedimientos sujetos al derecho pública.
- Convenio entre el Ministerio de Asuntos Económicos y Transformación Digital, Ministerio de Hacienda y Función Pública y CAPV para la prestación mutua de soluciones básicas de administración digital.
- Convenio de Colaboración entre la Administración General de la CAE, departamento de salud del gobierno vasco, y la comunidad de Castilla León en materia de asistencia sanitaria.
- Convenio de colaboración entre la Administración General de la CAE y el Instituto Aragonés de Ciencias de la Salud para la participación en proyectos de investigación.
- Convenio de colaboración entre la Administración General de la CAE y la Universitat de Valencia en materia de registro de tumores infantiles.
- Convenio entre INSS, ISM y Admón. Gral. de la CAE para acceso telemático a los informes médicos de los exp. administrativos del INSS y del ISM por parte de los Servicios Públicos de Salud.

3.5 REUNIONES

Se enuncian a continuación algunas de las reuniones en las que ha participado la Autoridad Vasca de Protección de Datos en el año 2024.

- Osakidetza: se subrayó la necesidad de fortalecer la cooperación y colaboración entre los dos entes, tanto en la tramitación de expedientes que afectan a Osakidetza, como para la elaboración de documentos que ayuden a desarrollar buenas prácticas en la protección de datos en el ámbito sanitario.
- Departamento de Educación del Gobierno Vasco: se abordaron sobre todo cuestiones relativas al uso de plataformas educativas.
- Departamento de Seguridad del Gobierno Vasco: se trataron temas de videovigilancia policial, así como de ejercicio de derecho de supresión en este ámbito.
- Basque Artificial Intelligence Center (Baic): se trató de la posibilidad de colaboración entre la Autoridad Vasca de Protección de Datos y el Basque Artificial Intelligence Center en materia de inteligencia artificial.



- Departamento de Cultura del Gobierno Vasco: se analizó la adecuación a la normativa de protección de datos de una solución tecnológica que pretende identificar el índice de uso del euskera en el ámbito del sector público vasco.
- Ararteko: se abordó la posible firma de un convenio de colaboración.
- Reunión de Autoridades de Protección de Datos en Vitoria para tratar el tema de la gestión de brechas de seguridad.
- Reunión de Autoridades de Protección de Datos en Madrid para tratar cuestiones relacionadas con la imposición de sanciones a responsables de tratamiento.
- Reunión de Autoridades de Control para la elaboración de una guía sobre el uso de tecnologías de seguimiento wifi.
- Reuniones con Ciberzaintza; se analizó la posibilidad de colaboración entre los dos entes para elaborar materiales que ayuden a la gestión eficiente de brechas de seguridad, así como para hacer llegar a la AVPD posibles supuestos de brechas.





4 ACTIVIDAD DE CONTROL

La protección y defensa del derecho fundamental a la protección de los datos personales se lleva a cabo, bien a través de una política preventiva y divulgativa y también por medio de la actuación de control, bien por propia iniciativa o tras la recepción de reclamaciones (denuncias o solicitudes de tutela de derechos).

La Autoridad Vasca de Protección de Datos despliega en los supuestos de denuncias casos su potestad sancionadora para garantizar el cumplimiento del derecho fundamental por parte de las Instituciones y entidades sometidas a su ámbito de actuación.

Igualmente, la Autoridad Vasca de Protección de Datos actúa como órgano de tutela de los diferentes derechos que integran el derecho fundamental (derecho de acceso, rectificación, supresión, oposición, limitación y portabilidad), al resolver aquellas reclamaciones que traen causa del previo ejercicio de derechos ante los responsables de tratamiento. Ejercicio de derechos que los reclamantes consideran no atendidos o no de forma satisfactoria.

El Reglamento General de Protección de Datos atribuye a todas las autoridades de control numerosas funciones y amplios poderes, entre otros, poderes de investigación y poderes correctivos, regulando las infracciones y las sanciones o actuaciones correctivas que pueden imponerse.

Estos poderes implican por el contrario, una obligación de colaborar con las autoridades de control, que en nuestro caso, se detalla en el artículo 13 de la Ley 16/2023, de 21 de diciembre, de la Autoridad Vasca de Protección de Datos, al disponer que las administraciones públicas, incluidas las haciendas forales, así como las personas físicas o jurídicas, estén o no sometidos sus tratamientos a lo dispuesto en dicha ley, estarán obligados a proporcionar a la Autoridad Vasca de Protección de Datos los datos, informes, antecedentes y justificantes que fueren necesarios para llevar a cabo la actividad de investigación en el ámbito de sus competencias.

La colaboración prestada por las Instituciones y entidades reclamadas ha sido, en general, buena, si bien, en algunas ocasiones, la Autoridad se ha visto obligada a reiterar sus peticiones de información, advirtiendo que la falta de cooperación con la Autoridad de Protección de Datos en el ejercicio de sus funciones es una conducta sancionable conforme al RGPD y a la Ley Orgánica 3/2018.

A este respecto, debe mencionarse que, Osakidetza-Servicio Vasco de Salud, que, en lo tocante a esta obligación de colaboración, fue objeto de una mención negativa en la memoria de la Autoridad correspondiente al año 2023, ha revertido esa tendencia desde los últimos meses de 2024 hasta la actualidad.

4.1 TUTELA DE DERECHOS

Al igual que ocurrió en el año 2023, durante 2024 han sido muchas las reclamaciones de tutela presentadas ante la Autoridad Vasca de Protección de Datos que ha sido objeto de estimación parcial, pues, aunque el derecho afectado había sido materialmente satisfecho, lo había sido de manera extemporánea, una vez



superado el plazo legal fijado para ello. De hecho, en ocasiones la presentación de la reclamación ante la autoridad ha servido de acicate para que los responsables atendieran las peticiones relacionadas con el ejercicio de derechos.

En este sentido, un año más, debe recordarse a los responsables de tratamiento que la satisfacción extemporánea del derecho constituye una vulneración del derecho fundamental. Cuestión que se ve agravada si tenemos en cuenta que los derechos de acceso, supresión... constituyen contenido esencial del derecho al evidenciarse en los mismos de una manera más intensa el poder de disposición sobre la información personal.

En lo referente al tipo de derecho ejercitado por la ciudadanía, podemos citar tres ámbitos predominantes entre las reclamaciones recibidas: solicitudes de acceso y supresión de datos obrantes en historias clínicas, solicitudes de acceso y supresión de datos policiales y solicitudes de supresión (olvido) de informaciones publicadas en páginas web.

En el primer caso se trata de solicitudes de acceso en muchas ocasiones orientadas a un control sobre posibles accesos indebidos, o a un deseo de eliminar información sensible que las personas pueden considerar estigmatizante. En el caso de peticiones relacionadas con datos policiales, se trata de eliminar información cuya permanencia puede ocasionar consecuencias desfavorables para las personas. En cuanto a las reclamaciones vinculadas con informaciones publicada en páginas web, se evidencia una voluntad de eliminar información obsoleta o innecesaria que los motores de búsqueda hacen accesible de forma muy sencilla a un tercero.

En lo relativo al número de estimaciones, podemos afirmar que han sido estimadas más del 71% de las reclamaciones de tutela presentadas y admitidas, de las cuales, casi el 40% se refieren a Osakidetza-Svs.

Datos 2024: 14 estimatorias, 3 archivo, 7 desestimatorias, 5 inadmitidos, 1 competencia AEPD y 1 Diligencia de cierre. (Total resueltas 31).

Se recogen a continuación las tutelas resueltas en el año 2024.

4.1.1 Derecho de acceso

- **Acceso a historia clínica obrante en Osakidetza-Svs (ET23-016)**

En el escrito de reclamación se pone de manifiesto que, habiendo ejercido el derecho de acceso a su historia clínica relativa a los años 2022 y 2023, su solicitud no había sido atendida.

Se estima la reclamación formulada dado que la misma no fue satisfecha por Osakidetza-Svs en el plazo legalmente establecido y que únicamente se le dio traslado de los accesos realizados los años 2021 y 2022, obviando los meses de 2023 que se solicitaban.

Se interpuso Recurso de Reposición (RR24-002) siendo desestimado.





- **Acceso a consultas realizadas a su ficha policial (ET23-019)**

Se desestima la reclamación formulada contra el Departamento de Seguridad del Gobierno Vasco por la denegación del derecho de acceso ejercido por el reclamante, dado que éste no ha especificado los datos sobre los cuales ejerce el derecho de acceso.

Se interpone recurso de reposición que se desestima, dado que el recurrente no especifica los datos sobre los cuales ejerce el derecho de acceso.

- **Denegación de acceso a certificado de empadronamiento (ET23-020)**

La pretensión del reclamante es la obtención de un certificado de empadronamiento. Si bien es cierto que la emisión de estos certificados conlleva un tratamiento de datos personales, en este caso la reclamación no está relacionada con el ejercicio de ninguno de los derechos reconocidos a los interesados por la normativa en esta materia. En sentido estricto, la reclamación se refiere al cumplimiento o no de las condiciones para que el Ayuntamiento expida el certificado de empadronamiento, lo que es una cuestión de legalidad ordinaria sujeta al derecho administrativo y, por lo tanto, ajena a la protección de datos personales. Por último, cabe señalar que el Ayuntamiento de Bilbao afirma haber accedido finalmente a la solicitud y ha proporcionado el certificado de empadronamiento al reclamante. A la vista de lo anterior, se inadmite la tutela presentada.

- **Acceso a partes de intervención de los Servicios Sociales de un Ayuntamiento (ET23-022)**

Una persona solicita el acceso a los partes de intervención de sus hijos realizados por los servicios sociales del Ayuntamiento de Abanto y Zierbena siendo inadmitida la reclamación dado que el derecho ejercitado en este supuesto no es el derecho de acceso del RGPD sino que es el derecho de acceso al expediente, regulado como derecho de acceso en la Ley 39/2015 y por ello, conforme a sus preceptos deben sustanciarse las solicitudes que a él hacen referencia. La resolución del ejercicio de este derecho no corresponde a la Autoridad Vasca de Protección de Datos, sino al propio Ayuntamiento de Abanto-Zierbena, al tratarse del acceso a un expediente, siendo impugnabile dicho acto tanto en vía administrativa como ante la jurisdicción contenciosa.

- **Acceso a datos policiales (ET23-025)**

Tal como establece la normativa de protección de datos, mediante el ejercicio del derecho de acceso el reclamante puede conocer qué datos personales tiene el responsable del tratamiento, y el procedimiento para ejercer este derecho conlleva dirigirse en primer lugar al responsable de tratamiento; es decir, al Departamento de Seguridad del Gobierno Vasco, invocando el derecho de acceso que le asiste. Si el Departamento de Seguridad no responde en el plazo de un mes o el reclamante considera que la respuesta obtenida no es satisfactoria, entonces puede presentar



una reclamación ante la Autoridad Vasca de Protección de Datos para que esta institución tutele su derecho de acceso.

En consecuencia, procede inadmitir la reclamación recibida, instando al reclamante a que se dirija previamente al Departamento de Seguridad del Gobierno Vasco siguiendo el procedimiento descrito.

- **Vulneración del derecho de acceso a historia clínica (ET23-026)**

La persona reclamante solicita a Osakidetza el acceso al registro de accesos a su historia clínica. Se estima la reclamación presentada al haber sido atendido el derecho de acceso de manera extemporánea, y se insta a Osakidetza para que adopte las medidas necesarias tendentes a garantizar el efectivo ejercicio de los derechos que a las personas les reconoce el Reglamento General de Protección de Datos.

- **Vulneración del derecho de acceso a historia clínica (ET24-003)**

Se reclama ante la AVPD la tutela de su derecho de acceso a su historia clínica, en concreto, el evolutivo o episodio concreto que, según refiere, se ha eliminado de su historial clínico, y los motivos de su eliminación, habiendo solicitado previamente dicha información a Osakidetza hasta en tres ocasiones.

Se estima la reclamación presentada por la reclamante por no haber sido atendido el derecho de acceso y se requiere al responsable del tratamiento para que adopte las medidas necesarias tendentes a garantizar el efectivo ejercicio de los derechos que a las personas les reconoce el Reglamento General de Protección de Datos.

- **Acceso a la historia clínica obrante en Osakidetza-Svs (ET24-004)**

Una persona ejercita el derecho de tutela ante esta Autoridad porque habiendo solicitado reiteradamente su historia clínica completa a Osakidetza, dicha solicitud no había sido debidamente atendida, puesto que una serie de documentos que la persona reclamante especificaba expresamente no le habían sido remitidos.

Se estima la reclamación de tutela presentada y se insta a Osakidetza-Servicio vasco de salud para que, en el plazo de diez días hábiles siguientes a la notificación de la resolución, remita a la parte reclamante los documentos solicitados y que se detallaban en el Fundamento Jurídico III de la propia resolución. Se le indica que las actuaciones realizadas como consecuencia de la Resolución deberán ser comunicadas a esta Autoridad en idéntico plazo. Se advierte, además, que el incumplimiento de la resolución de la Agencia podría comportar la comisión de la infracción incluida en el artículo 72.1m) de la LOPDGDD (incumplimiento de una resolución dictada por una autoridad de protección de datos), y se le insta al cumplimiento en lo sucesivo de las condiciones establecidas en el artículo 12 del Reglamento General de Protección de Datos.





- **Acceso a datos personales obrantes en el Colegio de la Abogacía de Bizkaia (ET24-007)**

El reclamante solicita la tutela del derecho de acceso solicitado al Colegio de la Abogacía de Bizkaia. Alega que la solicitud de acceso ha sido denegada.

Se resuelve con desestimación, ya que el Colegio demuestra que la solicitud ha sido contestada en plazo y satisfecita. Desde el Colegio se ha comunicado la inexistencia de datos personales del reclamante.

- **Vulneración del derecho de acceso y supresión (ET24-008)**

La parte reclamante se dirigió a esta Autoridad solicitando la tutela de su derecho de acceso, al entender que no se le había proporcionado toda la información personal de la que disponía el Ayuntamiento de Vitoria en relación a la atención recibida por su Servicio de Igualdad. La Administración reclamada argumentó que no se le facilitó la información personal de la reclamante ya que únicamente constan en el dossier notas manuscritas y apuntes que la titular del puesto había ido tomando en diferentes fechas, y que dicho dossier no incluye un expediente estructurado, unas conclusiones o una propuesta de acciones a realizar.

Esta Autoridad entiende que las circunstancias invocadas no pueden ser obstáculo para que la reclamante tenga acceso a sus datos personales en los términos indicados en el artículo 15 del RGPD. El artículo 15.3 del RGPD establece que el responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento, pero ello no afectará negativamente a los derechos y libertades de otros según matiza el artículo 15.4 del RGPD. Se estima la reclamación en cuanto al derecho de acceso.

La parte reclamante también se dirigió a la Autoridad para tutelar su derecho de supresión respecto a esos mismos datos personales. Se desestima la reclamación respecto a este derecho, puesto que el responsable atendió en plazo su derecho, previo bloqueo de los datos personales tal y como contempla el artículo 32 de la LOPDGDD durante el plazo de 3 años, acompañado, según expone el Ayuntamiento, de las medidas técnicas y organizativas adecuadas para impedir su tratamiento, incluyendo su visualización.

- **Desacuerdo con la respuesta obtenida por el ejercicio del derecho de acceso y otros derechos (ET24-010)**

El reclamante muestra su disconformidad con la respuesta obtenida por parte del Departamento de Igualdad, Justicia y Políticas Sociales del Gobierno Vasco tras haber ejercitado sus derechos; pero, a la luz de la información requerida al Gobierno Vasco, se estima que la contestación se ajusta a la normativa de protección de datos, por lo que se archiva la reclamación presentada.



- **Vulneración del derecho de acceso a historia clínica (ET24-012)**

En sus alegaciones, el reclamante sostiene que el documento que ha recibido por parte de Osakidetza es ilegible, que algunos de los accesos son incoherentes y que no se identifica a las personas que han realizado los accesos.

Respecto a la ilegibilidad, el documento es el habitual que utiliza esa institución para responder a las peticiones de acceso. En cuanto a la incoherencia de los accesos, que el reclamante no llega a identificar, se le indica que debe dirigirse al responsable de tratamiento; es decir, a Osakidetza, para obtener información sobre los mismos.

En relación con la identificación de los profesionales, en la actualidad, ni la normativa sanitaria estatal ni la autonómica vasca reconocen explícitamente que el derecho de acceso incluya la identificación de los profesionales sanitarios que acceden a la historia clínica.

