



MEMORIA DESCRIPTIVA DEL PROYECTO:

“PLAN DE ADECUACIÓN A LA NORMATIVA DE PROTECCIÓN DE DATOS DEL SECTOR PÚBLICO FORAL DEL TERRITORIO HISTÓRICO DE BIZKAIA: DIPUTACIÓN FORAL DE BIZKAIA Y ENTIDADES FORALES”

Candidatura Premio a la Proactividad y Buenas Prácticas en el Cumplimiento del Reglamento General de protección de datos y la Ley Orgánica de protección de datos Personales y Garantía de los Derechos Digitales convocado por la Agencia Española de protección de datos. Modalidad B.

noviembre de 2021

Índice

1. INTRODUCCIÓN.....	2
1.1. Sector Público Foral del Territorio Histórico de Bizkaia: valores, organización y competencias	8
1.1.1. El Sector Público Administrativo	8
1.1.2. El Sector Público Empresarial	11
2. CONTEXTO DE LA PROTECCIÓN DE DATOS EN EL SECTOR PÚBLICO FORAL DEL TERRITORIO HISTÓRICO DE BIZKAIA.....	16
2.1. Características y retos de la protección de datos en el Sector Público Foral	17
2.2. Marco normativo de la protección de datos en el Sector Público Foral del Territorio Histórico de Bizkaia	25
2.3. Situación del Sector Público Foral del Territorio Histórico de Bizkaia en relación a los tratamientos de datos personales realizados antes de la aplicación del RGPD	28
3. PLAN DE ADECUACIÓN.....	30
3.1. Alcance y objetivos del Plan de Adecuación	31
3.2. Contenido, fases y acciones	33
3.2.1. Fase I. Análisis del estado de situación.....	34
3.2.2. Fase II. Diseño del plan de acción	37
3.2.3. Fase III. Creación del modelo de gobernanza corporativa para la protección de datos y seguridad de la información.....	39
3.2.4. Fase IV. Implementación del Plan de Adecuación.....	46
3.2.5. Fase V. Formación y concienciación	73
3.2.6. Fase VI. Control, revisión y mejora continua	78
4. EJEMPLOS DE PROACTIVIDAD Y BUENAS PRÁCTICAS.....	80
4.1. Implementación del Plan de Adecuación en el Departamento de Acción Social y en el Departamento de Empleo, Inclusión Social e Igualdad de la Diputación Foral de Bizkaia: mecanismo para el cumplimiento del RGPD y la LOPDGDD en tratamientos de datos de categoría especial	81
4.2. Protección de datos desde el diseño y por defecto en los sistemas informáticos	83
4.3. Rol de la Sección de Asesoramiento Jurídico seguridad de la información y protección de datos de la Diputación Foral de Bizkaia como impulsora, supervisora y asesora para la implementación del Plan de Adecuación	84
4.4. Información sobre protección de datos en bizkaia.eus: transparencia, lenguaje claro y cercanía como principios inspiradores	85
5. CONCLUSIONES Y VALORACIÓN DEL PLAN DE ADECUACIÓN EN LA ACTUALIDAD.....	87



1. INTRODUCCIÓN

1. INTRODUCCIÓN: DIPUTACIÓN FORAL DE BIZKAIA Y EL CAMBIO DE PARADIGMA EN “PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN” EN SU SECTOR PÚBLICO FORAL DEL TERRITORIO HISTÓRICO DE BIZKAIA

El presente documento recoge la memoria descriptiva del proyecto que la Diputación Foral de Bizkaia presenta como candidatura a la modalidad B del «Premio a la Proactividad y Buenas Prácticas en el cumplimiento del Reglamento General de protección de datos y a la Ley Orgánica de protección de datos Personales y garantía de los derechos digitales» otorgado por la Agencia Española de protección de datos.

La Diputación Foral de Bizkaia como Administración Pública de referencia en el Territorio Histórico de Bizkaia y con el firme compromiso que tiene en **garantizar la privacidad de los datos personales que trata**, considera de interés presentar a la presente convocatoria el proyecto que lidera la Dirección General de Buen Gobierno y Transparencia del Gabinete de Estrategia Digital y Corporativa de la Diputación Foral de Bizkaia, consistente en el diseño e implantación del **Plan de Adecuación a la normativa de protección de datos del Sector Público Foral del Territorio Histórico de Bizkaia**. Un Plan que no solo se ha implementado en la propia Diputación Foral de Bizkaia, sino también en todas y cada una de las **diferentes entidades públicas forales** que junto con la propia Diputación conforman el Sector Público Foral del Territorio Histórico de Bizkaia.

La Diputación Foral de Bizkaia es consciente de que todo su entorno foral, tanto la propia Diputación en calidad de Administración Pública como sus Entidades Forales, son instituciones públicas que en su día a día manejan **gran cantidad de datos personales** e información de las personas que constituyen un **activo intangible a proteger**. Y es que, tanto la Diputación como las Entidades Forales, a fin de prestar o gestionar sus servicios públicos recaban, custodian y **realizan diversas operaciones y tratamientos de datos personales** de los que son titulares las personas físicas. Por ello, la Diputación y sus entidades son conscientes de la asunción del Rol de Responsables de estos datos y que, además, es su obligación cumplir con la normativa en vigor:

- *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante **RGPD**).*
- *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantía de derechos digitales. (en adelante, **LOPDGDD**)*

La Diputación Foral de Bizkaia entiende que esta normativa ha supuesto un auténtico **cambio de paradigma en el ámbito de la privacidad**. Es una realidad afirmar que, en pocos años, hemos dado un salto de un mundo principalmente analógico a un **mundo digital**: aplicaciones y servicios de Internet, correo electrónico, banca y compra *online*, domótica, inteligencia artificial, dispositivos conectados a Internet: relojes, gafas, teléfonos inteligentes, etc.

Esta nueva era de interconexión mundial de las redes digitales promueve la **globalización de la información**, convirtiendo Internet en un medio propicio para la circulación transfronteriza de los datos y de la información. Las nuevas tecnologías son recursos técnicos que permiten este movimiento de datos, pero esta globalización de la información no está exenta de **riesgos** como puede ocurrir si se produce un movimiento de datos sin contar con la debida base legitimadora o sin informar debidamente a las personas interesadas.

Es, por todo ello, que la Diputación Foral de Bizkaia, consciente de estas amenazas, trabaja en ofrecer a la ciudadanía servicios y prestaciones **adaptándose a la era digital**, pero garantizando un **nivel de seguridad adecuado** a la tipología y categoría de los datos personales que trata, a las necesidades y particularidades de las personas titulares de los mismos y a la información tratada. Tal y como se indica esta realidad digital, con sus ventajas y amenazas, debe reflejarse también en la práctica del Sector Público Foral del Territorio Histórico de Bizkaia que no puede ni debe quedarse atrás ni al margen de la nueva era digital, de modo que las personas que solicitan y acceden a los servicios y prestaciones que la Diputación Foral de Bizkaia y las Entidades Forales les ofrecen, lo hagan con las **máximas garantías en calidad, privacidad y seguridad de la información**.

Para el cumplimiento de estos objetivos, la Diputación Foral de Bizkaia, dentro de su Plan de Gobierno Foral diseña el Modelo de Gobernanza Corporativa para la protección de datos y la seguridad de la información, en particular el **Plan de Adecuación a la normativa de protección de datos del Sector Público Foral del Territorio Histórico de Bizkaia**, que aborda de manera **unificada** el tratamiento de la protección de datos personales y la seguridad de la información, con una visión **transversal y holística** para el conjunto del Sector Público Foral. Este Plan tiene sus orígenes e inicia su despliegue, siguiendo la sinergia unificada en privacidad, ya en el año **2013**:

- Por un lado, la Diputación Foral de Bizkaia aprobó el **Decreto Foral** de la Diputación Foral de Bizkaia **173/2013**, de 10 de diciembre, por el que se aprueba la implantación de medidas de seguridad, organizativas, de infraestructura, aplicaciones y servicios en materia de protección de datos de carácter personal, que diseña una **estructura organizativa en protección de datos**, con asignación de funciones y roles tanto a nivel de dirección (establece la dirección y control de los datos personales, de los procesos y asigna dentro de la Diputación Foral de Bizkaia la toma de decisiones) como a nivel de gestión (crea la figura de personas interlocutoras para el tratamiento de datos).
- Por otro lado, la Diputación Foral de Bizkaia aprobó en el año 2017 la **Política de seguridad de la información**.

Para llevar a cabo todos estos hitos y acciones que constituyen auténticos retos en el cambio de paradigma, la Diputación Foral de Bizkaia trabaja “mano a mano” con las Entidades Forales, realizando una mención especial a la Entidad Foral **Lantik S.A.M.P**, por cuanto que desempeña el rol de **Administrador tecnológico**, y con todos los Departamentos y Gabinetes Forales, principalmente a través de la designación de las **personas dinamizadoras** que permiten la comunicación y ejecución de actuaciones en materia de protección de datos impulsadas desde el Gabinete de Estrategia Digital y Corporativa.

Todo ello está siendo posible gracias a que desde la Diputación se apuesta por un Modelo de Gobernanza Corporativa que garantice la **gestión transversal** en materia de protección de datos, un modelo liderado por un equipo de personas **especializadas** en la materia que integran la **Sección de Asesoramiento Jurídico, seguridad de la información y protección de datos** de la Dirección General de Buen Gobierno y Transparencia perteneciente al Gabinete de Estrategia Digital y Corporativa y la designación de una persona Delegada de protección de datos (**DPO**) para todo el Sector Público Foral con un doble objetivo:

1. Cumplimiento de la normativa desde una cultura **preventiva** del riesgo, para la no materialización de amenazas.
2. Satisfacer las **nuevas necesidades y expectativas** que tiene la ciudadanía en la **era digital**. La Diputación Foral de Bizkaia avanza en el horizonte de incorporar las nuevas tecnologías en la prestación de servicios y realización de actividades,

pero con garantías de **seguridad jurídica** y regulando todas las actuaciones de manera previa.

Las novedades que introdujo el **RGPD**, principalmente el **cambio de enfoque** respecto al cumplimiento normativo motiva que se deba modificar la forma en la que las organizaciones cumplen con esta normativa. Así, en el ámbito de la protección de datos, se partía de una normativa previa (Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de Carácter Personal) que establecía de forma clara las obligaciones legales a cumplir y el modo en el que estas se debían cumplir, para tener en la actualidad una normativa con un **enfoque proactivo** donde las organizaciones Responsables del Tratamiento deben decidir la manera óptima de cumplir con las obligaciones legales en función de las dimensiones y características de cada organización.

Por ello, y de cara al presente y futuro de este ámbito, la Diputación Foral de Bizkaia enfoca su trabajo en la línea de adoptar una política de privacidad que aúne de manera indisoluble los dos ámbitos: **protección de datos y seguridad de la información**. Se ha trabajado y se está trabajando en el diseño y la implementación del Plan de Adecuación de Protección de datos y seguridad de la información, que es un modelo de organización y gestión que recoge los principios generales, medidas de seguridad, procedimientos (implantados o a implementar), responsables de aplicación y actividades de control. Destacamos los hitos principales de este Plan que se detallarán a lo largo de la presente Memoria:

1. **Despliegue del Principio de Responsabilidad proactiva:** la Diputación Foral de Bizkaia considera necesario **analizar** qué datos personales se tratan, con qué objetivos y qué tipo de operaciones de tratamiento se llevan a cabo y, a partir de esta realidad e infraestructura de datos, decidir las medidas a adoptar para asegurar su cumplimiento en función de los riesgos detectados y asumidos. Cumplir con este principio, esto es, **ser proactivo y organizado** supone evidenciar los pasos que se han dado para su cumplimiento.
2. **Despliegue del Principio de Protección de datos desde el diseño y por defecto:** la Diputación Foral de Bizkaia tiene en cuenta la privacidad desde el origen de cualquier nuevo desarrollo tecnológico y nuevo servicio a prestar a la ciudadanía. Este enfoque permite diseñar de manera previa medidas de seguridad necesarias y eficaces.

Para la Diputación Foral de Bizkaia crear una cultura de prevención de riesgos es un **objetivo estratégico** a conseguir, no sólo desde el punto de vista de la privacidad (protección de datos y seguridad de la información) sino desde diversos puntos de vista que abarcarían múltiples ámbitos, como puede tratarse de la prevención de delitos mediante la implantación de modelos de organización y gestión de cumplimiento normativo dentro de los que se pueden identificar los programas de cumplimiento (**compliance**) penal, o de mejora de la eficiencia y **transparencia** en la tramitación de los contratos públicos que se formalicen con la Diputación Foral de Bizkaia y el resto de entidades del Sector Público Foral, o simplemente alcanzar **mejores y mayores niveles de eficiencia en el desempeño de la relación funcional**.

3. Creación y nombramiento del rol de Persona Delegada de protección de datos (en adelante, **DPO**): se ha designado la figura de la persona Delegada de protección de datos tanto para la Diputación Foral de Bizkaia como sus Entidades Forales.
4. Diseño y alcance de los roles de **Responsable del tratamiento y Encargado del tratamiento** en el ámbito de la privacidad

- 1) **Diseño de Roles:** los diferentes Roles dentro de la organización del Sector Público Foral, que juegan un papel determinante en el cumplimiento de la normativa y que tiene clara comunicación entre ellos:
 - i. Capa de **dirección y gobierno:** con la existencia de un Comité de Dirección.
 - ii. Capa **operativa:** llevar a cabo las operaciones y procesos con la participación de Responsables de tratamiento, Encargados de tratamiento, Responsables de Información, personal dinamizador, entre otros.
 - iii. Capa de **supervisión y control:** mediante controles internos y externos (auditorías, órgano independiente), con la participación de roles desempeñados por Responsables de Seguridad, Administrador tecnológico y auditores externos.
- 2) Determinar las **funciones y obligaciones** de los diferentes Roles.
5. Revisión de las **bases legitimadoras** de los diferentes tratamientos de datos personales. La Diputación Foral de Bizkaia trata datos personales amparada en el ejercicio de sus competencias normativas, el cumplimiento de sus obligaciones legales y el interés público de acuerdo a las letras c y e del artículo 6.1. RGPD.
6. Revisión del cumplimiento del **deber de informar:** incorporando cláusulas informativas en sus servicios y prestaciones forales.
7. Se introducen los **nuevos derechos** en materia de protección de datos: el derecho de supresión u olvido, el de la limitación del tratamiento o el de la portabilidad de los datos.
8. Se establecen **planes formativos y de concienciación** del personal empleado foral con el objetivo de generar una cultura de compromiso y concienciación.
9. Se crea el **Registro de Actividades de Tratamiento**.
10. Se continúa con la realización de los **análisis de riesgos**, y se regulan, incorporan y realizan los procedimientos para las **evaluaciones de impacto**.