Por último, en lo relativo a la solicitud de conocer los accesos en la historia clínica a partir de noviembre de 2023, el reclamante debe dirigir su petición a Osakidetza, tal como hizo anteriormente, por tratarse de un nuevo ejercicio del derecho de acceso.

En conclusión, el único incumplimiento de la normativa de protección de datos achacable a Osakidetza es no haber respondido en el plazo fijado de un mes, ya que el reclamante realiza la petición de acceso el 20 de marzo de 2024 y se le facilita la información el 20 de mayo de 2024, por lo que resulta evidente que, si bien el interesado ha obtenido finalmente la información requerida, la satisfacción del derecho no se ha producido en el plazo de un mes marcado por el artículo 12.3 del RGPD. Por lo tanto, se estima la reclamación, al haber sido atendido extemporáneamente el derecho de acceso del reclamante.

- **Acceso a documentación del Instituto Foral de Bienestar Social de Álava (ET24-014)**

Se inadmite la tutela reclamada ya que el derecho que pretende ejercitar el reclamante es el acceso a los documentos contenidos en un procedimiento administrativo, regulado en el artículo 53.1 de la Ley 39/2015.

Por lo tanto, la resolución del ejercicio de ese derecho no corresponde a esta Autoridad, sino al propio IFBS que, a raíz de la solicitud de información requerida por parte de la AVPD, alega haber entregado la documentación solicitada anonimizando los datos personales de terceros.

- **Acceso a grabaciones telefónicas (ET24-024)**

Se presenta reclamación contra Lanbide-Servicio Vasco de Empleo porque habiendo solicitado el acceso a distintas grabaciones telefónicas le habían dado el acceso a las mismas, pero fuera del plazo establecido en el RGPD.





Se estima formalmente pero no materialmente la reclamación formulada dado que Lanbide-Servicio Vasco de Empleo atendió su derecho de acceso remitiéndole la grabación telefónica solicitada, pero fuera del plazo legalmente establecido.

4.1.2 Derecho de supresión

- **Supresión de datos personales obrantes en Osakidetza (ET23-014)**

La reclamante solicita la supresión de sus datos a Osakidetza. No obstante, no acredita haber ejercido previamente el derecho ante Osakidetza, por tanto, se ha requerido esa información por parte de la AVPD. Al no recibirse la información solicitada, no se puede continuar con el expediente, y en consecuencia se archiva mediante una diligencia de cierre.

- **Supresión de antecedentes policiales (ET23-023)**

Se desestima la solicitud de tutela del derecho de supresión no concedido por el Departamento de Seguridad del Gobierno Vasco, ya que de acuerdo con el art. 24 de la LO 7/2021, queda justificada legalmente la denegación de la supresión de los datos solicitados.

- **Supresión de publicación en el Boletín Oficial de Gipuzkoa (ET23-024)**

La persona reclamante solicita la tutela de la AVPD frente a la Diputación Foral de Gipuzkoa por denegación del derecho de supresión y olvido de datos publicados en el BOG, solicitando asimismo no solo la desindexación sino la eliminación del propio Boletín.

Se estima parcialmente la reclamación presentada dado que no se puede proceder a la supresión en la fuente, pues precisamente el derecho al olvido consiste en dificultar la búsqueda, el acceso a los datos sin que la fuente se vea afectada, tal y como se prevé en artículo 5.3 de la Norma Foral 5/2007, de 27 de marzo, reguladora del Boletín Oficial de Gipuzkoa. Por ello, debe procederse a la desindexación, medida que permite cohonestar el ejercicio del derecho de supresión y olvido con el respecto a la integridad de los Boletines Oficiales.

Asimismo, se requiere al responsable del tratamiento para que adopte las medidas necesarias tendentes a garantizar la desindexación de la información personal afectada tanto en los motores de búsqueda generales de internet como en el motor interno de búsqueda de la edición digital del Boletín Oficial.

La persona reclamante interpone recurso de reposición que se desestima por considerar la resolución ajustada a derecho.

- **Recepción de correos electrónicos desde el servicio de aparcamiento del Ayuntamiento de Bilbao (ET24-002)**

El reclamante denuncia que recibe correos desde ese servicio sin haberse dado de alta en él y pretende ejercer el derecho de supresión. Sin embargo, el



Ayuntamiento demuestra fehacientemente que sí está dado de alta, por lo que el envío de correos electrónicos encuentra su base de legitimación en la ejecución de un contrato en el que el interesado es parte. Aun así, una vez recibido el requerimiento de información de la AVPD mediante el que ha conocido el deseo del reclamante de no recibir más correos electrónicos, el Ayuntamiento ha procedido a darle de baja en la aplicación y comunicárselo, de forma que, en la práctica, su demanda se ha visto finalmente satisfecha. En definitiva, al no poder apreciarse ninguna vulneración de derechos, se archiva la reclamación.

- **Supresión de datos personales obrantes en material de formación (ET24-013)**

La persona reclamante acude a la AVPD, por la denegación del derecho de supresión por la Diputación Foral de Bizkaia. La persona reclamante solicitaba la supresión de sus datos personales (imagen y voz) tratados con ocasión de la impartición de un curso de formación. En concreto, solicitaba la supresión basándose en el artículo 21.1 del RGPD, que es la oposición al tratamiento de los datos.

Se estima la reclamación presentada y se exige a la Diputación Foral de Bizkaia el traslado de la efectiva satisfacción del derecho de supresión a la persona interesada.

- **Supresión de datos (ET24-016)**

Se presenta reclamación contra el Ayuntamiento de Bilbao, derivada del ejercicio del derecho de supresión, en la que la reclamante exponía que, habiendo presentado una instancia al Ayuntamiento de Bilbao, para la eliminación de ciertos datos personales que aparecen en abierto en internet, la misma no había sido atendida, por lo que solicitaba la intervención de la Autoridad para que se eliminaran sus datos de los lugares en los que aparecían y que detallaba en la reclamación.

Se estima formalmente la reclamación presentada por la reclamante porque, aunque fue atendida su reclamación, la misma se hizo efectiva fuera del plazo legalmente establecido en el artículo 12.3 del RGPD. Asimismo, se requiere al responsable del tratamiento para que adopte las medidas necesarias tendentes a garantizar el efectivo ejercicio de los derechos que a las personas les reconoce el Reglamento General de Protección de Datos.

- **Derecho de supresión de datos publicados en web (ET24-020)**

Se estima la reclamación presentada por la parte reclamante al haber sido atendido el derecho de supresión por el Ayuntamiento de Zumaia fuera del plazo legalmente establecido, requiriendo al Ayuntamiento para que adopte las medidas necesarias tendentes a garantizar el efectivo ejercicio de los derechos que a las personas les reconoce el Reglamento General de Protección de Datos.

De la documentación obrante en el expediente se constata que el derecho de supresión ejercido por la reclamante, aunque de forma tardía, ha sido atendido desde una perspectiva material.





- **Derecho de supresión de datos publicados en web (ET24-021)**

Se estima la reclamación presentada por la parte reclamante al haber sido atendido el derecho de supresión fuera del plazo legalmente establecido, requiriendo al Departamento de Educación del Gobierno Vasco para que adopte las medidas necesarias tendentes a garantizar el efectivo ejercicio de los derechos que a las personas les reconoce el Reglamento General de Protección de Datos.

De la documentación obrante en el expediente se constata que el derecho de supresión ejercido por la reclamante, aunque de forma tardía, ha sido atendido desde una perspectiva material.

- **Supresión de datos personales obrantes en el servicio de Alertas del Ayuntamiento (ET24-023)**

El reclamante solicita la supresión de sus datos personales del listado del servicio de alertas al móvil mediante SMS que gestiona el Ayuntamiento de Irún.

Se desestima la reclamación. No es posible la supresión de sus datos, ya que los mismos no están registrados en el listado de personas suscritas al servicio de alertas.

- **Supresión de datos policiales (ET24-025)**

La persona reclamante solicita la tutela de la AVPD por denegación del derecho de supresión de datos policiales solicitada al Departamento de Seguridad del Gobierno Vasco.

Se desestima la reclamación presentada dado que analizados los antecedentes, documentación obrante en el expediente y atendiendo a las concretas circunstancias del caso, resulta justificada la denegación de la supresión de los antecedentes policiales del reclamante, al no justificarse la concurrencia de ninguna de las circunstancias establecidas por el artículo 17 del RGPD, y estar acreditada la excepción del artículo 17.3 b) al existir una obligación legal impuesta por el Real Decreto 137/1993, de 29 de enero, por el que se aprueba el Reglamento de Armas y la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.

4.1.3 Derecho de rectificación

- **Vulneración del derecho de rectificación/supresión de historia clínica (ET24-001)**

El reclamante solicita a la AVPD la tutela de su derecho de rectificación y supresión al haber sido denegada su pretensión por Osakidetza, alegando que no se estima procedente tras realizar las gestiones correspondientes. A la Autoridad no le corresponde determinar si unos concretos datos médicos son necesarios para una eventual asistencia futura del paciente, pero sí le corresponde apreciar la falta de



un informe que especifique, con un mínimo detalle, la necesidad de conservar esa parte de la historia clínica.

Dado que la Administración no ha contestado a los requerimientos de información realizados por esta Autoridad, procede estimar la reclamación de tutela formulada a fin de que la Administración resuelva motivadamente sobre la supresión y rectificación ejercitada por el reclamante, requiriendo a Osakidetza para que remita dicha resolución al reclamante y a esta Autoridad.

- **Rectificación de datos policiales (ET24-006)**

La persona reclamante solicita la tutela de la AVPD por denegación del derecho de rectificación de datos erróneos que obran en los registros del Departamento de Seguridad del Gobierno Vasco relativos a sus antecedentes policiales.

Se desestima la reclamación presentada dado que, analizados los antecedentes y documentación obrante en el expediente, no consta acreditada la existencia de datos erróneos o incompletos.

- **Derecho de rectificación de la dirección postal en las bases de datos del Departamento de Educación del Gobierno Vasco (ET24-009)**

En este caso no se ha producido ningún tratamiento de datos personales, sino que nos encontramos ante un asunto de legalidad ordinaria, consistente en la subsanación de un trámite administrativo, que debe resolverse atendiendo a la ley 39/2015 del Procedimiento Administrativo Común del Procedimiento de las Administraciones Públicas y a la normativa que sea de aplicación. En este sentido, no corresponde a la AVPD pronunciarse sobre si el Departamento de Educación ha actuado correctamente al denegar el cambio de dirección postal solicitado por la reclamante al no haber presentado un certificado de empadronamiento en vigor. En todo caso, frente al acto administrativo que deniega la solicitud de cambio de dirección postal, la reclamante puede interponer los recursos previstos en la normativa administrativa. Por lo tanto, procede archivar la reclamación.

- **Vulneración del derecho de rectificación de historia clínica (ET24-011)**

La persona reclamante solicita la tutela de la AVPD por denegación por Osakidetza-Svs del derecho de rectificación de un informe clínico emitido por un médico de una especialidad médica concreta y que consta en su historia clínica.

Se desestima la reclamación presentada dado que el médico al que se le solicita la rectificación únicamente puede hacer referencia a los tratamientos que él esté llevando a cabo y a los que él, por su conocimiento, puede hacer referencia, no pudiendo valorar ni hacer referencia en sus informes a otras asistencias que él no ha prestado ni está tratando, respecto de las cuales está siendo tratado por otro médico especialista en esa materia.





- **Vulneración del derecho de rectificación y supresión de historia clínica de madre fallecida (ET24-015)**

La persona reclamante solicita la tutela de la AVPD por denegación del derecho de rectificación y supresión de determinados datos que constan en la historia clínica de su madre fallecida. Osakidetza le deniega dicho derecho al entender que es un derecho personalísimo y por tanto se extingue con la muerte de la persona.

Se estima la reclamación presentada dado que, aunque el artículo 2.2 de la LOPDGDD en principio excluya los datos de las personas fallecidas de la protección de datos, el artículo 3 regula una serie de situaciones en las que pueden llevarse a cabo determinadas acciones respecto al tratamiento de dichos datos. El artículo 3 establece expresamente que las personas vinculadas al fallecido por razones familiares o, de hecho, así como sus herederos, podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquélla y, en su caso, su rectificación o supresión. Por tanto, dicho precepto está legitimando a las personas vinculadas a la persona fallecida, como ocurría en el supuesto de referencia, para poder acceder a los datos y, en su caso, para solicitar su rectificación o supresión, siendo el alcance y los límites del derecho de rectificación y supresión (y en su caso derecho al olvido) regulados por las mismas disposiciones que el RGPD establece para las personas vivas. Únicamente se establece una excepción a esta regla general en el segundo párrafo del artículo 3.1, puesto que las personas vinculadas al fallecido no podrán acceder a los datos ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiera prohibido expresamente o así lo establezca la Ley.

4.2 DENUNCIAS

Se trata de reclamaciones presentadas por personas físicas o jurídicas en relación a actuaciones de las Administraciones, Instituciones y entidades sometidas a la potestad sancionadora de la Autoridad Vasca de Protección de Datos.

Las denuncias admitidas han derivado en un procedimiento de infracción o han sido archivadas por no existir indicios suficientes que pudieran justificar la apertura de dicho procedimiento.

4.2.1 Denuncias inadmitidas

Durante el año 2024 han sido varias las denuncias inadmitidas por referirse a personas físicas o entidades de naturaleza jurídico-privada excluidas del control de la Autoridad Vasca de Protección de Datos, y que han sido remitidas a la Agencia Española de Protección de Datos (DN24-035, DN24-039, DN24-066, DN24-038, DN24-024, DN24-028, DN24-056, DN24-057, DN24-065, DN24-082, DN24-032, DN24-020, DN24-075, DN24-016, DN24-026, DN24-029, DN24-054).

Otras dieciséis denuncias han sido inadmitidas por diferentes motivos. Siete de ellos se refieren al tratamiento de datos derivado del proyecto “Mi Salud@UE” del Ministerio de Sanidad (intercambio intracomunitario de datos para la atención sanitaria de los pacientes). Al respecto, se debe poner de manifiesto que los servicios ofrecidos bajo la denominación “Mi Salud@UE” a los que se hace



referencia en la reclamación no implican la comunicación, cesión o envío de datos. Solo en el caso de que el propio interesado solicite asistencia sanitaria en un estado miembro de la Unión Europea distinto al de su residencia los profesionales sanitarios implicados podrán consultar su historia clínica resumida. La base de legitimación de los citados tratamientos no es el consentimiento del interesado como se alega en la denuncia, al existir una obligación legal de los servicios públicos de salud de garantizar la asistencia a la ciudadanía, tal y como establece la Directiva 2011/24/UE, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza, y su norma de trasposición, el RD 81/2014 de 7 de febrero.

Más de un 70% de las denuncias recibidas y admitidas a trámite han finalizado en procedimientos en los que se ha declarado la comisión de infracciones de la normativa de protección de datos por las Administraciones Públicas de Euskadi.

4.2.2 Denuncias archivadas

- **Comunicación de una providencia de embargo de un vehículo a un tercero (DN23-041)**

La persona reclamante denuncia que se ha comunicado por parte del Departamento de Economía y Hacienda del Gobierno Vasco una providencia de embargo de un vehículo a un tercero.

Se archiva la denuncia presentada dado que no se acredita la comunicación a terceros objeto de denuncia, y por tanto no se acreditan actuaciones contrarias a la normativa de protección de datos por parte del Departamento de Economía y Hacienda del Gobierno Vasco.

El reclamante interpone recurso de reposición que se desestima por considerar la resolución ajustada a derecho.

- **Envío de una carta a un ciudadano por parte del Ayuntamiento (DN23-053)**

La persona reclamante denuncia que el Ayuntamiento de Sopela ha realizado un tratamiento inadecuado de datos personales, ya que ha recibido una carta en la que se le ha notificado que no está usando el sistema de recogida de residuos con apertura de contenedores.

Se archiva la denuncia presentada dado que el Ayuntamiento cuenta con legitimación para estos tratamientos.

- **Reclamación contra los protocolos de actuación de Osakidetza (DN23-055)**

El reclamante presenta escrito ante la AVPD porque considera que se produce una vulneración de la protección de datos por la información contenida en el sobre para el envío de correspondencia en el programa de detección precoz del cáncer de colon, así como en otras campañas preventivas (cáncer de mama), porque los resultados de las pruebas médicas se recogen en los ambulatorios en los mostradores estando en muchos casos en sobres no cerrados y porque en las





llamadas telefónicas para concertar una cita con un médico “la persona que atiende al teléfono, solicita datos médicos para derivar al paciente al médico de familia o a la enfermera...”.