Precisamente, los principales retos y fortalezas que tiene el Plan de Adecuación que se describe en la presente Memoria, es que este se ha diseñado a medida para que el mismo se **adapte** de forma minuciosa a las **diferentes y variadas realidades** existentes en relación a los tratamientos de datos personales que se llevan a cabo en el Sector Público Foral del Territorio Histórico de Bizkaia. Para alcanzar dicho objetivo y lograr que el Plan se pueda implementar de forma satisfactoria en todo el Sector Público Foral, este Plan se ha dividido en las siguientes **fases de trabajo que se detallan** a lo largo de los siguientes epígrafes:



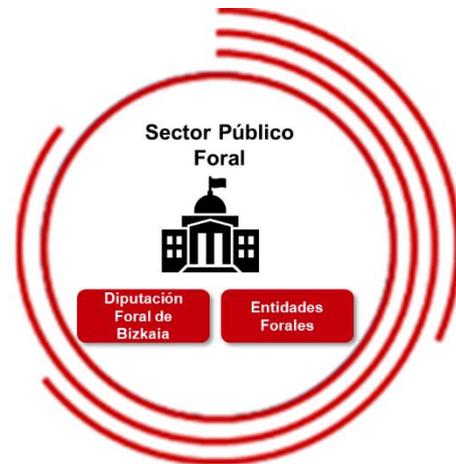
que persigue la Diputación en materia de protección de datos: la **implicación y concienciación** del personal de la Diputación y de las Entidades Forales en la importancia del respeto de la normativa de protección de datos. Concienciación que busca lograr la creación de una **óptima cultura de cumplimiento normativo en materia de protección de datos** dentro del Sector Público Foral.

A lo largo de los siguientes epígrafes se expondrá de forma detallada como las **especialidades** organizativas, el contar con competencias exclusivas en materia de **gestión tributaria**, la existencia de un **acervo jurídico foral propio** y específico que regula la actividad de las entidades del Sector Público Foral del Territorio Histórico de Bizkaia, unidas a la **gran cantidad de datos personales** que las entidades tratan, hacen que el Plan de Adecuación llevado a cabo y cuyo contenido se detalla en la presente Memoria, cuente con numerosas **particularidades** y sea novedoso respecto de los planes de cumplimiento de la normativa de protección de datos que tradicionalmente se llevan a cabo en la administración pública. Un Plan que se ha llevado a cabo buscando la **concienciación e implicación de todo el personal**, a través de una **fuerte estructura de seguridad interna** que impulsa y lidera los trabajos, y teniendo como premisa principal el compromiso que el Sector Público Foral tiene en **garantizar el derecho fundamental a la protección de datos** que toda persona tiene.

1.1. Sector Público Foral del Territorio Histórico de Bizkaia: valores, organización y competencias

El Sector Público Foral del Territorio Histórico de Bizkaia se halla integrado por el **Sector Público Administrativo** y el **Sector Público Empresarial**:

- **Sector Público Administrativo:**
 - Diputación Foral de Bizkaia.
 - Organismos Autónomos Forales.
- **Sector Público Empresarial:**
 - Entidades Públicas Empresariales Forales.
 - Sociedades Mercantiles Forales.
 - Fundaciones Forales.



1.1.1. El Sector Público Administrativo

Como se ha expuesto, el Sector Público Administrativo está formado por la Diputación Foral de Bizkaia y por los Organismos Autónomos Forales.

En primer lugar, la **Diputación Foral de Bizkaia** es el órgano colegiado que, en la esfera de sus competencias, asume el **gobierno** y administración de Bizkaia, correspondiéndole la función ejecutiva, la potestad reglamentaria y la iniciativa normativa. Bizkaia, como los otros Territorios Históricos de Araba y Gipuzkoa, cuenta con una **asamblea legislativa** que son las Juntas Generales y que desarrolla su capacidad normativa en materias de su competencia, y un **gobierno** que es la Diputación Foral.

Cabe mencionar que, tal y como establece la **Disposición Adicional Primera** de la Constitución española, los territorios históricos cuentan con un régimen foral propio que hace que cuenten con **especialidades organizativas y particularidades competenciales**. Así, la Diputación Foral de Bizkaia ejerce una amplia serie de competencias que le atribuye el Estatuto de Autonomía de Gernika¹, entre las que destacan la gestión de un **sistema tributario propio**, las carreteras y caminos del territorio, las obras públicas, los servicios sociales, o el patrimonio cultural y el medioambiental.

Actualmente, la Diputación Foral de Bizkaia se divide en **11 departamentos y gabinetes**:

- Gabinete del Diputado General.
- Gabinete de Estrategia Digital y Corporativa.
- Sostenibilidad y Medio Natural;
- Acción Social;
- Euskera, Cultura y Deporte;
- Hacienda y Finanzas;
- Transportes y Movilidad Sostenible;
- Administración Pública y Relaciones Institucionales;
- Promoción económica;

¹ Aprobado mediante la *Ley Orgánica 3/1979, de 18 de diciembre, de Estatuto de Autonomía para el País Vasco*.

- Empleo, Inclusión Social e Igualdad;
- Infraestructuras y Desarrollo Territorial.

Respecto a las competencias, la Diputación Foral de Bizkaia ejerce su actividad pública en el marco general de competencias definido por:

- *Ley Orgánica 3/1979, de 18 de diciembre, de Estatuto de Autonomía para el País Vasco.*
- *Ley 27/1983, de 25 de noviembre, de Relaciones entre las Instituciones Comunes de la Comunidad Autónoma y los Órganos Forales de sus Territorios Históricos* y demás disposiciones de delegación o transferencia.
- *Ley 12/2002, de 23 de mayo, por la que se aprueba el Concierto Económico con la Comunidad Autónoma del País Vasco*, adaptado al Impuesto sobre el Valor Añadido y otras disposiciones de carácter tributario y demás normas que en este sentido se establezcan.
- Las disposiciones legales que establecen el marco competencial en el que actualmente se desenvuelven las Diputaciones de Régimen Común y en particular según lo dispuesto en la Disposición Adicional 2ª de la *Ley 7/85, de 2 de abril, reguladora de las Bases de Régimen Local*.
- *Norma Foral 3/1987, de 13 de febrero, sobre Elección, Organización, Régimen y Funcionamiento de las Instituciones Forales del Territorio Histórico de Bizkaia.*

Las citadas normativas atribuyen a la Diputación Foral de Bizkaia una serie de competencias. Entre otras, **destacan por su relevancia en materia de protección de datos**, las siguientes competencias las cuales son desarrolladas por los diferentes departamentos y gabinetes forales:

Administración Pública y Relaciones Institucionales
<ul style="list-style-type: none">• Contratación, selección y formación del personal, régimen retributivo y el régimen jurídico en el que se incluye el sancionador del personal de la Diputación Foral de Bizkaia.• Ayuda y asesoramiento en materia jurídica, económica y técnica a las Entidades Locales.• Protección civil dentro del Territorio Histórico de Bizkaia.
Promoción económica
<ul style="list-style-type: none">• Vigilar y controlar la gestión de los Servicios Públicos, Fundaciones, Entidades y Empresas.• El impulso y desarrollo de todas las actividades que tengan relación con la promoción empresarial, la creación de nuevas empresas y la promoción de la cultura emprendedora, la diversificación empresarial y la consolidación de sectores emergentes y en crecimiento y la atracción y promoción del talento y el conocimiento.• Impulso y desarrollo de las actividades que tengan relación con la imagen de Bizkaia en el exterior y la promoción turística.
Hacienda y Finanzas
<ul style="list-style-type: none">• Regulación del régimen tributario del Territorio Histórico de Bizkaia.• Exacción, gestión, liquidación, inspección, revisión y recaudación de los tributos que integran el sistema tributario del Territorio Histórico de Bizkaia.
Euskera, Cultura y Deporte
<ul style="list-style-type: none">• Promover proyectos relativos a cultura, patrimonio cultural, deporte y euskera.
Sostenibilidad y Medio Natural

<ul style="list-style-type: none">• La definición y desarrollo de la política ambiental de Bizkaia.• Gestión de los espacios naturales, agricultura y ganadería.
Acción social
<ul style="list-style-type: none">• La promoción, coordinación, dirección y, en su caso, ejecución de la actividad política y administrativa en materia de protección de personas menores de edad.• La definición y ejecución de la política de prevención, detección, diagnóstico, tratamiento, orientación e integración de las personas en situación de dependencia y discapacidad
Empleo, Inclusión Social e Igualdad
<ul style="list-style-type: none">• La colaboración y coordinación con la política general en el ámbito de la inclusión social, propugnando la disminución de las desigualdades sociales y de las causas generadoras de la marginación social, así como el tratamiento asistencial y la reinserción comunitaria y laboral.• La atención a la problemática social específica de la mujer y de la familia.• La promoción y sostenimiento de la empleabilidad de las personas a través de la gestión de las políticas activas de empleo dentro del ámbito competencial de la Diputación Foral de Bizkaia.• La inserción laboral de las personas con dificultades de acceso al empleo: mayores de 45 años, desempleadas de larga duración, personas con discapacidad y personas en situación de riesgo o exclusión social.• Gestión de las políticas de igualdad de mujeres y hombres en el Territorio Histórico de Bizkaia.• Diseño de políticas de cooperación directa y descentralizada.
Transportes y movilidad sostenible
<ul style="list-style-type: none">• Ordenación, fomento, inspección, sanción y desarrollo de la organización administrativa y de la planificación del transporte en Bizkaia.• Fomentar e impulsar la cultura del de la movilidad sostenible promoviendo la concienciación social y adoptando medidas y procedimientos que promuevan el cambio de hábitos sociales y de los sistemas de transporte tradicional
Infraestructuras y desarrollo territorial
<ul style="list-style-type: none">• Planificación, proyecto, construcción, conservación, modificación, financiación, uso y explotación de carreteras y caminos del Territorio Histórico de Bizkaia.• Ordenación Territorial, planeamiento urbanístico, organización y gestión viaria.
Gabinete del Diputado General
<ul style="list-style-type: none">• Programar, impulsar y coordinar la acción exterior de la Diputación Foral de Bizkaia y de sus Entidades Forales.
Gabinete de Estrategia Digital y Corporativa
<ul style="list-style-type: none">• Dirección, impulso y coordinación de iniciativas corporativas, proyectos y actuaciones de naturaleza interdepartamental de la Diputación Foral de Bizkaia y de las entidades del Sector Público Foral encaminadas a la consecución de una administración avanzada, digital e innovadora en su modelo de gestión.• Impulso de la transparencia y el buen gobierno en el Sector Público Foral.

En segundo lugar, los organismos autónomos forales son aquellas entidades del Territorio Histórico de naturaleza pública cuyo objetivo es la realización en régimen de descentralización de actividades pertenecientes a la competencia del mismo y que se rigen por el **derecho público**. El **Instituto Foral de Asistencia Social** es un organismo autónomo foral adscrito al Departamento de Acción Social de la Diputación Foral de Bizkaia. Este Organismo ofrece una atención integral y personalizada a todas aquellas

personas que presentan necesidades complejas, garantizándoles servicios y recursos sociales especializados de calidad que ayudan tanto a las personas usuarias como a sus familias, a tener una vida digna, apoyando un entorno favorable al ejercicio de sus derechos y desarrollo de sus potencialidades.

1.1.2. El Sector Público Empresarial

Por su parte, el Sector Público Empresarial está formado por

- Entidades Públicas Empresariales Forales.
- Sociedades Mercantiles Forales.
- Fundaciones Forales.

Estas Entidades Forales tienen personalidad jurídica diferenciada, patrimonio y tesorería propios, así como autonomía de gestión, en los términos previstos en el *Decreto Foral Normativo 5/2013 de 3 de diciembre, por el que se aprueba el texto refundido de la Norma Foral 5/2006, de 29 de diciembre, General Presupuestaria* y demás normativa aplicación.

Actualmente, las **Entidades Forales** que dentro del Sector Público Foral del Territorio Histórico de Bizkaia componen el Sector Público Empresarial, son las siguientes:

i. Entidades públicas empresariales forales:

Entidades de naturaleza pública cuyo objeto es la realización de actividades prestacionales, la gestión de servicios o la producción de bienes de interés público susceptibles de contraprestación.

Las entidades públicas empresariales forales y sus funciones son las siguientes:

- **BizkaiKOA, E.P.E.F.²** Difusión del patrimonio cultural de Bizkaia, su sensibilización y fomento social, su gestión coordinada y bajo un prisma de eficiencia en la disposición de recursos, así como su preservación, conservación, salvaguarda, difusión y fomento de cara a las generaciones venideras
- **Delegación en Bizkaia de Loterías y Apuestas del Estado (LAE).** Delegación comercial en Bizkaia de la Sociedad Estatal Loterías y Apuestas del Estado, S.M.E, S.A.
- **Instituto Tutelar de Bizkaia.** Ejerce la tutela y curatela de los mayores de edad incapacitados legalmente, residentes en el Territorio Histórico de Bizkaia, cuando así lo determine la autoridad judicial competente, así como la defensa judicial de quienes estén sometidos a un proceso de incapacitación o el ejercicio de cuantas otras funciones determine la autoridad judicial en defensa de presuntos incapaces en situación de desamparo.

ii. Sociedades mercantiles forales:

Sociedades mercantiles en cuyo capital la participación del Sector Público Foral es **superior al 50%**.

Las sociedades mercantiles forales y sus funciones son las siguientes:

- **Aparkabisa. Centro de transportes de Bizkaia S.A.** Construcción y gestión en Bizkaia de centros de transporte y aparcamiento de vehículos pesados.
- **Azpiegiturak, S.A.M.P³.** Proyectar, construir, conservar y explotar, por sí misma, por terceras personas o en calidad de concesionario y en nombre propio o por

² Ente Público Empresarial Foral.

³ Sociedad Anónima Medio Propio.

cuenta de la Diputación Foral de Bizkaia, las obras públicas de infraestructura y equipamientos de todo tipo.

- **Basalan, S.A.M.P.** Planificación, mejora y ejecución de toda clase de trabajos forestales y de conservación de la naturaleza.
- **BEAZ, S.A.U.** Presta apoyo a las empresas y a las personas emprendedoras en su esfuerzo por crear nuevos proyectos, innovar e internacionalizarse.
- **Crowdfunding Bizkaia, S.L.** Plataforma de financiación participativa que pone en contacto a promotores que tienen proyectos innovadores nacidos y ubicados en Bizkaia, con inversores de todo el mundo.
- **Garbiker, S.A.M.P.** Gestión de los residuos urbanos generados en Bizkaia.
- **Interbiak, S.A.M.P.** Realización de estudios, proyección, construcción, conservación, mantenimiento y explotación, por sí misma o de terceros, de las infraestructuras viarias que le encomiende la Diputación Foral de Bizkaia.
- **Lantik, S.A.M.P.** Planificar y ejecutar la Política de Sistemas de Información definida por la Diputación Foral de Bizkaia.
- **Palacio Euskalduna, S.A.** Palacio de la Música y Congresos en Bilbao para la organización de Congresos y Festivales Musicales.
- **SEED-Capital de Bizkaia, S.A.** Sociedad Gestora de Entidades de Inversión de Tipo Cerrado S.A. (S.G.E.I.C.) destinada a la administración y gestión de diversos instrumentos de financiación para fomentar la innovación, el impacto social y la promoción y regeneración del tejido empresarial en Bizkaia.
- **Seed Capital Mikro, S.A.** Apoyo y fortalecimiento del tejido empresarial en Bizkaia ofreciendo una financiación alternativa en forma de microcréditos.
- **Sestao Bai, S.A.** Instrumento para la consolidación de un nuevo tejido industrial generador de empleo de calidad y riqueza, que contribuya a aumentar la calidad de vida de las personas de Sestao.
- **Zugaztel, S.A.M.P.** Prestación de servicios especializados en asegurar la entrada masiva de datos a los sistemas de información, así como en facilitar la comunicación a través de los diferentes canales de atención a la ciudadanía a favor de todas las entidades del Sector Público Foral del Territorio Histórico de Bizkaia.

iii. Fundaciones forales

Son fundaciones forales aquellas que se constituyan con una aportación mayoritaria del Sector Público Foral, o aquellas cuyo patrimonio fundacional esté formado en más de un 50% por bienes o derechos aportados o cedidos por los referidos entes.