Se archiva la reclamación presentada, tras el estudio detallado de las circunstancias denunciadas, al no observarse la existencia de ningún tipo de violación de la normativa de protección de datos, ya que en dicho sobre no se revela la edad ni dato médico ni confidencial del destinatario de este. Aun en el supuesto de que los informes sean entregados de la forma que indica, circunstancia que no ha quedado acreditada, debe señalarse que toda persona que esté en contacto con datos personales (sean éstos médicos o de cualquier otro tipo) tiene obligación de guardar secreto sobre los mismos.

En lo referente a las solicitudes de cita en el ambulatorio, la persona que atiende el teléfono, solicita datos médicos “para derivar al paciente al médico de familia o a la enfermera” tal y como indica el propio reclamante. Por ello, la razón que le asiste para solicitar dichos datos es que parece necesaria para poder ser atendido adecuadamente, sin perjuicio de que, como se ha señalado anteriormente, dicha persona tiene la obligación de guardar secreto sobre toda la información a la que tiene acceso y tratar los datos conforme a los principios determinados en el RGPD y en la LOPDGDD.

- **Recogida y tratamiento de datos sin consentimiento (DN23-059)**

La parte reclamante denuncia que Lanbide obtuvo sus datos personales (identificativos, de padrón, y datos fiscales referidos a ingresos y patrimonio) en el curso de un procedimiento de revisión de la prestación del ingreso mínimo vital del hijo de la parte reclamante, y que dicho tratamiento no ha sido informado, ni se ha consentido el mismo ni ha tenido la posibilidad de ejercitar el derecho de oposición.

Examinada la reclamación y la documentación aportada al expediente se constata que la potestad inspectora reconocida a la Administración reclamada por la normativa aplicable es la base jurídica que ampara el tratamiento de los datos personales de la parte reclamante, y no el consentimiento.

En cuanto al deber de información del responsable del tratamiento, nos encontraríamos en una de las excepciones contempladas en el artículo 14.5 c) del RGPD, es decir, cuando la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros, como es el caso, en concreto en las leyes reguladoras del ingreso mínimo vital.

Y en cuanto al derecho de oposición, no resulta acreditado que se haya vulnerado el mismo, puesto que no consta ni que haya ejercitado el mismo ni la denegación o falta de respuesta por Lanbide.

Por tanto, se resuelve archivar la reclamación presentada.

Contra la resolución de archivo se interpuso Recurso de Reposición (RR24-003). La parte recurrente basa fundamentalmente el recurso de reposición en que Lanbide accedió y recopiló sus datos tributarios sin la preceptiva autorización expresa, tal y como lo exige el párrafo tercero del apartado 7 del artículo 21 de la Ley 19/2021,



de 20 de diciembre, por la que se establece el ingreso mínimo vital, y el artículo 28.3 de la Ley 39/2015 de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

En aplicación de la normativa recogida en la resolución del recurso y la fundamentación de la resolución recurrida, esta Autoridad entiende que Lanbide obtuvo los datos tributarios de la Hacienda Foral sin consentimiento de los reclamantes al tener su amparo en lo que prevé la propia Ley 19/2021, que excepciona el consentimiento de los interesados en el supuesto de colaboración con las entidades encargadas de la gestión de la prestación económica del ingreso mínimo vital y en la lucha contra el fraude en la obtención y disfrute de la misma.

Desestimadas las alegaciones, esta Autoridad desestima el recurso de reposición interpuesto confirmando, por ajustada a derecho, la resolución recurrida.

- **Recepción de correos electrónicos de Lanbide sin haberse dado de alta en el servicio (DN23-063)**

Lanbide explica que ha sido una persona usuaria con el mismo nombre y primer apellido que el reclamante quien proporcionó una dirección electrónica incorrecta que coincide con la del reclamante, razón por la que éste ha recibido los correos electrónicos de forma indebida. Así, la inexactitud de este dato personal no es imputable a Lanbide al haberla obtenido de un usuario. Por otra parte, tras tener constancia de que la dirección de correo electrónico era inexacta, Lanbide contactó con la persona usuaria y ha procedido a cambiarla en su base datos, con el fin de que el reclamante no reciba ningún correo más.

En definitiva, Lanbide no es responsable de la inexactitud de la dirección de correo electrónico y, una vez conocida, ha actuado para asegurarse que en el futuro no puedan producirse envíos de correos electrónicos indebidos al denunciante, por lo que se archiva la denuncia.

- **Accesos indebidos a historia clínica (DN23-064)**

El reclamante denuncia que en Osakidetza se han producido accesos indebidos a su historia clínica y aporta la respuesta de Osakidetza en la que se informa que todos los accesos cuestionados, a excepción de dos, fueron correctos y debidos a diversos cometidos, entre otros, trabajo asistencial, respuestas a las peticiones de la persona reclamante, trámites administrativos, o salud pública; y que respecto a esos dos accesos cuestionados no ha abierto expediente disciplinario al haber prescrito la acción objeto de sanción.

En cuanto a la presunta infracción de la normativa de protección de datos, se constata la prescripción de la misma en cuanto a dos accesos cuestionados, al haberse cumplido el plazo máximo de prescripción para las infracciones más graves de la normativa de protección de datos (3 años, de conformidad con la LOPDGDD). Y respecto al resto de accesos cuestionados no ha quedado acreditado la existencia de accesos indebidos. Se resuelve, por tanto, archivar la reclamación presentada.



- **Accesos indebidos a historia clínica (DN23-065)**

La parte reclamante denuncia a Osakidetza por accesos indebidos a su historia clínica y asimismo solicita tutela de su derecho de acceso a su historia clínica respecto de unos episodios concretos.

Respecto a los accesos cuestionados, de la documentación que aporta la parte reclamante, no ha quedado acreditada la existencia de accesos indebidos a la historia clínica de la parte reclamante, al considerar Osakidetza que dichos accesos se consideraron adecuados al pertenecer a profesionales que corresponden a su círculo de asistencia en Osakidetza. Por tanto, esta Autoridad resuelve archivar la reclamación en cuanto a los accesos denunciados por la parte reclamante.

Y en cuanto al derecho de acceso pretendido, esta Autoridad resuelve tramitarlo como procedimiento de tutela de derechos, no como denuncia.

- **Obligatoriedad de presentar el consentimiento de tratamiento de datos para la realización de gestiones en el Ayuntamiento (DN23-070)**

La parte reclamante denuncia que el Ayuntamiento de Bilbao no accedió a recoger una solicitud de alta en el servicio público de teleasistencia gestionado por el Gobierno Vasco porque dicha entidad local exigía la autorización para la comunicación de datos personales a terceros.

La reclamación plantea en realidad una cuestión de legalidad ordinaria que queda fuera de la competencia de esta Autoridad, ya que se refiere a la propia negativa de presentar y dar trámite a una solicitud por parte de la Administración en las condiciones manifestadas por el reclamante.

Pese a que en la reclamación se hace referencia a un consentimiento sobre el tratamiento de sus datos personales (para recabar y/o ceder) que el reclamante no estaba dispuesto a otorgar, y que el Ayuntamiento reconoce que la cláusula informativa del tratamiento de datos en el momento de los hechos denunciados estaba en fase de revisión, lo cierto es que en este caso la Administración reclamada no ha realizado un tratamiento de datos personales del reclamante que esta Autoridad pueda someter a su análisis y control. Por tanto, esta Autoridad resuelve archivar la reclamación.

- **Comunicación a un tercero de información relativa a la renovación de la cuota de las Instalaciones Municipales (DN23-072)**

Se denuncia al Ayuntamiento de Vitoria-Gasteiz por la comunicación a un tercero de información relativa a la renovación de la cuota de las Instalaciones Municipales.

Se archiva la denuncia por no haber acreditado vulneración de la normativa de protección de datos, ya que el Ayuntamiento de Vitoria-Gasteiz comunicó la información a la persona que figuraba como representante en la solicitud inicial, y no se acredita la comunicación a terceros.



- **Solicitud e impresión del DNI para realizar cualquier trámite en Osakidetza (DN24-017)**

El reclamante presenta escrito ante la AVPD porque al menos en Bizkaia, tanto en sus centros de salud como en los hospitales, se toman datos privados innecesariamente dado que, cada vez que se pone una instancia, queja o cualquier otro escrito, se obliga a escribir el DNI y el número de tarjeta sanitaria y firmarlo. En otras ocasiones fotocopian el DNI y la tarjeta sanitaria.

Se archiva la reclamación presentada ya que el artículo 8.1 de la Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana (LOPSC) establece que el DNI *“es el único documento con suficiente valor por sí solo para la acreditación, a todos los efectos, de la identidad y los datos personales de su titular”* y la Administración tiene la obligación de verificar la identidad de los interesados en un procedimiento administrativo, tal y como se recoge en el artículo 9.1 de la Ley 39/2015, mediante la comprobación de su nombre y apellidos que consten en el Documento Nacional de Identidad o documento identificativo equivalente.

Esta obligación de la Administración de verificar la identidad no implica necesariamente que se tenga que exigir y recoger la fotocopia del DNI del interesado por lo que se debe examinar cada caso concreto a la hora de determinar los requisitos y documentos que son necesarios aportar para la realización de una actuación administrativa, ya que en algunos supuestos y con relación a determinados procedimientos, podría sustituirse la fotocopia del DNI o documento equivalente, como ha señalado el Comité Europeo de Protección de Datos como buena práctica, que el responsable del tratamiento, después de comprobar el documento de identidad, anote, por ejemplo, *“Se ha comprobado el documento de identidad”* para evitar la copia o el almacenamiento innecesario de copias del documento de identidad.

Por otra parte, la persona reclamante manifiesta que la solicitud del DNI y la fotocopia del mismo sucede *“...Todo esto una y otra vez, da igual que vayas para solicitar una cita por escrito, una queja...cualquier escrito que haces ante ellos, te cogen la documentación y la fotocopian”*, es decir, a su entender dicha actuación se produce de forma generalizada.

Sin embargo, de la documentación obrante en el expediente, no se constata de forma fehaciente que Osakidetza-Svs requiera, como señala la persona reclamante, siempre y de forma generalizada para cualquier trámite que se pretenda realizar fotocopia del DNI, por lo que no existe en este caso una justificación indiciaria razonable que permita tramitar un expediente sancionador.

Este expediente fue objeto de recurso de reposición RR24-010, el cual fue desestimado.





- **Presunta utilización de datos personales tras haber sido beneficiario de asistencia jurídica gratuita (DN24-023)**

En su escrito a la AVPD, el reclamante plantea la posibilidad de que el Departamento de Igualdad, Justicia y Políticas Sociales del Gobierno Vasco esté recogiendo y tratando sus datos económicos y financieros de seguros.

Por su parte, la Delegada de Protección de Datos del Gobierno Vasco informa que el Departamento no está tratando datos económicos y financieros de seguros del reclamante y que los únicos datos personales que se han tratado fueron los necesarios para resolver la solicitud de justicia gratuita instada por el reclamante. Una vez concedido este derecho, ni se han recabado ni se han tratado más datos y así se le ha hecho saber al reclamante.

A la vista de que no existe ninguna evidencia de que se haya producido ningún tratamiento más allá de los relacionados con la tramitación del derecho de justicia gratuita, no cabe constatar ninguna infracción y se procede archivar la reclamación.

- **Tratamiento de datos recabados por los arcos de detección de dispositivo de Telepeaje (DN24-047)**

El reclamante denuncia que se está monitorizando a los vehículos que disponen de un dispositivo de telepeaje a través de los arcos que la Sociedad Pública Foral ha instalado en la carretera A-8 en Bizkaia, lo que va en contra de su intimidad y protección de datos, y que la Sociedad Pública Foral al disponer de sus datos que previamente le facilitó, puede conocer de esa forma ser la persona que circula con su coche por la vía.

Se archiva la denuncia porque el tratamiento de datos personales de los titulares de los vehículos que pasan por la citada vía está amparado en la Norma Foral 7/2022, de 20 de julio.

El tratamiento de los datos personales relativos a los vehículos no obligados al pago del canon (entre ellos, la imagen de la matrícula, el medio de pago vinculado o el alta o registro en el sistema Free Flow) se realiza para poder excluirlos de aquellos vehículos que sí están obligados (vehículos pesados), no pudiendo destinarse a finalidades distintas a las que prevé la Norma Foral, y sólo podrán tratarse durante el tiempo estrictamente necesario para descartar la obligación de pago del canon derivado del uso del eje viario.

La información particular que dispone la Sociedad Pública Foral de determinados usuarios es recabada no en aplicación de la Norma Foral 7/2022, sino que ha sido aportada por los usuarios al realizar su registro en la base de datos de Interbiak, con el fin de acogerse a subvenciones que otorga anualmente la Diputación Foral de Bizkaia o al solicitar la emisión de facturas que en su caso realicen.

4.3 PROCEDIMIENTOS DE INFRACCIÓN DE LAS ADMINISTRACIONES PÚBLICAS

Son los procedimientos que se incoan a las Administraciones e Instituciones Públicas de esta Comunidad Autónoma, cuando existen indicios de que su conducta pudiera



ser constitutiva de infracción en materia de protección de datos de carácter personal. Finalizan con el archivo o, en su caso, con apercibimiento y requerimiento de adopción de medidas correctoras.

En el año 2024 se han incoado 31 nuevos procedimientos y se han resuelto un total de 28, con el siguiente resultado: se han declarado 28 apercibimientos.

- **Notificación a persona no autorizada de la resolución de reconocimiento de grado de dependencia del interesado (PI23-015)**

En el procedimiento tramitado queda acreditado que personal de un Instituto Foral de Bienestar Social de Álava entregó a una persona no autorizada una resolución de reconocimiento de dependencia, referida al padre de la persona denunciante.

Se apercibe al Instituto Foral por una infracción del principio de integridad y confidencialidad proclamado en el artículo 5.1.f) del Reglamento General de Protección de Datos.

- **Instalación irregular de cámaras de videovigilancia en instalaciones municipales (PI23-020)**

El Ayuntamiento de Zambrana instaló cámaras de videovigilancia en la entrada y fachada del Ayuntamiento, el Txikipark, el frontón municipal, así como en las piscinas municipales, realizando un tratamiento de datos personales a través de imágenes en algunos casos sin cartel informativo ni la adopción de medidas de seguridad.

Se apercibe al Ayuntamiento de Zambrana por vulneración del principio de transparencia, del principio de licitud y del principio de confidencialidad proclamado en el artículo 5 del Reglamento General de Protección de Datos, conducta constitutiva de tres infracciones previstas en el artículo 83.5 a) del RGPD. No se le requiere que adopte medidas correctivas ya que el Ayuntamiento Zambrana desde que tuvo conocimiento y control de los sistemas de videovigilancia instalados adoptó medidas oportunas para reducir la afección a la privacidad.

- **Notificación de memoria explicativa íntegra a todos los solicitantes de un proceso de provisión por el sistema de libre designación (PI23-022)**

En un procedimiento de provisión de un puesto de trabajo, Osalan-Instituto Vasco de Seguridad y Salud Laboral, comunicó a todos los participantes en dicho procedimiento, la memoria explicativa de imposibilidad de adjudicar el puesto objeto de provisión, en la que se contenían apreciaciones muy desfavorables para el denunciante.

Se apercibe a Osalan-Instituto Vasco de Seguridad y Salud Laboral por una infracción del principio de integridad y confidencialidad proclamado en el artículo 5.1.f) del Reglamento General de Protección de Datos.





- **Acceso indebido a historia clínica y falta de colaboración (PI23-023)**

Se denuncia a Osakidetza-Svs por una multiplicidad de accesos indebidos a su historia clínica y a la de su hijo, menor de edad, por parte de personal de Osakidetza- Servicio vasco de salud, sin su conocimiento, consentimiento, ni habilitación legal.

De la documentación obrante en el expediente se constata que, durante el año 2022, a través de los programas informatizados de historias clínicas, se realizaron diferentes accesos a la historia clínica de la reclamante y de su hijo menor por personal de Osakidetza-Servicio vasco de salud, sin contar con su consentimiento y sin que estos accesos hayan quedado justificados por actuación asistencial.