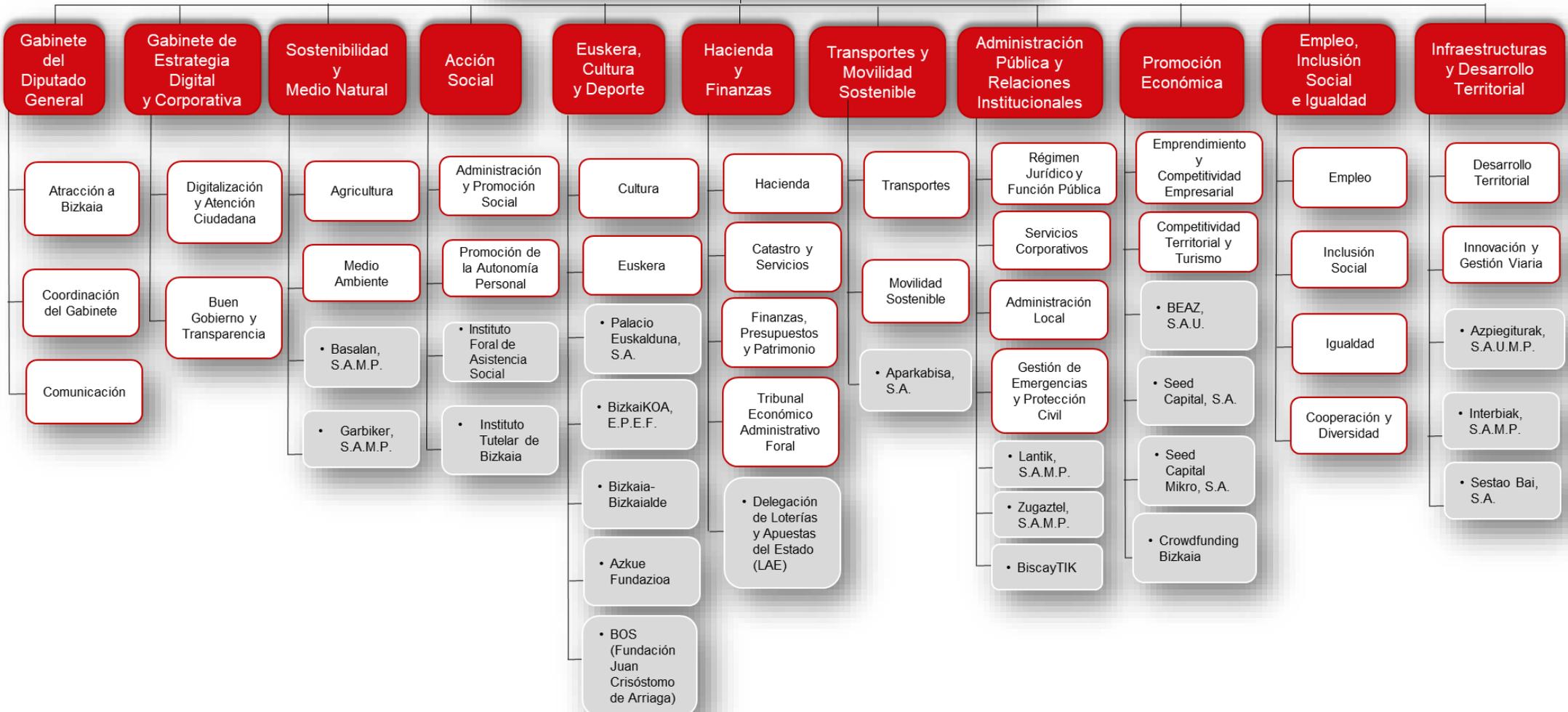
Las fundaciones forales y sus funciones son las siguientes:

- **BOS (Fundación Juan Crisóstomo de Arriaga).** Entidad sin ánimo de lucro creada por la Diputación Foral de Bizkaia y el Ayuntamiento de Bilbao para gestionar la Bilbao Orkestra Sinfonikoa.
- **Fundación Azkue.** Fomento del uso del euskara de manera dinámica, aprovechando la tecnología y adaptándose a los nuevos tiempos.
- **Fundación BiscayTIK.** Fundación pública sin ánimo de lucro creada por la Diputación Foral de Bizkaia, con el objetivo de modernizar los ayuntamientos y mancomunidades mediante el uso de nuevas tecnologías, y convertir a Bizkaia en un referente en el ámbito de la administración electrónica local.
- **Fundación Bizkaia Bizkaialde.** Institución que concentra fondos públicos y privados destinados a coordinar los esfuerzos económicos de los patrocinadores del deporte, con el objeto de rentabilizar al máximo su inversión, de cooperar en la promoción de Bizkaia y de contribuir a lograr una correcta y eficaz ordenación del propio deporte.

Con objeto de ilustrar de forma gráfica la organización del Sector Público Foral del Territorio Histórico de Bizkaia expuesta en el presente epígrafe, se reproduce a continuación dos **organigramas**:

- Organigrama de la Diputación Foral de Bizkaia.
- Organigrama del Sector Público Foral.