Se resuelve apercibir a Osakidetza-Servicio vasco de salud por vulneración del principio de integridad y confidencialidad establecido en el artículo 5.1.f) del Reglamento General de Protección de Datos y se le requiere para que adopte las medidas organizativas necesarias para dar cumplimiento al principio de confidencialidad e integridad, comunicándolas en el plazo de un mes a esta autoridad

- **Utilización de los servicios Google Workspace for Education en centros docentes de la CAE (PI23-025)**

El Departamento de Educación del Gobierno Vasco y Google suscribieron un convenio para la utilización de los servicios Google WorkSpace For Education en los centros docentes del Departamento de Educación, y para su implementación la Administración reclamada no realizó una evaluación de impacto relativa a la protección de datos. Los datos personales de los usuarios finales de la plataforma (docentes y alumnado) pueden ser tratados por Google para el uso de servicios adicionales que no son objeto del Convenio. En los distintos registros de actividades tratamiento dependientes del Departamento de Educación publicados en la página web del Gobierno Vasco, no consta información en la que se prevea el tratamiento de datos personales que supone la ejecución de la citada plataforma educativa. El procedimiento se resuelve por la AVPD con tres apercibimientos por tres conductas infractoras: por haber infringido el artículo 35 del RGPD, lo que constituye una infracción prevista en el artículo 83.4.a) del RGPD; por haber infringido el principio de lealtad y transparencia proclamado en el artículo 5.1.a) del RGPD, lo que constituye una infracción prevista en el artículo 83.5.a) del RGPD por haber infringido el artículo 30 del RGPD y el artículo 30 de la LOPDGDD, lo que constituye una infracción prevista en el artículo 83.4 a) del RGPD y en el artículo 74 l) de la LOPDGDD.

- **Publicación de datos personales en página web dentro de un proceso selectivo (PI23-026)**

En la página web de la Diputación Foral de Bizkaia a la que acceden los aspirantes a una convocatoria de un proceso selectivo se hicieron públicos determinados datos personales de la persona reclamante (número completo de su DNI, domicilio y



teléfono), por lo que el responsable vulneró el principio de minimización de datos consagrado en el artículo 5.1 c) del RGPD, ya que tan sólo era necesario conocer la identidad del aspirante que recurría un acto del tribunal, es decir lo estrictamente necesario para dicha finalidad.

La vulneración de dicho principio constituye una infracción prevista en el artículo 83.5 a) del RGPD, por lo que se apercibió a la Administración reclamada por dicha infracción, reconociendo una menor reprochabilidad de su conducta por la rapidez en que resolvió la eliminación de los datos excesivos. No fue necesario que la autoridad requiriese la adopción de medidas organizativas internas porque ya fueron adoptadas.

- **Acceso con el certificado digital de la FNMT otorgado para la representación de una empresa, a la carpeta de salud de la persona física que ostenta el apoderamiento de la sociedad (PI23-027)**

Con el certificado digital de la Fábrica Nacional de Moneda y Timbre otorgado para la representación de una empresa, se accede a la carpeta de salud de la persona física que ostenta el apoderamiento de la sociedad. Asimismo, Osakidetza no ha dado respuesta a los requerimientos realizados por la AVPD para esclarecer los hechos denunciados.

Osakidetza es el responsable del tratamiento de datos y quien decide sobre los medios de identificación electrónica que se pueden utilizar en su sede electrónica. Por lo tanto, es responsable también de adoptar las medidas técnicas y organizativas que aseguren que los certificados sólo pueden ser utilizados para cumplir las finalidades para las que son concedidos.

Sin embargo, no se han tomado las medidas necesarias para evitar que con el certificado digital de la Fábrica Nacional de Moneda y Timbre otorgado, la persona física que ostenta el apoderamiento de la sociedad acceda a su carpeta de salud, lo que supone una vulneración del principio de integridad y confidencialidad.

Se apercibe a Osakidetza por infracción del principio de integridad y confidencialidad y por su falta de cooperación con la AVPD, requiriendo que adopte las medidas organizativas necesarias para garantizar el cumplimiento de sus obligaciones respecto a la responsabilidad proactiva y a la colaboración con la AVPD y las comunique en el plazo de un mes.

- **Comunicación de su teléfono particular a una pluralidad de terceros (PI23-28)**

Se denuncia a Osakidetza-Svs por el envío a una pluralidad de personas de un correo electrónico con el listado de los médicos que forman parte de la plantilla de un hospital, con su nombre, apellidos y teléfono personal.

De las actuaciones y documentos que obraban en el expediente resultó acreditado que, por parte de Osakidetza, sin previa autorización ni consentimiento de la reclamante se remitió a través un correo electrónico, un listado en el que se incluía su nombre y apellidos con su número de teléfono personal, al resto de médicos que



realizaban guardias en el hospital, a pesar de que la reclamante, como el resto de médicos contenidos en el listado remitido, contaba con un número de teléfono corporativo facilitado por la organización para estar localizados. Igualmente, por parte de Osakidetza-Servicio vasco de salud no se contestó a ninguno de los requerimientos efectuados por esta Agencia Vasca de Protección de Datos a lo largo de todo el procedimiento.

Se resuelve apercibir a Osakidetza-Servicio vasco de salud por vulneración del principio de integridad y confidencialidad establecido en el artículo 5.1.f) del Reglamento General de Protección de Datos, constitutiva de una infracción tipificada en el artículo 83.5 a) del mismo texto legal, apercibirle igualmente por infracción del artículo 83.4.a) del RGPD, por falta de colaboración con la autoridad y requerirle que adopte las medidas organizativas necesarias para garantizar el cumplimiento de sus obligaciones respecto a la responsabilidad proactiva y a la colaboración con la AVPD en el ejercicio de sus funciones, comunicándolas en el plazo de un mes a esta autoridad de control.

- **Tratamiento de datos personales en la tramitación de solicitud de ambulancias y falta de colaboración (PI24-001)**

Se denuncia que al solicitar una ambulancia se tratan datos pertenecientes a las personas que prestan el servicio lo que pudiera ser una infracción de la normativa de protección de datos.

En el procedimiento tramitado quedaron acreditados los hechos denunciados constatándose que la plataforma “Osabide Integra” perteneciente a Osakidetza-Svs mediante la que se solicitan las ambulancias por las residencias de ancianos, trata datos relativos a nombre y apellidos del solicitante, así como su DNI, siendo visibles en el volante que se obtiene en la tramitación.

Se resuelve apercibiendo a Osakidetza-Servicio vasco de salud por haber vulnerado el principio de minimización del artículo 5.1.c) del Reglamento General de Protección de Datos, apercibiéndole igualmente por infracción del artículo 83.4.a) del RGPD por no colaborar con esta Autoridad de control y requiriéndole que adopte las medidas organizativas necesarias para dar cumplimiento al principio de minimización, así como garantizar el cumplimiento de sus obligaciones respecto a la responsabilidad proactiva y a la colaboración con la AVPD en el ejercicio de sus funciones, debiendo comunicarlas en el plazo de un mes a esta autoridad.

- **Tratamiento de datos sanitarios excesivos: Vulneración del principio de minimización en datos sanitarios, remisión al Juzgado de datos excesivos, y falta de colaboración (PI24-002)**

Se denuncia que en contestación a un oficio se remite al Juzgado, por parte de Osakidetza, una extensa documentación, entre ella 5 informes de atención primaria y la Historia Clínica resumida del reclamante, documentación que no había sido solicitada por el Juzgado y que contenía patologías que nada tenían que ver con lo que se discutía en el proceso, habiéndole requerido el Juzgado únicamente la documentación relativa a una patología concreta.



En el procedimiento tramitado quedaron acreditados los hechos denunciados e igualmente se constata que el propio Juzgado consideró excesivo el envío de dicha documentación ya que determinó que lo remitido excedía de lo solicitado y decidió eliminarlo del procedimiento.

Se resuelve apercibiendo a Osakidetza-Servicio vasco de salud por haber vulnerado el principio de minimización del artículo 5.1.c) del Reglamento General de Protección de Datos, apercibiéndole igualmente por infracción del artículo 83.4.a) del RGPD por no colaborar con esta Autoridad de control y requiriendo a Osakidetza-Servicio vasco de salud para que adopte las medidas organizativas necesarias para dar cumplimiento al principio de minimización, así como garantizar el cumplimiento de sus obligaciones respecto a la responsabilidad proactiva y a la colaboración con la AVPD en el ejercicio de sus funciones, debiendo comunicarlas en el plazo de un mes a esta autoridad.

- **Utilización de documentación protegida del reclamante en procedimiento judicial: Vulneración del principio de exactitud, y falta de colaboración (PI24-003)**

El reclamante denuncia a Osakidetza-Svs por el acceso y utilización por parte de uno de sus letrados de documentación protegida (últimas voluntades) sin tener habilitación legal para ello, en la contestación a una demanda presentada por el reclamante relativa a un procedimiento judicial que nada tenía que ver con las mismas.

De la documentación obrante en el expediente se constata que por parte de Osakidetza-servicio vasco de salud se accedió y se reveló, sin conocimiento ni consentimiento de un paciente y sin tener habilitación legal para ello, las últimas voluntades del mismo, haciéndose referencia expresa a las mismas en la contestación a una demanda presentada por el reclamante relativa a un procedimiento judicial que no tenía ninguna relación con las últimas voluntades del paciente, al tratarse de un proceso que versaba sobre la información que debe facilitarse a un paciente antes de realizar cualquier acto médico. Igualmente, por parte de Osakidetza-Servicio vasco de salud no se contestó a ninguno de los requerimientos efectuados por esta Agencia Vasca de Protección de Datos a lo largo de todo el procedimiento.

Se resuelve apercibir a Osakidetza-Servicio vasco de salud por vulneración del principio de integridad y confidencialidad establecido en el artículo 5.1.f) del Reglamento General de Protección de Datos. Se le apercibe igualmente por infracción del artículo 83.4.a) del RGPD por no colaborar con esta Autoridad de control y se le requiere para que adopte las medidas organizativas necesarias para dar cumplimiento al principio de confidencialidad e integridad, así como garantizar el cumplimiento de sus obligaciones respecto a la responsabilidad proactiva y a la colaboración con la AVPD en el ejercicio de sus funciones, debiendo comunicarlas en el plazo de un mes a esta autoridad.





- **Tratamiento indebido de historia clínica (PI24-004)**

Se presenta escrito en el que se denuncia que se ha tratado indebidamente su historia clínica para contestar a una carta suya publicada en un periódico.

De las actuaciones y documentos que obran en el expediente resulta acreditado que por parte de la Consejería de Salud se utilizó el contenido de la Historia Clínica de la reclamante para contestar a una carta publicada en un medio de comunicación en la que se quejaba de la situación sanitaria de Osakidetza-Servicio vasco de salud en general (de las listas de espera para operaciones quirúrgicas, del número de camas de hospital cerradas durante el verano...) utilizando y tratando para contestar datos de la historia clínica de la reclamante respecto de los que no ha existido consentimiento ni legitimación legal para ello.

Se resuelve apercibir al Departamento de Salud del Gobierno Vasco por vulneración del principio de legitimación recogido en el artículo 5.1 a) del RGPD, lo que constituye una infracción prevista en el artículo 83.5.a) del mismo texto legal y requerirle para que adopte las medidas organizativas tendentes a evitar en el futuro situaciones como las referidas en este procedimiento.

- **Cesión indebida de historia clínica (PI24-005)**

Se presenta escrito en el que se denuncia a Osakidetza-Svs por tratar indebidamente su historia clínica al cederla al Departamento de Salud para contestar a una carta suya publicada en un periódico.

De las actuaciones y documentos que obran en el expediente resulta acreditado que por parte de personal de Osakidetza-Servicio vasco de salud se accedió, a través de sus programas informatizados, a la historia clínica de la reclamante sin su consentimiento, conocimiento ni habilitación legal y se cedió la información a la Consejería de Salud del Gobierno Vasco para contestar a una carta suya publicada en un medio de comunicación.

Se resuelve apercibir a Osakidetza-Servicio vasco de salud por vulneración del principio de integridad y confidencialidad de datos recogido en el artículo 5.1. f) del Reglamento General de Protección de Datos, constitutiva de una infracción tipificada en el artículo 83.5 a) del mismo texto y requerirle para que adopte las medidas organizativas tendentes a evitar en el futuro situaciones como las referidas en este procedimiento.

- **Acceso y utilización sin consentimiento de datos obtenidos de la historia clínica (PI24-008)**

La recogida de datos personales por el Servicio Vasco de Salud tiene como objetivo la asistencia sanitaria de la población. Sin embargo, en este caso, un auxiliar de enfermería ha utilizado la dirección de correo personal y el número de teléfono para ponerse en contacto con la reclamante sin que medie ningún fin relacionado con una prestación sanitaria. Por lo tanto, ese tratamiento de datos no tiene cobertura legal y supone una vulneración del principio de limitación de la finalidad.



Por otra parte, Osakidetza no ha dado respuesta a ninguno de los requerimientos de información realizados por parte de la AVPD para el esclarecimiento de los hechos, ni durante la tramitación de la denuncia, ni durante la tramitación del expediente de infracción posterior.

En consecuencia, se apercibe a Osakidetza por ambas cuestiones y se propone que inicie actuaciones disciplinarias contra el auxiliar de enfermería, instando a que comunique la apertura o no del expediente disciplinario, cuestión que no ha confirmado hasta la fecha.

- **Publicación de fotografía en el buzón del ciudadano de un Ayuntamiento (PI24-009)**

Se denuncia que en el Buzón del Ciudadano, alojado en la página web del Ayuntamiento de Vitoria, hay publicada una queja a la que se adjuntó una fotografía en la que aparece identificada la persona reclamante.

Se apercibe a la Administración reclamada por vulneración del principio de confidencialidad del artículo 5.1 f) del RGPD y en el artículo 5 de la LOPDGDD, conducta constitutiva de una infracción prevista en el artículo 83.5 a) del RGPD, y no se le requiere la adopción de medidas organizativas por haber sido adoptadas en el transcurso del procedimiento.

- **Reenvío del correo electrónico por el que la reclamante solicita la baja de una newsletter (PI24-010)**

La reclamante remitió un correo electrónico a la UPV/EHU con el objeto de darse de baja de una newsletter, siendo posteriormente reenviado a todos los destinatarios de la misma sin su consentimiento, vulnerando de esta forma el principio de confidencialidad contenido en el artículo 5.1 f) del RGPD. Se apercibe a la UPV/EHU.

- **Publicación en portal corporativo de datos personales y profesionales (PI24-011)**

La parte reclamante denuncia que el Departamento de Seguridad del Gobierno Vasco publicó, a efectos de notificación, en el portal corporativo Gurenet una resolución dirigida al reclamante en la que constaban su nombre y apellidos, número de identificación profesional, situación de incapacidad por enfermedad común con indicación del comienzo de la misma, y destino que venía ocupando. La Administración reclamada reconoce que únicamente debía haber sido notificada a la persona interesada, así como a su Jefatura de Unidad, a los efectos de la organización de los servicios policiales.

Se apercibe a la Administración reclamada por infracción de los principios de licitud y del principio de confidencialidad, lo que constituye una infracción del artículo 83.5 a) del RGPD, y se requiere al responsable para que adopte las medidas organizativas necesarias para dar cumplimiento a los principios vulnerados y las que sean oportunas a fin de que en el futuro no se reitere esta conducta.



- **Acceso indebido a historia clínica y falta de colaboración (PI24-012)**

Se denuncia a Osakidetza-Svs por una multiplicidad de accesos indebidos a su historia clínica durante los años 2020, 2021 y 2022 por parte de personal de Osakidetza-Servicio vasco de salud, sin su conocimiento, consentimiento, ni habilitación legal.

En el procedimiento tramitado se constata que, durante los años 2021 y 2022, a través de los programas informatizados de historias clínicas Osabide Global y Osabide Primaria, hubo diferentes accesos a la historia clínica de la reclamante por personal de Osakidetza-Servicio vasco de salud, sin contar con el conocimiento ni consentimiento de la persona afectada y sin que estos accesos hayan quedado justificados por actuación asistencial. Igualmente, por parte de Osakidetza-Servicio vasco de salud no se contestó a ninguno de los requerimientos efectuados por esta Autoridad Vasca de Protección de Datos a lo largo de todo el procedimiento.

Se resuelve apercibir a Osakidetza-Servicio vasco de salud por vulneración del principio de integridad y confidencialidad establecido en el artículo 5.1.f) del Reglamento General de Protección de Datos, se le apercibe igualmente por infracción del artículo 83.4.a) del RGPD por no colaborar con esta Autoridad de control y se le requiere para que adopte las medidas organizativas necesarias para dar cumplimiento al principio de confidencialidad e integridad, así como garantizar el cumplimiento de sus obligaciones respecto a la responsabilidad proactiva y a la colaboración con la AVPD en el ejercicio de sus funciones, comunicándolas en el plazo de un mes a esta autoridad.

- **Vulneración del deber de cumplimentar el encargo correspondiente (PI24-013)**

Se denuncia la instalación de cámaras de videovigilancia en las Ambulancias por la empresa adjudicataria del contrato de servicio de transporte de emergencias del Departamento de Salud del Gobierno.