DIPUTACIÓN FORAL DE BIZKAIA

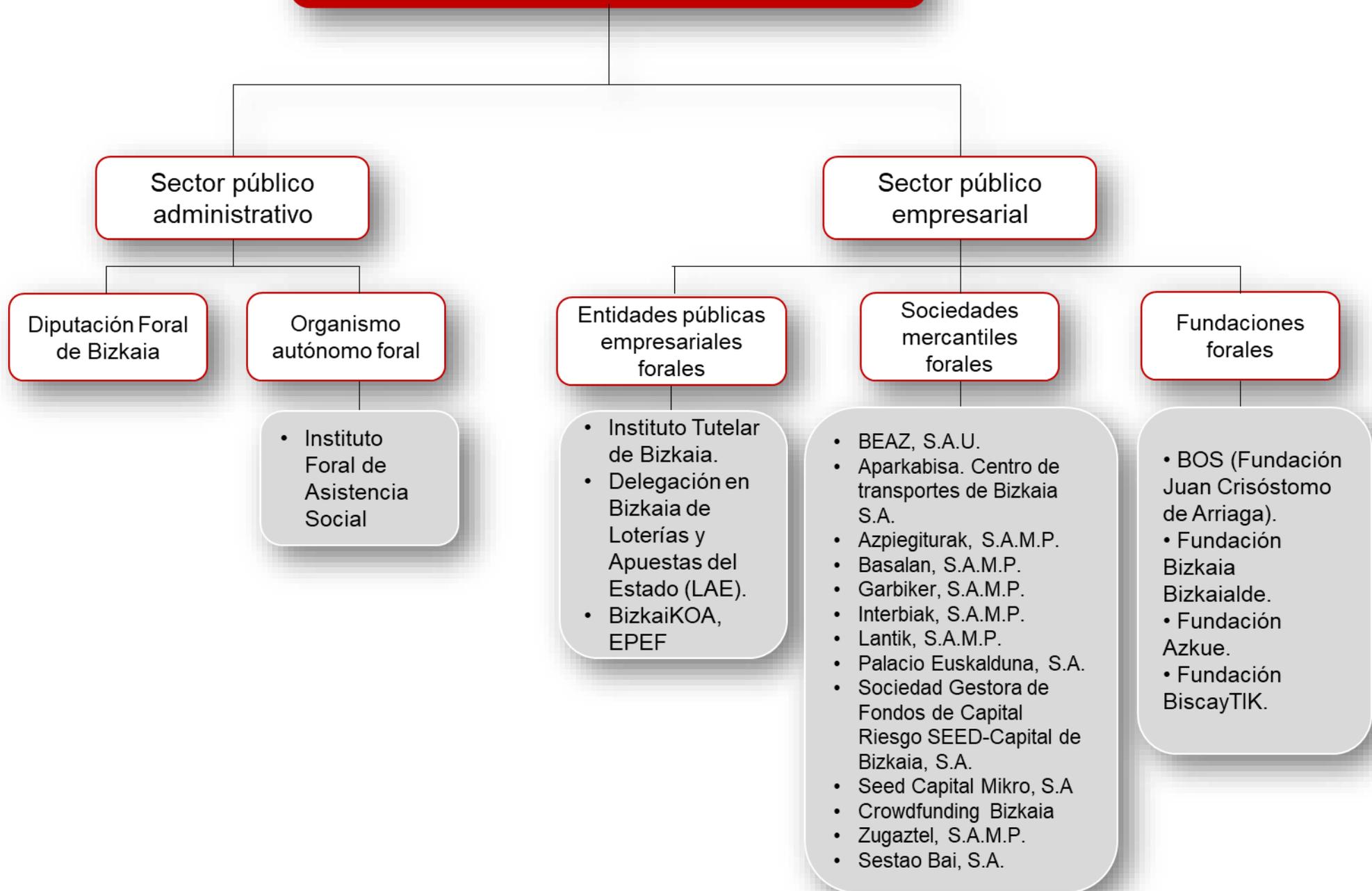


Departamentos Forales / Gabinetes

Direcciones generales

Entidades Forales

SECTOR PÚBLICO FORAL DEL TERRITORIO HISTÓRICO DE BIZKAIA





2. CONTEXTO DE LA PROTECCIÓN DE DATOS EN EL SECTOR PÚBLICO FORAL DEL TERRITORIO HISTÓRICO DE BIZKAIA

2.1. Características y retos de la protección de datos en el Sector Público Foral

Una vez descritas las particularidades competenciales, normativas y organizativas del contexto foral, en este epígrafe se expondrán las **principales características que dicho Sector Público tiene en materia de protección de datos personales** y como las mismas han supuesto un **desafío** en el diseño e implementación de este Plan de Adecuación.

Dichos retos son los siguientes:



A continuación, se desarrollan los citados retos con objeto de poner en contexto cómo los mismos han supuesto un **desafío en el diseño de Plan de Adecuación** que es objeto de exposición en la presente Memoria, y cómo se han integrado los mismos en dicho Plan.

i. Gran volumen de datos personales

Tanto la Diputación como administración pública y como institución que ejerce el gobierno del Territorio Histórico de Bizkaia, como el resto de entidades integrantes del Sector Público Foral, tratan una gran cantidad de datos personales de la ciudadanía. Dichos datos han de ser objeto de tratamiento ya sea porque sus titulares tributan en Bizkaia, porque solicitan alguna ayuda o subvención gestionada por la institución foral o, en definitiva, porque se les presta algún servicio cuya competencia está encomendada al Sector Público Foral.

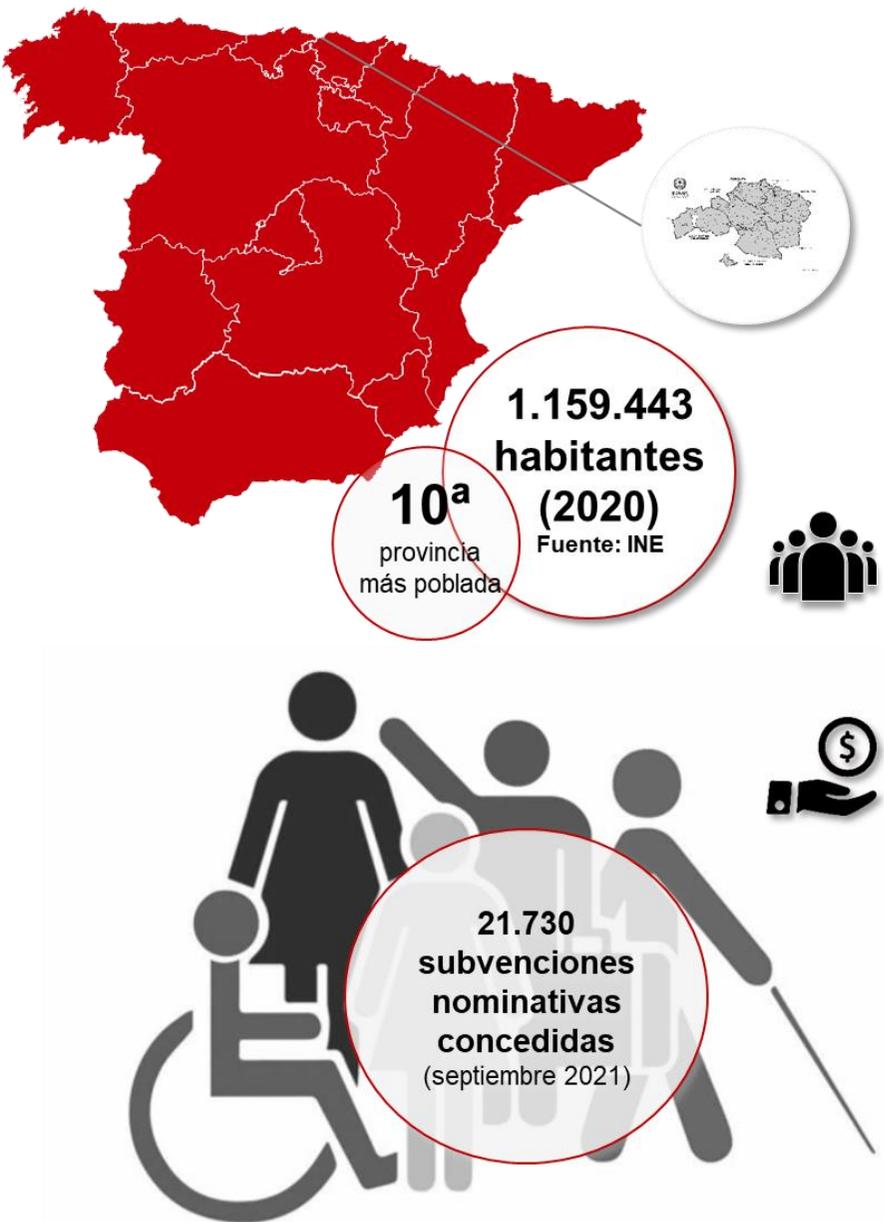
En particular, la Diputación Foral de Bizkaia en el desempeño de su rol de Administración Pública, gestiona recursos públicos por y para la ciudadanía y requiere de múltiples intercambios continuos de datos con la misma, entre los que hay datos personales.

Este gran volumen de datos personales gestionados hace que uno de los principales retos del Plan de Adecuación haya sido la implementación efectiva del principio de minimización de datos mediante el diseño de procedimientos que permiten verificar que solo se recaban en cada caso los datos personales adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. Asimismo, también

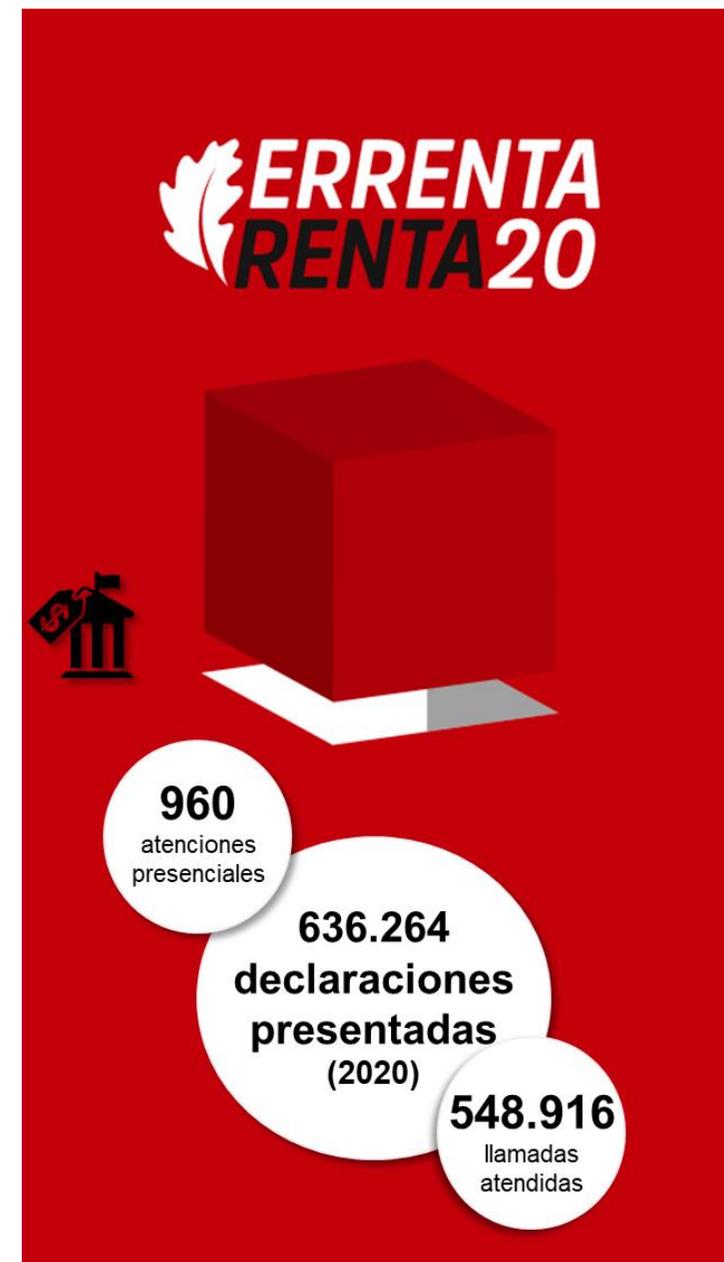
se ha dado importancia a la implementación de los principios de **exactitud y limitación de la finalidad**. La implementación de, principalmente, estos tres principios junto con el resto de obligaciones normativas, ha tenido como objeto principal evitar que existan bases de datos obsoletas, desactualizadas o empleadas para finalidades ilícitas.

Especial importancia ha tenido la implementación de dichos principios en uno de los principales canales de entrada de los datos personales en el Sector Público Foral: la Entidad Foral Zugaztel, S.A.M.P. Tanto Diputación como la mayor parte de Entidades Forales, encomiendan de forma exclusiva a Zugaztel la prestación de servicios especializados en asegurar la **entrada masiva de datos a los sistemas de información**, así como en facilitar la comunicación a través de los diferentes canales de atención a la ciudadanía. Esta Entidad es, por tanto, una de las principales **encargadas del tratamiento** del Sector Público Foral y, en consecuencia, debe atener a las instrucciones de las Entidades Responsables del Tratamiento. Para ello, se ha trabajado dentro del Plan de Adecuación en que las directrices que se dan por cada una de las Entidades Responsables del Tratamiento a Zugaztel estén **armonizadas** con el fin de agilizar la prestación de los servicios y garantizar la calidad de los mismos. Especialmente reseñable es el trabajo que se ha llevado a cabo para diseñar **cláusulas informativas adaptas al modelo de atención telefónica**. Concretamente se ha procurado que estas cláusulas informen de forma correcta de los tratamientos de datos que se realizarán, pero **sin perder claridad ni concreción** teniendo en cuenta las limitaciones del medio en el cual se debe aportar dicha información.

Finalmente, con objeto de ilustrar el gran volumen de datos personales que se tratan por el Sector Público Foral, se recoge a continuación una infografía con datos variados que pretende ilustrar el **elevado número de personas** que se relacionan con el Sector Público Foral y que, para ello, en la mayor parte de supuestos algunos de sus datos personales han de ser objeto de tratamiento.



Fuente: opendatabizkaia.eus



En la anterior infografía se incluyen **algunos ejemplos que muestran la relevancia de los datos personales en nuestra actividad**. Como se puede observar en la infografía, el territorio histórico de Bizkaia cuenta con más de un millón de habitantes, haciendo de Bizkaia la **décima provincia más poblada** del Estado. Respecto al Sector Público Foral, en el mismo trabajamos cerca de **4.000 personas** con la gestión de datos personales que ello supone. Solo en septiembre del presente año la Diputación **concedió cerca de 22.000 subvenciones nominativas** destinadas principalmente al apoyo a colectivos vulnerables, en materia tributaria, durante la campaña de la Renta del pasado año 2020 recibimos más de **600.000 declaraciones de** la renta y atendimos **más de 540.000 consultas**.

De la infografía reproducida y tal y como se avanzaba en anteriores líneas, es también reseñable el **elevado número de personas** del Sector Público Foral que intervienen durante todo el ciclo de vida de los datos personales. Desde la recogida de los datos hasta su supresión, en todo el ciclo de vida son muchas las personas que participan y que deben estar **formadas y concienciadas** tanto en la importancia de respetar la confidencialidad de los datos que tratan en ejercicio de sus funciones profesionales, como de los límites del tratamiento que han de realizar con los mismos.

Precisamente, la **formación y la concienciación** son **pilares básicos** sobre los que se ha sustentado este Plan de Adecuación.

Además, no se han incluido en la infografía, pero también **cabe destacar por su relevancia** en materia de protección de datos, que en Diputación gestionamos al año alrededor de **20.000 solicitudes de dependencia** de personas o representantes que facilitan sus datos y emitimos anualmente alrededor de 20.000 certificados catastrales.

Estos ejemplos tratan de ilustrar el importante trabajo que como Administración y entidades públicas debemos desempeñar para **garantizar a la ciudadanía su derecho fundamental a la protección de datos**, protegiendo su intimidad personal y familiar.

ii. Tratamiento de datos de categoría especial y pertenecientes a colectivos vulnerables

Otro importante reto que afronta el Sector Público Foral en materia de protección de datos es el tratamiento de **datos de categoría especial** regulados por el artículo 9.1. RGPD, y datos pertenecientes a **colectivos vulnerables** (personas en riesgo de exclusión social, víctimas de violencia de género, menores, personas con discapacidad etc.).

En primer lugar, cabe mencionar que la mayor parte de los tratamientos de datos personales **de categoría especial** que realiza el Sector Público Administrativo se llevan a cabo para **cumplir con las obligaciones legales** y para el **ejercicio de las competencias** que el ordenamiento jurídico les atribuye⁴.

El ejercicio de dichas competencias exige en ocasiones que el Sector Público Foral deba tratar datos personales de **categoría especial**. Así, en el ámbito de la Diputación destacan principalmente los tratamientos de datos llevados a cabo por las diferentes Direcciones Generales del **Departamento de Acción Social** y el **Departamento de Empleo, Inclusión Social e Igualdad**. Estos Departamentos, dadas sus competencias, deben llevar a cabo numerosos tratamientos de datos de categoría especial. Entre los tratamientos de datos que llevan a cabo los citados Departamentos, destacan los relacionados con el desarrollo de las siguientes competencias:

⁴ Art. 6.1.c) y e) RGPD.