Se apercibe al Departamento de Salud del Gobierno Vasco por vulneración del artículo 28 del RGPD (por no haber cumplimentado el encargo correspondiente con la empresa adjudicataria), conducta constitutiva de una infracción prevista en el artículo 83.4 a) del RGPD.

- **Recepción de carta con datos personales en la ventanilla del sobre (PI24-014 y PI24-016)**

El Ayuntamiento de Basauri envía cartas a las reclamantes en la que, junto al nombre y apellidos de la persona destinataria, aparece el número del documento de identidad, que resulta visible en la ventanilla del sobre.

El Ayuntamiento reconoce la existencia de un error informático que ha permitido que ocurra este hecho y, por lo tanto, cabe constatar la vulneración del principio de confidencialidad por lo que se apercibe a la institución. Asimismo, no corresponde dictar la adopción de medidas correctoras puesto que se ha corregido el error informático que dio lugar a la infracción.



- **Recepción de carta con dato de salud visible (PI24-015)**

La Diputación Foral de Gipuzkoa envía una carta a la reclamante en la que queda a la vista en la ventanilla del sobre la alusión “*falta de documentación para la valoración de la discapacidad*”. El dato sobre discapacidad es un dato de salud; es decir, una de las categorías de datos especialmente protegida cuyo tratamiento está prohibido según el artículo 9.1 del RGPD, con las excepciones establecidas en el segundo apartado del mismo artículo.

La Diputación Foral de Gipuzkoa reconoce la comisión de la infracción por lo que se le apercibe por vulnerar el principio de confidencialidad. No se acuerdan medidas correctoras ya que la propia Diputación, al tener conocimiento de la reclamación, se ha dirigido al servicio informático para pedirle que haga un cambio en la plantilla del texto, de forma que la mención al objeto de las notificaciones no se pueda ver a través de la ventanilla de los sobres.

- **Remisión de escrito por parte de Etxebide a la dirección anterior de la reclamante (PI24-017)**

La reclamante solicita un cambio de dirección postal a la Dirección de Planificación y Procesos Operativos de Vivienda del Gobierno Vasco pero este cambio no se produce y, en consecuencia, se envía una carta a su anterior dirección postal. La institución reclamada reconoce su responsabilidad en no haber cambiado la dirección postal de la reclamante. Asimismo, tras la reclamación ha cambiado la dirección postal en su base de datos y ha comunicado la subsanación a la reclamante.

Por otra parte, cabe destacar que la Dirección de Planificación y Procesos Operativos de Vivienda del Gobierno Vasco ha tomado medidas destinadas a evitar que casos similares puedan producirse en el futuro, implantando un sistema de doble aviso que advierta a las personas encargadas de la tramitación de solicitudes de modificación de datos. Por esta razón, la resolución no insta a la adopción de medidas correctoras y se limita reconocer la vulneración del principio de exactitud, razón por la que se apercibe a Etxebide.

- **Acceso indebido a historia clínica (PI24-018)**

Se denuncia a Osakidetza-Svs por una multiplicidad de accesos indebidos a su historia clínica durante los años 2019 a 2023 por parte de personal de Osakidetza-Servicio vasco de salud, sin su conocimiento, consentimiento ni habilitación legal

En el procedimiento tramitado se constata que durante los años 2022 y 2023, a través de los programas informatizados de historias clínicas, ha habido al menos tres accesos a la historia clínica de la persona reclamante por personal de Osakidetza-Servicio vasco de salud, sin contar con su consentimiento y sin que estos accesos hayan quedado justificados por actuación asistencial.

Se resuelve apercibir a Osakidetza-Servicio vasco de salud por vulneración del principio de integridad y confidencialidad establecido en el artículo 5.1.f) del Reglamento General de Protección de Datos y se le requiere para que adopte las





medidas organizativas necesarias para dar cumplimiento al principio de confidencialidad e integridad, comunicándolas en el plazo de un mes a esta autoridad.

- **Acceso indebido a historia clínica y falta de colaboración (PI24-019)**

Se denuncia a Osakidetza-Svs por una multiplicidad de accesos indebidos a su historia clínica de 24 de febrero de 2022 a 30 de noviembre de 2023 por parte de personal de Osakidetza-Servicio vasco de salud, sin su conocimiento, consentimiento ni habilitación legal

En el procedimiento tramitado se constata que, durante el año 2022, a través de los programas informatizados de historias clínicas, hubo diferentes accesos a la historia clínica de la persona reclamante por personal de Osakidetza-Servicio vasco de salud, sin contar con su consentimiento y sin que estos accesos hayan quedado justificados por actuación asistencial.

Se resuelve apercibir a Osakidetza-Servicio vasco de salud por vulneración del principio de integridad y confidencialidad establecido en el artículo 5.1.f) del Reglamento General de Protección de Datos y se le requiere para que adopte las medidas organizativas necesarias para dar cumplimiento al principio de confidencialidad e integridad, comunicándolas en el plazo de un mes a esta autoridad.

- **Vulneración del principio de minimización y falta de colaboración (PI24-021)**

Se denuncia al Ayuntamiento de Zalla por trasladar, completo y con todos los datos personales del reclamante que constan en el mismo, un recurso de reposición interpuesto contra varios actos de aprobación de listas definitivas de un proceso de consolidación.

De la documentación obrante en el expediente se constata que el Ayuntamiento de Zalla realizó traslado de alegaciones a los interesados de un recurso de reposición interpuesto por el reclamante frente a la aprobación de listas definitivas de procesos de consolidación incluyendo sus datos personales como nombre y apellidos, número de DNI, su dirección postal, dirección de correo electrónico, así como datos relativos a su firma electrónica. Igualmente, no contestó a ninguno de los requerimientos realizados por esta Autoridad a lo largo del procedimiento de infracción.

Se resuelve apercibir al Ayuntamiento de Zalla por haber vulnerado el principio de minimización del artículo 5.1.c) del Reglamento General de Protección de Datos, apercibiéndole igualmente por infracción del artículo 83.4.a) del RGPD por no colaborar con esta Autoridad de control y requiriéndole a que adopte las medidas organizativas necesarias para dar cumplimiento al principio de minimización, así como garantizar el cumplimiento de sus obligaciones respecto a la responsabilidad proactiva y a la colaboración con la AVPD en el ejercicio de sus funciones, debiendo comunicarlas en el plazo de un mes a esta autoridad.



- **Envío de correo electrónico en el que se adjunta un archivo con datos personales de 905 personas (PI24-022)**

Denuncian que el Ayuntamiento de Portugalete envió un correo electrónico en el que se adjuntaba un archivo Excel con datos personales (nombre, apellidos, DNI, dirección y correo electrónico) de 905 personas, no estando los destinatarios del correo electrónico enviado legitimados para acceder a toda la información contenida en el archivo adjunto.

Se apercibe al Ayuntamiento de Portugalete por vulneración del principio de confidencialidad recogido en el artículo 5.1 f) del Reglamento General de Protección de Datos, conducta constitutiva de una infracción prevista en el artículo 83.5 a) del RGPD.

- **Comunicación de datos bancarios a tercero (PI24-025)**

Se presenta escrito de reclamación en el que se denuncia al Ayuntamiento de Vitoria-Gasteiz por la remisión a un tercero de la cuenta bancaria del denunciante.

De las actuaciones y documentos que obran en el expediente resulta acreditado que el Ayuntamiento de Vitoria-Gasteiz comunicó a un tercero el número de cuenta bancaria del reclamante para abonar unas cantidades pendientes de cobro.

Se resuelve apercibir al Ayuntamiento de Vitoria-Gasteiz por haber infringido el principio de confidencialidad proclamado en el artículo 5.1 f) de y se le requiere para que adopte las medidas organizativas internas tendentes a evitar en el futuro situaciones como las referidas en este procedimiento, debiendo notificarlas a esta Autoridad en el plazo de un mes desde la notificación de la resolución.

4.4 AUTOS Y SENTENCIAS

Durante el año 2024 los Juzgados y Tribunales se han pronunciado respecto al siguiente asunto:

- **Inclusión de fotografías tomadas en parcela privada en un expediente administrativo municipal (DN23-016)**

Las imágenes tratadas constituyen elementos probatorios en los que se funda la denuncia urbanística. La Ley 2/2006, de 30 de junio, de Suelo y Urbanismo establece como principios generales del urbanismo en la CAPV el principio de participación ciudadana y el de información pública. El artículo 8.2 c) recoge que el principio de participación comportará el derecho a: “Ejercer en vía administrativa y judicial, sin necesidad de legitimación especial, las acciones pertinentes para exigir de las administraciones públicas y de los sujetos privados el cumplimiento de la legislación y la ordenación urbanística”. El tratamiento de datos personales denunciado en el presente caso es acorde al principio de licitud establecido por el art. 5.1 a) del RGPD.

Contra la resolución de archivo el reclamante interpuso Recurso de Reposición (RR23-009) que fue desestimado por entenderse que el tratamiento de datos



personales denunciado es acorde al principio de licitud establecido por el art. 5.1 a) del RGPD al concurrir un interés legítimo por el autor de las fotografías para el ejercicio de la acción pública urbanística. La Resolución del Recurso de Reposición se ha recurrido ante la Jurisdicción contencioso-administrativa.

Finalmente, en febrero de 2024 el Juzgado de lo Contencioso-Administrativo declara la inadmisibilidad del recurso por falta de legitimación activa.



5 EL REGISTRO DE PERSONAS DELEGADAS DE PROTECCIÓN DE DATOS

El Reglamento (UE) 679/2016 General de Protección de Datos (RGPD) Reglamento UE-2016/379 RGPD contempla, en su artículo 37.1, la obligación de designación de Delegado de Protección de Datos (DPD-DBO) cuando los tratamientos de datos personales sean llevados a cabo por una **autoridad u organismo público**. Asimismo, el artículo 37.7 establece la obligación de comunicar los datos de contacto a la Autoridad de control correspondiente.

Si bien el RGPD prevé la designación de DPD-DBO tanto para responsables como para encargados de tratamiento, teniendo en cuenta el actual ámbito competencial de la AVPD, establecido por la *Ley 16/2023 de 21 de diciembre, de la Autoridad Vasca de Protección de Datos*, los sujetos obligados son los establecidos en su ámbito de aplicación (artículo segundo).

Es necesario destacar que en marzo de 2022 se produjo un cambio en la forma de comunicación de DPD-DBO por parte de las administraciones públicas de la CAE. Hasta dicha fecha la comunicación se realizaba mediante la cumplimentación de un formulario pdf y su posterior remisión por correo electrónico a la AVPD. Con posterioridad, se hace mediante un trámite telemático, accesible en la página web de la AVPD.

Asimismo, durante el año 2023 se ha modificado el trámite telemático para que se pueda comunicar la designación de delegado de protección de datos tanto a personas físicas como a entidades jurídicas, comités, y grupos de trabajo (para estos tres últimos tipos se debe designar una persona de contacto).

El número de solicitudes de comunicación de datos (alta, modificación de datos de contacto de DPD, cese) y las solicitudes que finalmente han sido inscritas en el año 2024 se refleja en la siguiente tabla:

Tipo de solicitud	Comunicados	Inscritos
Alta	99	88
Modificación datos contacto de DPD	1	1
Cese	3	2
Total	103	91

El resumen general en cuanto a número de Entidades y Organismos Públicos que han realizado la comunicación de los datos de contacto de sus DPD-DBO al finalizar 2024 se presenta en el siguiente cuadro:

TIPO DE ADMINISTRACIÓN	DPD-DBOs COMUNICADOS
Instituciones autonómicas	91
Instituciones forales	35
Instituciones locales	270
Otros Organismos	60
Total	456



El número total de DPD registrados ha pasado de 389 en 2023 a 456 en 2024, lo que supone un incremento del 17,22%.

5.1 ADMINISTRACIÓN LOCAL

Con respecto de los Ayuntamientos, la distribución del número de ayuntamientos y personas delegadas comunicadas, según los estratos de población, es la siguiente:

HABITANTES	AYUNTAMIENTOS	DPD-DBOs	%
< 500	60	45	75,00%
500 - 999	38	32	84,21%
1.000 - 4.999	81	69	85,19%
5.000 - 9.999	29	27	93,10%
10.000 - 19.999	24	21	87,50%
20.000 - 49.999	14	14	100,00%
50.000 - 99.999	2	2	100,00%
> 100.000	4	4	100,00%
Total	252	214	84,92%

Con respecto al año 2023, el número de ayuntamientos que ha comunicado el DPD-DBO a la AVPD ha pasado de 202 a 214, lo que supone un incremento del 5,94%.

5.2 VINCULACIÓN DE LOS RESPONSABLES DE TRATAMIENTO CON SUS DPD-DBO

La relación de la persona delegada de protección de datos con la entidad Responsable de Tratamiento puede ser:

- interno:
 - persona física
 - grupo de trabajo o comité
- externo:
 - autónomo
 - empresa

La distribución de los DPD-DBO designados, atendiendo a la naturaleza de su relación de empleo (interno: persona física, grupo de trabajo o comité; externo: autónomo, empresa) con el Responsable de Tratamiento ha sido la siguiente:

Interno		Externo	
Persona física	Grupo de Trabajo / Comité	Autónomo	Empresa
113	5	30	308
118		338	
Total		456	



La distribución de los DPD-DBO designados, atendiendo al territorio histórico es la siguiente:

Araba	Bizkaia	Gipuzkoa
94	207	155
Total	456	

La distribución de los DPD-DBO designadas, atendiendo a la naturaleza de su relación de empleo (interno o externo) con el Responsable de Tratamiento, según el tipo de administración, es la siguiente:

TIPO DE ADMINISTRACIÓN	DPD-DBOs	Interno	Externo	% Interno
Instituciones autonómicas	91	36	55	39,56%
Instituciones forales	35	11	24	31,43%
Instituciones locales	270	61	209	22,59%
Otros Organismos	60	10	50	16,67%
Total	456	118	338	25,88%

Una cuarta parte de las Administraciones Públicas Vascas han optado por la designación de DPD-DBO interna, ya sea de la propia plantilla o de otra Entidad Pública.

Si centramos el análisis en los DPD-DBO designadas por las corporaciones locales, atendiendo al tamaño de su población, en los ayuntamientos de más de 50.000 habitantes es mayoritaria la designación de la DPD-DBO interna, mientras que en aquellos que no llegan a 20.000 han acudido a la contratación de los servicios de una DPD-DBO externa:

HABITANTES	DPD-DBOs	Interno	Externo	% Interno
< 500	45	16	29	35,56%
500 - 999	32	9	23	28,13%
1.000 - 4.999	69	10	59	14,49%
5.000 - 9.999	27	2	25	7,41%
10.000 - 19.999	21	3	18	14,29%
20.000 - 49.999	14	6	8	42,86%
50.000 - 99.999	2	1	1	50,00%
> 100.000	4	4		100,00%
Total	214	51	163	23,83%

Todavía 38 de los 252 ayuntamientos (el 15,07% del total) no han cumplido con la obligación legal de comunicar la persona DPD-DBO a la Autoridad Vasca de Protección de Datos.



6 LA NOTIFICACIÓN DE BRECHAS DE SEGURIDAD

El Reglamento (UE) 679/2016 General de Protección de Datos (RGPD) Reglamento UE-2016/379 RGPD contempla, en su artículo 33 (Notificación de una violación de la seguridad de los datos personales a la autoridad de control), que tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una brecha de datos personales debe efectuar la correspondiente notificación a la Autoridad de Control competente, cuando sea probable que la brecha constituya un riesgo para los derechos y libertades de las personas; en su caso, debe realizarse sin dilación y a más tardar en las 72 horas siguientes, computando también las horas transcurridas durante fines de semana y festivos.

Durante el año 2024 se han notificado 20 brechas de seguridad de datos personales (una notificación NO procede), sabiendo que estas notificaciones de brechas de seguridad de datos personales pueden ser del tipo iniciales (9), completas (4), y complementarias (6).

TIPO DE NOTIFICACIÓN	EXPLICACIÓN
Inicial	Cuando en el momento de la notificación no fuese posible cumplir con la obligación de facilitar toda la información necesaria, se prevé la posibilidad de realizar una notificación de tipo INICIAL, rellenando el formulario electrónico con la información preliminar que se disponga, o en su caso las estimaciones preliminares sobre la brecha de seguridad de datos personales.
Completa	Cuando en el momento de la notificación se disponga de toda la información relevante para la gestión y resolución de la brecha de seguridad de datos personales, incluida la decisión sobre la comunicación de la brecha a las personas afectadas, se realizará una notificación de tipo COMPLETA, dado que no está previsto que el responsable de tratamiento tenga que aportar información adicional.
Complementaria	Antes del plazo máximo de 30 días desde la notificación inicial, el responsable de tratamiento deberá completar toda la información mediante una notificación de tipo COMPLEMENTARIA, incluida la decisión tomada sobre la comunicación de la brecha de datos personales a las personas afectadas.

El resumen general en cuanto a número de Entidades y Organismos Públicos según el tipo de administración que han realizado notificaciones de brechas de seguridad al finalizar 2024 se presenta en el siguiente cuadro:



TIPO DE ADMINISTRACIÓN	BRECHAS NOTIFICADAS
Instituciones autonómicas	4
Instituciones forales	3
Instituciones locales	11
Otros Organismos	1
Total	19

Nivel de severidad de la brecha y consecuencias para las personas afectadas:

NIVEL DE SEVERIDAD	BRECHAS NOTIFICADAS
Muy alta	Las personas pueden enfrentar consecuencias muy significativas, o incluso irreversibles, que no pueden superar (exclusión o marginación social, dificultades financieras tales como deudas considerables o incapacidad para trabajar, dolencias psicológicas o físicas a largo plazo, muerte, etc.). Daña derechos fundamentales y libertades públicas de forma irreversible.
Alta	Las personas pueden enfrentar consecuencias significativas, que deberían poder superar, aunque con serias dificultades (malversación de fondos, listas negras de los bancos, daños a la propiedad, pérdida de empleo, citación judicial, empeoramiento de la salud, etc.). En general cuando las consecuencias afectan a derechos fundamentales, pero pueden revertirse.
Media	Las personas pueden encontrar inconvenientes importantes, produciendo un daño limitado, que podrán superar a pesar de algunas dificultades (costos adicionales, denegación de acceso a servicios comerciales, miedo, falta de comprensión, estrés, dolencias físicas menores, etc.)
Baja	Las personas no se verán afectadas o pueden encontrar algunos inconvenientes muy limitados y reversibles que superarán sin ningún problema (tiempo de reingreso de información, molestias, irritaciones, etc.)

El resumen general en cuanto al nivel de severidad de la brecha y consecuencias para las personas afectadas para con la notificación de brechas de seguridad al finalizar 2024 se presenta en el siguiente cuadro:



NIVEL DE SEVERIDAD	NÚMERO DE BRECHAS NOTIFICADAS
Muy alta	0
Alta	2
Media	2
Baja	15
TOTAL	19

En cuanto a la comunicación de las brechas a las personas físicas interesadas, cuando la brecha de datos personales entrañe un alto riesgo para los derechos y libertades de las personas afectadas, además de la notificación a la Autoridad de Control, se deberá comunicar a los afectados la brecha de datos personales sin dilación indebida, además, dicha comunicación se debe realizar con un lenguaje claro y sencillo, de forma concisa y transparente. El parámetro determinante para notificar una brecha de datos personales a la Autoridad de Control o comunicarla a los afectados es el nivel de riesgo. No cualquier tipo de riesgo o un riesgo para la organización, sino específicamente el riesgo para los derechos y libertades de las personas físicas afectadas por la brecha.

El resumen general en cuanto a las comunicaciones de las brechas de seguridad de datos personales a las personas físicas interesadas al finalizar 2024 se presenta en el siguiente cuadro:

COMUNICACIÓN DE LA BRECHA A LAS PERSONAS INTERESADAS	NÚMERO DE BRECHAS
SI, COMUNICADA	14
NO COMUNICADA	5
PENDIENTE DE DECIDIR	0
TOTAL	19



7 FORMACION IMPARTIDA POR EL PERSONAL DE LA AVPD

Como ya se indica en la Ley 16/2023, de 21 de diciembre, entre las funciones muy diversas de la Autoridad Vasca de Protección de Datos, le corresponde como competencia la formación en protección de datos personales, por cuanto deberá promover la difusión de las disposiciones contenidas en la normativa de protección de datos personales, con la finalidad de garantizar el adecuado conocimiento tanto por la ciudadanía de su derecho fundamental a la protección de tales datos, como por los responsables de las obligaciones que las normas les imponen para respetarlo.

En ese sentido, el personal de la AVPD ha participado en múltiples acciones de difusión y formación destinadas a dar a conocer a la ciudadanía los nuevos derechos reconocidos en el RGPD y a expandir una conciencia pública acerca del valor de la privacidad y la necesidad de que ésta sea escrupulosamente respetada en el quehacer diario de entidades del Sector Público Vasco.

Este es un resumen de algunas de las formaciones impartidas por personal de la AVPD durante el 2024:

- Impartición del “Curso específico para Referentes de Protección de Datos de la Administración General de la CAE (enero).
- Módulo de transparencia y acceso a la información pública del Master de Experto en Derecho Digital 2023-2024, Universidad de Deusto (febrero)
- Participación en la XXI reunión del foro de Seguridad y Protección de Datos de Salud celebrado en Toledo (febrero).
- Ponencia en la Facultad de Empresariales de Mondragon Unibertsitatea - “Conceptos Generales de la normativa de Protección de Datos” (febrero).
- VIII Jornada Abierta de Administración Local y Protección de Datos, Biscaytik (abril)
- Módulo de protección de datos del Master Universitario de Acceso a la Abogacía de la Universidad de Deusto y del Ilustre Colegio de la Abogacía de Bizkaia (abril).
- Participación como ponente en el Título Propio Experto en Organización y Gestión de Servicios Sanitarios, organizado por la Universidad Pública de Navarra y el Departamento de Salud del Gobierno de Navarra (abril).
- Ponencia en el Colegio de Abogados de Bizkaia sobre videovigilancia y videovigilancia policial (mayo).
- Participación como ponente en las Jornadas de la Asociación de administrativos sanitarios celebrada en Tarragona (mayo).
- Arabako Foru Aldundia- Impartición del curso “Reglamento General de Protección de Datos” (mayo).



- Gipuzkoako Foru Aldundia - Impartición del curso “Datu pertsonalen babesa. Europako Erregelamendua eta Lege Organikoa.” (octubre/noviembre).
- La protección de datos de carácter personal desde la transparencia, Diputación Foral de Álava (octubre).
- IVAP (modalidad online)- “Taller práctico sobre la aplicación de la protección de datos personales en la Administración Pública” (noviembre).
- Hedatu, primer encuentro vasco de Delegadas de Protección de Datos (noviembre).
- XVI Jornada de seguridad y protección de datos, presentación de la ponencia “La protección de datos en el ámbito de la ingeniería informática”. UPV / Escuela de Ingeniería de Vitoria-Gasteiz (diciembre).



8 CENTRO DOCUMENTACION

A continuación, se analizan las actividades relacionadas con la gestión de la información y documentación del Centro de Documentación de la Autoridad Vasca de Protección de Datos (AVPD), destacando su rol tanto en la gestión directa como en la colaboración con otros actores dentro de la institución. El Centro de Documentación, creado en febrero de 2009, actúa como un centro especializado en la recopilación, organización y difusión de información vinculada a áreas como protección de datos, transparencia, seguridad informática y acceso a la información, así como en temas generales de la administración pública y electrónica. La gestión de la información proporciona a la AVPD un conocimiento profundo de su entorno y facilita una adecuada planificación estratégica y la correcta distribución de la información dentro de la organización.

El 2024 ha sido un año de transición con avances en diversas áreas clave, como la gestión de la información, la difusión de contenidos y la integración de la AVPD en nuevos canales de comunicación y medios. También se mencionan algunos retos y problemas, como los asociados con la migración de herramientas y la necesidad de actualizar y mejorar procesos internos.

8.1 PRINCIPALES ACCIONES EN EL ÁREA DE DOCUMENTACIÓN

A lo largo de 2024, el Centro de Documentación ha desarrollado diversas acciones clave en la gestión y difusión de la información. Entre las iniciativas más relevantes se encuentra la implementación de un Sistema de Gestión Documental (SGD), que se encuentra en fase de desarrollo, y la transferencia de documentación de 2022 al archivo, con un total de 162 expedientes transferidos.

- **Sistema de Gestión Documental y Archivo.** En 2024 se avanzó en la definición de herramientas documentales clave, como cuadros de clasificación y calendarios de conservación. Aunque el desarrollo completo del sistema se encuentra aún en progreso, se han realizado los primeros análisis sobre el estado de la cuestión del sistema de gestión documental y archivo.
- **Boletines Informativos.** Además, el Centro de Documentación mantiene diversos boletines informativos para el personal de la AVPD, tales como el boletín diario de noticias, gestionado con la empresa Ubermetrics. En 2024 se redefinieron las sentencias de búsqueda y se actualizaron las fuentes de información. Además, se ha seguido gestionando el boletín "Legesarea", que ofrece acceso a referencias de boletines oficiales y noticias jurídicas de interés.
- **Boletín de Difusión Selectiva de Información.** Hasta 2024, se elaboraba un boletín mensual con información proactiva de interés para el personal. Sin embargo, debido a la implicación del equipo en nuevos proyectos, este boletín ha



sido reducido a la distribución descentralizada de información relevante a medida que se recibe.

- **Dictámenes e Informes de Legalidad.** A lo largo de 2024, el equipo ha publicado 55 documentos, entre dictámenes y resoluciones, en la web institucional, contribuyendo así a la difusión de la normativa y directrices de la AVPD.
- **Servicio de Acceso al Documento.** El Centro de Documentación también ha facilitado el acceso a documentos relevantes para el personal, incluyendo artículos de investigación y monografías. Durante 2024, se suministraron 16 documentos por préstamo interbibliotecario y se resolvieron 8 consultas personalizadas.
- **Bases de Datos Bibliográficas.** El Centro continúa utilizando Refworks como gestor bibliográfico, aunque han surgido ciertos inconvenientes con la nueva versión de la herramienta. Estos problemas se encuentran pendientes de resolución, ya que no se ha priorizado su solución. Por otro lado, la colaboración con la base de datos Dialnet sigue activa, permitiendo la actualización continua de los contenidos relacionados con las áreas de interés de la AVPD.

8.2 GESTIÓN DOCUMENTAL

- **Sistema de Gestión Documental (SGD):** Se ha trabajado en la incorporación de un sistema electrónico para la tramitación de expedientes, aunque los avances en 2024 fueron limitados. También se han transferido al archivo 162 expedientes finalizados en 2022.
- **Boletines diarios de noticias:** Se han seguido gestionando boletines diarios, tales como el Boletín de la AVPD y el Legesarea, con la colaboración de empresas externas y actualizaciones de las herramientas de búsqueda y clasificación.
- **Difusión selectiva de información:** Aunque la elaboración de boletines proactivos ha disminuido por la implicación del personal en otros proyectos, se ha mantenido la distribución de revistas y artículos según las herramientas disponibles.
- **Base de datos bibliográfica (Refworks):** Se han identificado problemas tras la migración de la herramienta y, aunque no se ha abordado la solución, se mantienen pendientes varios documentos para su inclusión en la base de datos.
- **Fondo Bibliográfico:** Se ha gestionado la adquisición de 15 monografías y se ha realizado un proceso de expurgo de 32 obras de la colección. También se ha trabajado en la integración de términos de búsqueda en el catálogo colectivo de la Red de Lectura Pública de Euskadi.
- **Formación:** Se ha proporcionado formación sobre herramientas como Ubermetrics-Delta, bases de datos profesionales como Aranzadi y Mementix Administrativo, así como cursos sobre gestión documental y e-administración.



8.3 COMUNICACIÓN

- **Página web:** Se ha colaborado en la reestructuración de la página web de la AVPD, con actualizaciones de información y contenido tras la entrada en vigor de la Ley 16/2023. La renovación del diseño está en marcha con la contratación de una empresa externa.
- **Redes sociales:** Se ha incrementado la actividad en X (anteriormente Twitter) y LinkedIn, con un notable aumento en la frecuencia de publicaciones y en la cantidad de seguidores.
- **Medios de comunicación:** La presencia en prensa ha aumentado, con 45 apariciones en medios de comunicación. Destaca la colaboración con el programa “Consumidores” de Radio Vitoria, con el cual se ha comenzado a emitir un espacio mensual.
- **Wikipedia:** Se ha colaborado en la mejora de las entradas de la AVPD y su presidente, Unai Aberasturi, en Wikipedia.

8.4 HERRAMIENTAS DE TRABAJO

- Se ha creado una carpeta en **SharePoint** específica para la comunicación, recopilando recursos como bases de datos de medios de comunicación, aplicaciones útiles para la creación de contenidos y un vocabulario controlado en euskera y castellano.
- **Modelos y plantillas:** Se ha renovado la plantilla y los modelos de documentos genéricos de la organización, adaptándolos a la nueva identidad visual corporativa.

8.5 OTROS PROYECTOS

Este resumen presenta las acciones realizadas en 2024, destacando el trabajo en comunicación, gestión documental y organización de eventos importantes:

- **HEDATU, Comunidad de Delegadas y Delegados de Protección de Datos.** HEDATU es más que una plataforma informática; es un espacio de encuentro y desarrollo profesional para Delegados de Protección de Datos (DPD). Su principal objetivo es crear una comunidad sólida donde los DPD puedan conectarse, compartir experiencias y colaborar eficazmente. La plataforma ofrece herramientas, recursos y una red de expertos a los que los DPD pueden recurrir.

Las funcionalidades de HEDATU incluyen:

- **Foros de debate:** Espacios para plantear dudas y discutir temas de interés común.
- **Acceso a recursos especializados:** Material documental sobre protección de datos.
- **Agenda:** Información sobre eventos relevantes.





- **Espacios de colaboración:** Herramientas para trabajar en equipo.
- **Red de contactos:** Un directorio profesional para facilitar la cooperación entre DPD.

El servicio de documentación ha colaborado activamente en el diseño, parametrización y carga inicial de recursos en la plataforma, estructurando los contenidos por categorías y proporcionando ejemplos de buenas prácticas.

- **I Encuentro Vasco de DPD.** Este evento se celebró el 18 de noviembre de 2024 en Bilbao, con el propósito de promover la formación y el networking entre profesionales del ámbito de la protección de datos. Durante este encuentro, se presentaron casos prácticos, estrategias de gestión de brechas de seguridad, y la plataforma HEDATU. El servicio de documentación participó en la organización, encargándose de aspectos logísticos, como la solicitud de presupuestos, la elección de proveedores y la gestión de la imagen del evento.
- **Gala 20º Aniversario de la AVPD.** En 2024, la Autoridad Vasca de Protección de Datos celebró su 20º aniversario. La celebración culminará con una gala en el Palacio Euskalduna, programada para el 27 de febrero de 2025. El servicio de documentación ha estado involucrado en la organización del evento, gestionando tareas como la elección de proveedores, la definición de la agenda y la gestión de las invitaciones.

8.6 MEDIOS DE COMUNICACIÓN

A continuación se presenta un resumen de las principales apariciones de la Autoridad Vasca de Protección de Datos en medios de comunicación durante el 2024:

- 7 de enero, El Correo: <https://www.elcorreo.com/alava/araba/llega-quejas-accesos-indebidos-historiales-osakidetza-20240107003330-nt.html?edtn=alava&vca=fixed-btn&vso=rrss&vmc=tw&vli=alava/araba>
- 8 de enero, Bizkaia Gaur: <https://www.bizkaia.gaur.com/2024/01/05/16-2023-legea-abenduaren-21ekoa-datuak-babesteko-euskal-agintaritzarena-indarrean-sartu-da/>
- 18 de enero, En Jake: <https://x.com/i/status/1747965576742416623>
- 18 de enero, RTVEuskadi: <https://x.com/i/status/1748005319219843091>
- 19 de enero, Gaur Egun y Teleberri: (vídeo no disponible)
videovigilancia 22 de enero, Faktoria: <https://www.eitb.eus/eu/irratia/euskadi-irratia/programak/faktoria/oso/9404064/unai-aberasturi-kaleetako-kamerak-jartzeko-justifikazio-bat-behar-da-eta-gardentasuna-ere-bai/>



- 25 de enero, Gaur Egun y Teleberri: worldcoin25 de enero, GanbaraEITB:
<https://www.eitb.eus/es/radio/radio-euskadi/programas/ganbara/detalle/9406650/unai-aberasturi-estas-perdiendo-por-completo-control-sobre-informacion-que-se-refiere-a-tu-persona/>
- 25 de enero, Más de uno Álava:
https://www.ondacero.es/emisoras/pais-vasco/vitoria/mas-de-uno-alava/mas-uno-alava-susana-marques-24012024_2024012465b10aced8aa250001d886ce.html
- 29 de enero, Diario Vasco:
<https://www.diariovasco.com/#/sociedad/publico-fotos-hijos-instagram-puedo-decir-hagan-20240127065708-nt.html?vca=fixed-btn&vso=rrss&vmc=tw&vli=sociedad>
- 29 de enero, Hoy por hoy Bizkaia:
https://cadenaser.com/audio/ser_bilbao_hoyporhoybizkaia_20240129_082004_083000/
- 30 de enero, Egun On: (vídeo no disponible) entrevista larga, varios temas de actualidad
- 31 de enero, Cadena Ser:
<https://cadenaser.com/euskadi/2024/01/31/por-lo-que-nos-dicen-varias-personas-no-se-esta-informando-debidamente-sobre-el-uso-que-estando-a-los-datos-biometricos-radio-bilbao/>
- 1 de febrero, Quédate con Ane:
<https://www.eitb.eus/es/television/programas/quedate-con-ane/videos/detalle/9412085/unai-aberasturi-merece-pena-ceder-parte-de-lo-que-somos-por-pocos-euros/>
- 6 de febrero, Deia:
<https://www.deia.eus/bizkaia/2024/02/03/expertos-alertan-riesgo-escanear-iris-7824190.html>
- 6 de febrero, ABC: <https://www.abc.es/espana/pais-vasco/quiere-guardar-iris-creador-chatgpt-20240205180834-nt.html?vca=compartirrrss&vso=abc&vmc=rrss&vli=fixed-twitter>
- 12 de febrero, Deia:
<https://www.deia.eus/bizkaia/2024/02/11/bilbao-cuenta-265-camaras-getxo-7858206.html>



- 13 de febrero, Onda Vasca: <https://www.ondavasca.com/programas/onda-vasca-con-kike-alonso/>
- 21 de febrero, Noticias de Gipuzkoa: <https://www.noticiasdegipuzkoa.eus/sucesos/2024/02/19/aler-tan-estafa-tarjeta-mugi-7893373.html>
- 21 de febrero, En Jake: estafa con Mugi y Bat
- 6 de marzo, Cadena Ser: <https://cadenaser.com/euskadi/2024/03/06/la-agencia-de-proteccion-de-datos-ordena-bloquear-la-captacion-de-datos-biometricos-a-worldcoin-radio-bilbao/>
- 6 de marzo, Financial Times: <https://www.ft.com/content/204c1c81-7a6f-4a6a-907e-8782b9d1bed2>
- 7 de marzo, Quédate con Ane: worldcoin
- 7 de marzo, Teleberri: worldcoin
- 7 de marzo, En Jake: worldcoin
- de marzo, Naiz: https://irratia.naiz.eus/eu/info_irratia/20240312/datu-pertsonalek-osatzen-duten-negozioa-gero-eta-handiagoa
- de marzo, Cadena Ser: [Colectivos antirracistas estudian unirse a la denuncia por la filtración de las fichas policiales en Aste Nagusia. "¿En manos de quien estamos?" | Actualidad | Cadena SER](#)
- 18 de marzo, Gara: [«Datuek osatzen duten negozioa gero eta handiagoa da» | Euskal Herria | GARA Euskal Herriko egunkaria](#)
- 21 de marzo, EITB noticias: [Unai Aberasturi: 'En la decisión ha prevalecido el interés público, el contenido y la libertad de información'](#)
- 25 de marzo, Diario Vasco: [«Es normal que no se aplicase el 'derecho al olvido' al asesino de Nagore Laffage» | El Diario Vasco](#)
- 25 de marzo, Diario Vasco: [La extensión de cámaras en la calle en Euskadi dispara las quejas por posibles abusos en videovigilancia | El Diario Vasco](#)
- 27 de marzo, Quédate con Ane: videovigilancia
- 30 de abril, Gaur Egun y Teleberri: estafas por whatsapp
- 3 de mayo, Dirección asistida: [Dirección asistida \(2023-2024\) \(01/05/2024\): Unai Aberasturi, coches de la Zarzuela, BH y Seat Ibiza](#)
- 19 de junio, Euskadi Irratia: [Unai Aberasturi: "Herritarrok kontziente izan behar dugu sare sozialetaz egiten dugun erabileraz"](#)



- 25 de junio, Cadena Ser: ["Tenemos que comprender que WhatsApp no es una herramienta para niños" | Sociedad | Cadena SER](#)
- 3 de julio, Quédate: APP antiporno
- 17 de julio, Diario Vasco: [Las llamadas comerciales siguen sin fin | El Diario Vasco](#)
- 19 de julio, Naiz: mensaje tranquilizador ante la caída de Microsoft 31 de julio, Boulevard: [Boulevard \(31/07/2024\)](#)
- 1 de agosto, Radio Euskadi: [Audio: Entrevista a Unai Aberasturi, Presidente de la Autoridad Vasca de Protección de Datos](#)
- 30 de agosto, Boulevard: cámaras en taxis de Vitoria
- 21 de octubre, Consumidores (saldremos el 3º sábado de cada mes)
- 21 de noviembre, Radio Vitoria: [La Autoridad Vasca de Protección de Datos pone en marcha la red HEDATU](#)

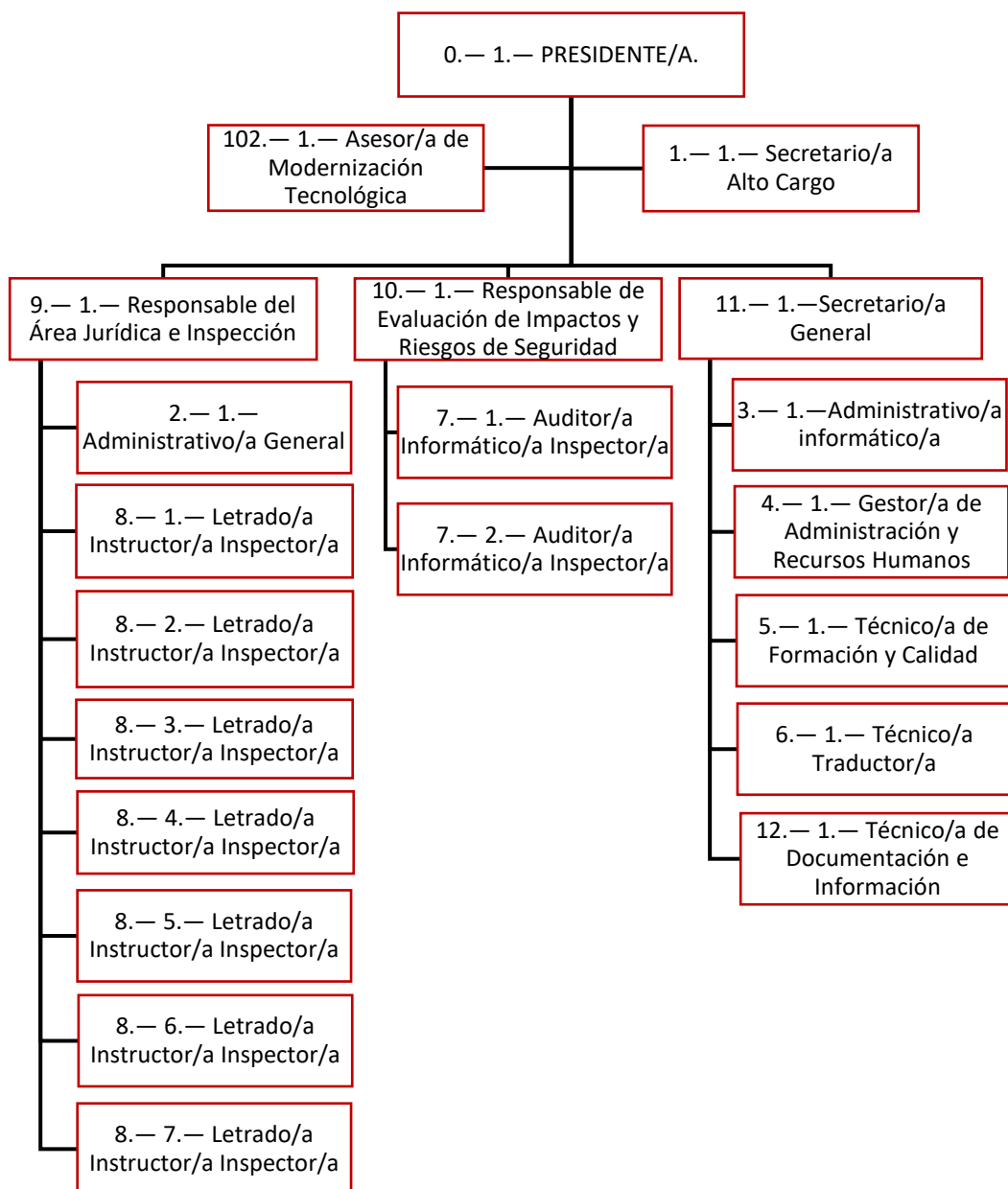




9 GESTIÓN INTERNA

9.1 ESTRUCTURA Y PLANTILLA DE PERSONAL

9.1.1 Plantilla de Personal





9.1.2 Estructura orgánica y relaciones de puestos de trabajo

Dentro del nuevo marco normativo de las Autoridades de Protección de Datos merecen especial mención el Reglamento UE 2016/679, del Parlamento Europeo y del Consejo, del 27 de abril, relativo a las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), la posterior aprobación de la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDyGDD), y la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales,

La actual estructura orgánica, fue aprobada por Resolución de 29 de marzo de 2023, de la entonces Directora de la Agencia Vasca de Protección de Datos.

Como consecuencia de la modificación de la estructura orgánica, se llevó a cabo la actualización de la Relación de Puestos de Trabajo de la AVPD adecuándola a las necesidades generadas por las nuevas normas jurídicas aprobadas en el ámbito de la protección de datos, de forma que reflejara tales cambios, y fue aprobada por Resolución de 25 de mayo de 2023.

Por último, la actual relación de puestos de trabajo de personal eventual de la Autoridad Vasca de Protección de Datos se aprobó por Resolución de 18 de septiembre de 2023, del Director.

9.1.3 Plan para la Ordenación de Recursos Humanos

El Plan para la Ordenación de los Recursos Humanos, aprobado por Resolución de 28 de junio de 2024, del Presidente de la Autoridad Vasca de Protección de Datos, viene a articular y organizar los recursos humanos a disposición de la Institución, y hacer frente a los nuevos retos que tanto las nuevas normativas que van surgiendo en materia de protección de datos, como la continua irrupción de tecnologías emergentes para la gestión de los procesos de la información plantean.

En ejercicio de la previsión establecida en la disposición transitoria tercera de la ley 16/2023, de 21 de diciembre, sobre la integración del personal funcionario de la Agencia Vasca de Protección de Datos en los cuerpos y escalas del personal funcionario de la Autoridad Vasca de Protección de Datos, en base a su situación a la entrada en vigor de dicha ley, por Resolución de 28 de junio de 2024, del Presidente de la AVPD, se reguló y convocó el procedimiento para la integración del personal funcionario en los nuevos cuerpos y en las escalas creados por esa ley.

Dicho proceso se dio por finalizado por Resolución de 30 de julio de 2024, del Presidente de la Autoridad Vasca de Protección de Datos.

9.1.4 Jornada laboral y horarios.

En el marco del cumplimiento de la jornada laboral y los horarios establecidos para el ejercicio 2024, como una forma facilitar la conciliación laboral y personal se ha continuado con la flexibilización de los horarios de la jornada laboral y el trabajo



en entorno domiciliario, minimizando además el estrés generado por los desplazamientos, además de evitar la presencia masiva de personas en los centros de trabajo. Estas medidas ya se contemplaban en el Plan de Contingencia por Riesgo de Exposición a Coronavirus SARS-CoV-2, elaborado en 2020.

La experiencia llevada a cabo en esta Autoridad está resultando, con carácter general, satisfactoria, tanto como medida preventiva, como en el desempeño de la actividad y la adecuada prestación del servicio, generando una mayor productividad.

9.2 PRESUPUESTOS

El artículo 13 de la Ley 2/2004, de 25 de febrero, establecía que *“La Agencia Vasca de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno Vasco para que sea integrado, con la debida independencia, en los Presupuestos Generales de la Comunidad Autónoma, de acuerdo con la legislación reguladora del régimen presupuestario de la Comunidad Autónoma del País Vasco”*.

Mediante Resolución de 23 de octubre de 2023, del Director de la Agencia Vasca de Protección de Datos, se aprobó el anteproyecto de presupuesto para el año 2024, y se llevó a cabo su remisión al Gobierno Vasco para su integración, con la debida independencia, en los Presupuestos Generales de la CAPV.

Así, la Ley 21/2023, de 22 de diciembre, por la que se aprueban los Presupuestos Generales de la Comunidad Autónoma de Euskadi para el ejercicio 2024, establecía en su artículo 1.4. que *“Se aprueba e incorpora, a los efectos contemplados en el artículo 13 de la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, el presupuesto de la Agencia Vasca de Protección de Datos”*.

9.2.1 Ejecución presupuestaria

PRESUPUESTO DE GASTOS

CAPÍTULO	DENOMINACIÓN DE LOS CAPÍTULOS	Créditos Totales	Obligaciones Reconocidas	Pagos Realizados	Pendiente de Pago	Estado de Ejecución
1	Gastos de Personal	2.496.050,00	1.377.029,47	1.350.851,33	26.178,14	55,17%
2	Gastos en Bienes Corrientes y Servicios	576.100,00	223.038,89	185.112,37	37.926,52	38,72%
4	Transferencias Corrientes	9.000,00	5.000,00		5.000,00	55,56%
6	Inversiones Reales	92.000,00	78.970,20	18.549,30	60.420,90	85,84%
	Suma Total Gastos.	3.173.150,00	1.684.038,56	1.554.513,00	129.525,56	53,07%



PRESUPUESTO DE INGRESOS

CAPÍTULO	DENOMINACIÓN DE LOS CAPÍTULOS	Previsiones Definitivas	Derechos Netos	Ingresos Realizados	Pendiente de Cobro	Estado de Ejecución
3	Tasas y Otros Ingresos		1.918,85	1.918,85		100,00%
4	Transferencias Corrientes	2.713.148,00	2.713.148,00	2.713.148,00		100,00%
5	Ingresos Patrimoniales		105.906,03	80.346,55	25.559,48	75,87%
6	Enajenación de inversiones reales		1.887,60	1.887,60		100,00%
7	Transferencias de Capital	15.000,00	15.000,00	15.000,00		100,00%
8	Activos Financieros	445.002,00				
	Suma Total Ingresos.	3.173.150,00	2.837.860,48	2.812.301,00	76.678,44	99,10%

9.2.2 Control económico-financiero y contable

La AVPD está sometida al régimen de contabilidad pública y al control económico financiero y de gestión del Departamento de Hacienda y Finanzas de la Administración General de la Comunidad Autónoma, sin perjuicio de la fiscalización de sus actividades económico-financieras y contables por el Tribunal Vasco de Cuentas Públicas.

La verificación de la adecuada gestión económico financiera y de gestión de la AVPD conforme a las disposiciones y directrices que deben regir la actuación económica de la misma, se viene realizando por la Oficina de Control Económico del señalado Departamento del Gobierno Vasco, mediante auditorías financieras anuales.

• Auditoría 2023

Las cuentas anuales correspondientes al ejercicio 2023, presentadas junto con la Memoria de cumplimiento de los objetivos programados, fueron auditadas con fecha 26 de marzo de 2024. El informe final de auditoría indica que:

“...las cuentas anuales adjuntas expresan, en todos - los aspectos significativos, la imagen fiel del patrimonio y de la situación financiera de la Entidad a 31 de diciembre de 2023, así como de sus resultados y flujos de efectivo correspondientes al ejercicio terminado en dicha fecha, de conformidad con el marco normativo de información financiera que resulta de aplicación (que se identifica en la nota 6.3 de la memoria) y, en particular, con los principios y criterios contables contenidos en el mismo.

.....

Sobre la base del trabajo realizado, hemos determinado que no existen riesgos mas significativos que generen cuestiones claves considerados en la auditoría que se deban comunicar en nuestro informe.

.....

La información que contiene la memoria de cumplimiento de los objetivos concuerda con la de las cuentas anuales del ejercicio 2023 y su contenido y presentación son conformes a la normativa que resulta de aplicación.”



9.3 RECURSOS MATERIALES

9.3.1 Sede

La AVPD desarrolla su actividad en el Edificio Seminario, Beato Tomás de Zumárraga, 71, 3 planta, 01008 Vitoria-Gasteiz, hasta el 31 de marzo de 2023 con un contrato de subarriendo a EJIE S.A. para el uso de dichos locales.

A partir del 1 de abril la responsabilidad de la gestión del edificio “Seminario” corresponde a la Dirección de Recursos Generales y esta AVPD sigue prestado su actividad en los mismos locales, cuyo uso está cedido de forma gratuita.

9.3.2 Otros contratos menores

Para garantizar el funcionamiento de la AVPD se han realizado diferentes contrataciones, siendo las principales las referidas a:

- Mantenimiento de fotocopiadoras
- Adquisición de material y equipos de oficina
- Adquisición prensa, revistas y libros
- Servicio de comunicaciones postales
- Mantenimiento y explotación de aplicaciones informáticas
- Organización y participación en eventos
- Edición de la Memoria Anual
- Estudios e informes
- Nuevo diseño gráfico de la entidad
- Servicio de prevención ajeno
- Seguros de vida y accidentes del personal

9.3.3 Estructura tecnológica y mejora de aplicaciones

El Convenio Marco de colaboración suscrito entre la AVPD y EJIE y desarrollado a través de la respectiva Adenda de 2024, ha posibilitado la prestación de servicios y dotaciones informáticas y de comunicaciones, y continuar en la mejora de la estructura informática, tanto a nivel de hardware como de software.



9.4 POLÍTICA DE PREVENCIÓN DE RIESGOS LABORALES

9.4.1 Plan de Prevención de Riesgos Laborales

La Ley de Prevención de Riesgos Laborales establece deberes y obligaciones que implican una planificación de la Prevención que debe abarcar toda la actividad laboral de las organizaciones, y que la Autoridad Vasca de Protección de Datos ha asumido como nivel básico de actuación.

La Autoridad Vasca de Protección de Datos considera que la seguridad en el trabajo, la salud de sus personas y el cuidado y mejora de su entorno laboral son factores fundamentales en su gestión.

Desde esta perspectiva de consolidación y mejora de la acción preventiva, la AVPD tiene implantada la Política de Prevención de Riesgos Laborales, que desarrolla anualmente mediante la planificación y ejecución de acciones preventivas y correctoras, con carácter anual.

Durante el año 2024, los respectivos Planes de actuación se han concretado con las siguientes actuaciones

- Programa Anual de actividades en materia de Seguridad, Higiene y Ergonomía/Psicología.
 - Evaluación continua de riesgos laborales en el puesto de trabajo
 - Información al personal sobre los riesgos en el trabajo.
- Programa Anual del Plan de actuación en Vigilancia de la Salud.
 - Reconocimientos médicos

9.5 GESTIÓN SOSTENIBLE E IMPACTO AMBIENTAL

9.5.1 Gestión sostenible

Considerando la actividad a la que se dedica esta Entidad, la misma no tiene responsabilidades, gastos, activos, provisiones ni contingencias de naturaleza medioambiental que pudieran ser significativos en relación con su patrimonio, la situación financiera y los resultados de la misma.

Esta Entidad no es titular ni posee el control de derechos de emisión de gases de efecto invernadero.

En el funcionamiento ordinario de la Autoridad Vasca de Protección de Datos se aplican políticas de mejora en cuestiones sociales, medioambientales y económicas más allá de las obligaciones legales en el ejercicio de sus competencias.





10 DATOS RELATIVOS A LA ACTIVIDAD CONSULTIVA

Consultas

Año 2024		Número
Administración General de la Comunidad Autónoma del País Vasco	Departamento de Gobernanza pública y Autogobierno	1
Administración Foral y Administración Local	Diputación Foral de Gipuzkoa	1
	Instituto Foral de Bienestar Social. Álava	1
	Ayuntamiento de Bilbao	1
	Ayuntamiento de Barakaldo	1
	Ayuntamiento de Getxo	1
Otras entidades	Lanbide	1
NÚMERO TOTAL DE CONSULTAS RECIBIDAS		7

Dictámenes

Año 2024	Número
TOTAL DICTÁMENES EMITIDOS	7

Informes de legalidad

Año 2024	Número
Anteproyectos de Ley / proyectos de Decreto/ Órdenes	17
TOTAL INFORMES EMITIDOS	17



11 DATOS RELATIVOS A LA ACTIVIDAD DE CONTROL

Reclamaciones de tutela de derechos

Año 2024	Número
Tutelas recibidas	32
Tutelas resueltas	31

Denuncias

Año 2024	Número
Denuncias presentadas	84
Denuncias resueltas	74

Procedimientos de Infracción

Año 2024	Número
Procedimientos de infracción incoados	31
Procedimientos de Infracción resueltos	28



12 DATOS RELATIVOS A LA GESTION INTERNA

12.1 DATOS RELATIVOS A LA PLANTILLA PRESUPUESTARIA

La plantilla media de la Agencia en 2024, por categorías genéricas, ha sido la siguiente:

Categoría	Dotaciones	Plantilla media real
Presidente /a	1	1
Técnicos/as superiores	16	13,29
Administrativos/as	4	2
TOTAL	21	16,29

La distribución del personal de la plantilla al 31 de diciembre de 2024, por sexos, ha sido la siguiente:

Categoría	Mujeres	Hombres	Total
Presidente /a		1	1
Técnicos/as superiores	6	8	14
Administrativos/as	1	1	2
TOTAL	7	10	17

La variación de las plazas de la plantilla presupuestaria anual ha sido como sigue:

Plantilla por tipo personal y nivel	dic-24		dic-23	
	Dotación	Real	Dotación	Real
Altos Cargos				
Presidente /a	1	1	1	1
Personal Eventual				
Asesor/a nivel I-A / 28	1	1	1	1
Funcionarios				
Técnico/a superior nivel I-A / 28	3	1	3	2
Técnico/a superior nivel II-A / 27	2	2	2	2
Técnico/a superior nivel II-B / 27	7	7	7	7
Técnico/a superior nivel III-B / 25	2	1	2	1
Técnico/a superior nivel III-C / 25	1	1	1	1
Administrativo/a nivel IV-A / 22	1	1	1	1
Administrativo/a nivel V-A / 20	1	1	1	1
Administrativo/a nivel V-C / 20	1		1	
Secretario/a de alto cargo nivel VI-A / 18	1		1	
TOTAL	21	16	21	17



12.2 DATOS RELATIVOS A LA EJECUCIÓN PRESUPUESTARIA

12.2.1 Liquidación del Presupuesto

Presupuesto de gastos

Descripción	Créditos Presupuest. Definitivos	Obligaciones Reconocidas	Pagos	Obligacio. Pendientes de Pago a 31 de diciembre	% de Ejecución del Presupuesto	Obligaciones Reconocidas 2023
Retribuciones de Altos Cargos	99.815,00	84.679,47	84.679,47	—	84,84	89.791,20
Personal Eventual	78.193,00	77.023,36	77.023,36	—	98,50	52.469,39
Retribuciones de Funcionarios	1.724.187,00	979.725,23	979.725,23	—	56,82	942.097,14
Cotizaciones Sociales a cargo de la entidad	510.300,00	193.891,94	172.244,26	21.647,68	38,00	215.284,22
Aportaciones a sistemas complementarios pensiones	47.555,00	22.800,80	18.270,34	4.530,46	47,95	21.527,40
Formación y perfeccionamiento del personal	6.500,00	5.558,35	5.558,35	—	85,51	654,90
Acción Social	7.500,00	5.607,00	5.607,00	—	74,76	7.500,01
Seguros	22.000,00	7.743,32	7.743,32	—	35,20	8.147,95
Edificios y otras construcciones	286.500,00	—	—	—	—	—
Equipos para procesos de inform. y Aplicaciones informáticas	15.000,00	14.452,81	10.932,45	3.520,36	96,35	15.065,23
Edificios y otras construcciones	—	788,90	788,90	—	—	—
Mobiliario	10.000,00	193,00	193,00	—	1,93	5.497,26
Equipos de oficina	—	3.949,94	3.198,84	751,10	—	—
Equipos para procesos de información	—	—	—	—	—	59,99
Aplicaciones informáticas	141.100,00	72.080,00	41.756,09	30.323,91	51,08	117.526,25
Material de oficina	5.000,00	2.732,90	2.732,90	—	54,66	2.645,66
Prensa, revistas, libros y otras publicaciones	10.000,00	15.742,51	15.532,71	209,80	157,43	16.418,06
Comunicaciones postales y mensajería	4.000,00	1.091,02	1.002,90	88,12	27,28	1.091,16
Locomoción y gastos de estancia	18.000,00	44.387,90	42.054,75	2.333,15	246,60	17.713,31
Atenciones protocolarias y representativas	6.000,00	2.146,41	2.146,41	—	35,77	1.243,15
Comunicación institucional, publicidad y propaganda	18.000,00	—	—	—	—	—
Jurídicos y contenciosos	5.000,00	—	—	—	—	—
Reuniones, conferencias y cursos	15.000,00	46.999,84	46.943,34	56,50	313,33	4.898,67
Otros gastos diversos	—	6.313,16	5.669,58	643,58	—	10.067,36
Edición y distribución de publicaciones	10.000,00	1.028,50	1.028,50	—	10,29	—
Servicios bancarios y similares	—	—	—	—	—	31,00
Estudios, informes, consultoría	—	—	—	—	—	6.050,00
Trabajos técnicos y servicios de profesionales independiente	32.500,00	11.132,00	11.132,00	—	34,25	5.687,00
A empresas, familias e ISFL	9.000,00	5.000,00	—	5.000,00	55,56	—
Total de operaciones corrientes	3.081.150,00	1.605.068,36	1.535.963,70	69.104,66	52,09	1.541.466,31



Aplicaciones informáticas	80.000,00	69.483,80	9.062,90	60.420,90	86,85	53.341,71
Mobiliario	12.000,00	6.364,60	6.364,60	—	53,04	—
Equipos de oficina	—	—	—	—	—	3.291,20
Equipos para procesos de información	—	3.121,80	3.121,80	—	—	1.560,90
Total de operaciones de capital	92.000,00	78.970,20	18.549,30	60.420,90	85,84	58.193,81
Suma total	3.173.150,00	1.684.038,56	1.554.513,00	129.525,56	53,07	1.599.660,12

Presupuesto de ingresos

Descripción	Previsiones presupuestarias definitivas	Drchos Reconocidos	Recaudación Líquida	Derechos Pendientes de Cobro	% ejecución	Derechos reconocidos 2023
Otros ingresos de derecho privado	—	1.918,85	1.918,85	—	—	—
Intereses de cuentas corrientes bancarias	—	105.906,03	80.346,55	25.559,48	—	2.650.200,00
De la Administración General de la CAE	2.713.148,00	2.713.148,00	2.713.148,00	—	100,00	—
Total operaciones corrientes	2.713.148,00	2.820.972,88	2.795.413,40	25.559,48	104,04	2.650.200,00
De equipos de oficina	—	1.887,60	1.887,60	—	—	—
De la Administración General de la CAE	15.000,00	15.000,00	15.000,00	—	100,00	15.000,00
Remanentes de Tesorería	445.002,00	—	—	—	—	—
Total operaciones de capital	460.002,00	16.887,60	16.887,60	—	100,00	15.000,00
Suma Total	3.173.150,00	2.837.860,48	2.812.301,00	25.559,48	89,43	2.665.200,00

Resultado presupuestario

Conceptos	Derechos reconocidos netos	Obligaciones reconocidas netas	Resultado presupuestario ejercicio corriente	Resultado presupuestario ejercicio 2023
a) Operaciones corrientes	2.820.972,88	1.605.068,36	1.215.904,52	1.108.733,69
b) Operaciones de capital	16.887,60	78.970,20	(- 62.082,60)	(- 43.193,81)
I. RESULTADO PRESUPUESTARIO DEL EJERCICIO CORRIENTE (I=a+b)	2.837.860,48	1.684.038,56	1.153.821,92	1.065.539,88
RESULTADO PRESUPUESTARIO AJUSTADO	2.837.860,48	1.684.038,56	1.153.821,92	1.065.539,88



12.2.2 Liquidación de Presupuestos Cerrados

Descripción	Obligaciones pendientes de pago a 01/ene	Pagos realizados
Cotizaciones Sociales a cargo de la entidad	14.369,98	14.369,98
Aportaciones a sistemas complementarios pensiones	4.636,99	4.636,99
Formación y perfeccionamiento del personal	284,55	284,55
Equipos para procesos de información y Aplicaciones informáticas	2.410,54	2.410,54
Mobiliario	1.203,97	1.203,97
Aplicaciones informáticas	17.333,91	17.333,91
Material de oficina	26,58	26,58
Prensa, revistas, libros y otras publicaciones	189,2	189,2
Comunicaciones postales y mensajería	169,48	169,48
Locomoción y gastos de estancia	2.314,07	2.314,07
Trabajos técnicos y servicios de profesionales independiente	5.203,00	5.203,00
Aplicaciones informáticas	8.716,68	8.716,68
Equipos de oficina	3.291,20	3.291,20
Equipos para procesos de información	1.560,90	1.560,90
Obligaciones de presupuestos cerrados - 2023	61.711,05	61.711,05

12.2.3 Cuenta del Resultado Económico Patrimonial

	2024	2023
2. Transferencias y subvenciones recibidas	2.728.148,00	2.665.200,00
a) Del ejercicio	2.728.148,00	2.665.200,00
a.2) Transferencias	2.728.148,00	2.665.200,00
A) TOTAL INGRESOS DE GESTIÓN ORDINARIA (2+6)	2.728.148,00	2.665.200,00
8. Gastos de personal	(-1.375.110,62)	(-1.337.472,21)
a) Sueldos, salarios y asimilados	(-1.141.428,06)	(-1.084.357,73)
b) Cargas sociales	(-233.682,56)	(-253.114,48)
9. Transferencias y subvenciones concedidas	(-5.000,00)	
11. Otros gastos de gestión ordinaria	(-223.038,89)	(-203.994,10)
a) Suministros y servicios exteriores	(-223.038,89)	(-203.994,10)
12. Amortización del inmovilizado	(-42.655,63)	(-34.070,60)
B) TOTAL GASTOS DE GESTIÓN ORDINARIA (8+9+11+12)	(-1.645.805,14)	(-1.575.536,91)
I. Resultado (ahorro o desahorro) de la gestión ordinaria (A+B)	1.082.342,86	1.089.663,09
13. Deterioro de valor y resultados por enajenación del inmovilizado no financiero y activos en estado de venta	490,89	—
b) Bajas y enajenaciones	490,89	—
II. Resultado de las operaciones no financieras (I+13+14))	1.082.833,75	1.089.663,09
15. Ingresos financieros	105.906,03	—
b) De valores representativos de deuda, de créditos y de otras inversiones financieras	105.906,03	—
b.2) Otros	105.906,03	—
III. Resultado de las operaciones financieras (15+16+17+18+19+20+21)	105.906,03	—
IV. Resultado (ahorro o desahorro) neto del ejercicio (II+ III)	1.188.739,78	1.089.663,09



12.2.4 Inmovilizado

	Valores acumulados al final del ejercicio			Valores acumulados al inicio del ejercicio			Variaciones en el ejercicio		Amortizaciones en el ejercicio		Bajas netas
	V.A.F.E.			V.A.I.E.			V.E.		A.E.		
	V.A.F.E. Bruto	V.A.F.E. Amortiz.	V.A.F.E. Neto	V.A.I.E. Bruto	V.A.I.E. Amortiz.	V.A.I.E. Neto	V.E. Nuevo	V.E. Bajas	A.E. Año	A.E. Bajas	
Aplicaciones informáticas	774.103,43	635.485,33	138.618,16	704.619,63	596.740,36	107.879,27	69.483,80	—	38.744,97	—	—
Equipos de oficina	21.764,24	8.722,40	13.041,85	20.691,99	10.238,90	10.453,09	6.364,60	-5.292,35	2.379,14	-3.895,64	-1.396,71
Equipos informáticos	6.152,85	2.353,83	3.799,02	3.031,05	1.010,73	2.020,32	3.121,80	—	1.343,10	—	—
Mobiliario	160.751,52	160.353,80	397,72	160.751,52	160.247,08	504,44	—	—	106,72	—	—
Otras inversiones	5.005,80	5.005,80	—	5.005,80	5.005,80	—	—	—	—	—	—
Otros equipos	2.418,20	2.418,20	—	2.418,20	2.336,50	81,70	—	—	81,70	—	—
Maquinaria y utillaje	387,80	387,80	—	387,80	387,80	—	—	—	—	—	—
Total general	970.583,84	814.727,16	155.856,75	896.905,99	775.967,17	120.938,82	78.970,20	-5.292,35	42.655,63	-3.895,64	-1396,71