- La promoción, coordinación, dirección y, en su caso, ejecución de la actividad política y administrativa en materia de **protección de personas menores de edad**.
- La atención a la problemática social específica de la **mujer y de la familia**.
- La definición y ejecución de la política de prevención, detección, diagnóstico, tratamiento, orientación e integración de las **personas en situación de dependencia**.
- La colaboración y coordinación con la política general en el ámbito de la **inclusión social**, propugnando la disminución de las desigualdades sociales y de las causas generadoras de la marginación social, así como el tratamiento asistencial y la reinserción comunitaria y laboral.
- La colaboración con los organismos competentes para hacer frente a las situaciones de **emergencia social**, estableciendo, en su caso, el régimen de ayudas para tales situaciones y efectuando la tramitación de las mismas, su resolución e inspección.
- La tramitación y, en su caso, autorización administrativa para la homologación y registro de centros, entidades y servicios de **servicios sociales**, así como la posterior inspección de los mismos.
- La articulación y gestión de programas de cooperación y desarrollo, así como de salvaguarda de los derechos ciudadanos de personas pertenecientes a **colectivos en situación de riesgo** de pérdida de los mismos.
- La prestación, en el ámbito de Bizkaia, de **servicios sociales** de carácter supramunicipal y, en su caso, supracomarcal, tanto de forma directa, como indirecta, en función de su naturaleza.
- El tratamiento asistencial y la **reinserción comunitaria y laboral**.

El efectivo ejercicio de las citadas competencias requiere que los Departamentos deban tratar numerosos datos de categoría especial como, por ejemplo, datos de salud.

En el ámbito de las **Entidades Forales**, cabe destacar los tratamientos de datos realizados por el Instituto Foral de Asistencia Social y por el Instituto Tutelar de Bizkaia. El primero, presta y garantiza **servicios y recursos sociales** especializados y, el segundo, ejerce la **tutela y curatela de los mayores de edad incapacitados** legalmente residentes en el Territorio Histórico de Bizkaia. Por tanto, el desarrollo de las funciones atribuidas a ambas Entidades Forales implica el tratamiento de **numerosos datos de categoría especial** que requieren de especial protección.

Dentro del Plan de Adecuación y en relación al tratamiento de datos de categoría especial, se han establecido los procedimientos para la realización de las pertinentes **Evaluaciones de Impacto** relativas a la protección de datos (EIPD), así como los análisis que permiten determinar los riesgos asociados a los tratamientos de datos y establecer las salvaguardas a implementar en cada caso. Así, se han establecido protocolos para la **anonimización** de datos personales que han sido previamente sometidos a la correspondiente EIPD, se han **reforzado las medidas de seguridad de los sistemas de información** que almacenan y tratan estos datos, y se ha trabajado en estrecha colaboración con el personal responsable de las diferentes Direcciones Generales que componen este Departamento para **concienciar** en la importancia de mantener la privacidad de, especialmente, los datos de categoría especial a los que acceden en el ejercicio de sus funciones.

Finalmente, en relación al tratamiento de datos de **colectivos vulnerables**, cabe destacar la labor que realiza la Diputación, concretamente el Departamento de Euskera, Cultura y Deporte, en materia de campamentos de verano (*Udalekuak*) en el marco de los cuales se tratan **datos de menores de edad** y, en ocasiones, datos de **salud** de dichos menores.

El Plan de Adecuación ha tenido en cuenta estas realidades existentes y, dada la especial protección que merecen las personas pertenecientes a colectivos vulnerables, se hecho énfasis en **reforzar la claridad de la información** sobre protección de datos que se aporta a estas personas, y a sus tutores o progenitores. Asimismo, en materia de tratamiento de datos de menores, destacan las labores de concienciación llevadas a cabo por parte del Sector Público Foral para **evitar la difusión de sus imágenes** a través de los diferentes canales de comunicación del Sector Público. Especialmente destacable es el énfasis puesto en evitar la captación de imágenes de menores y los diferentes procedimientos articulados para, en su caso, recabar los pertinentes consentimientos para el tratamiento de sus datos personales.

iii. Tratamiento de datos con trascendencia tributaria

Como se ha expuesto en la introducción de la presente Memoria, una de las competencias que ostenta la Diputación Foral de Bizkaia y que, en materia de protección de datos presenta importantes desafíos, es la **competencia tributaria del** Territorio Histórico de Bizkaia.

La *Norma Foral 2/2005, de 10 de marzo, General Tributaria del Territorio Histórico de Bizkaia* establece los principios y las normas jurídicas generales del sistema tributario del Territorio Histórico de Bizkaia, constituyendo el marco de referencia en el que se contienen las normas que regulan los aspectos generales del sistema tributario. En el ámbito de la Diputación Foral de Bizkaia, el desempeño de estas funciones corresponde al **Departamento Foral de Hacienda y Finanzas** que para ejercer las mismas ha de realizar una serie de **tratamientos de datos personales**.

Dada su **especial naturaleza**, los datos con trascendencia tributaria tienen una serie de peculiaridades que hacen que su tratamiento tenga diferencias respecto al tratamiento del resto de datos personales. Se consideran datos con trascendencia tributaria aquellos datos, informes o antecedentes obtenidos por la Administración tributaria en el desempeño de sus funciones. Dichos datos, según lo establecido por la Norma Foral General Tributaria, tienen **carácter reservado**. Este carácter reservado supone que:

2. Los datos con trascendencia tributaria **solo** pueden ser utilizados para la efectiva aplicación de los tributos o recursos cuya gestión tenga encomendada la Administración tributaria, y para la imposición de las sanciones que procedan;
3. **No es posible ceder o comunicar los datos** con trascendencia tributaria salvo que se den alguno de los supuestos tasados por el artículo 94.1 de la Norma Foral General Tributaria.

Asimismo, la Norma Foral General Tributaria establece para todas aquellas entidades que ejerzan funciones públicas, el **deber de informar y colaborar** con la Administración Tributaria lo cual supone que las mismas **deberán facilitar** cuantos datos, informes y antecedentes con trascendencia tributaria recabe la Administración Tributaria mediante disposiciones de carácter general o a través de requerimientos concretos, y a prestarle apoyo, concurso, auxilio y protección para el ejercicio de sus funciones.

Por tanto, la especial naturaleza de los datos con trascendencia tributaria, el **gran número de datos** de este tipo que se recaban y las estrictas reglas que la Norma Foral General Tributaria establece en relación a su tratamiento y cesión, hacen que esta realidad haya sido tenida en cuenta en el diseño del Plan de Adecuación. Concretamente, se han establecido **procedimientos específicos** para este tipo de datos con el fin de verificar que los mismos se tratan siguiendo la normativa especial de aplicación. Dichos procedimientos buscan garantizar que la comunicación de datos con trascendencia tributaria únicamente se realiza en aquellos casos habilitados por la normativa de aplicación, y para asegurar que los mismos **únicamente se tratan para las finalidades habilitadas** por la normativa tributaria.

Finalmente, cabe destacar la importante labor de **concienciación** que se ha llevado a cabo para procurar que el personal que accede a diario a los datos con trascendencia tributaria guarde el debido **sigilo** sobre los mismos. Así, se han establecido mecanismos como la **auditoría aleatoria de los registros de accesos** a los diferentes expedientes electrónicos lo cual permite que se reduzcan los accesos a expedientes cuya tramitación no corresponde al empleado/a público que realizaba el acceso.

iv. Pluralidad de realidades y diferentes estructuras organizativas

Como se ha expuesto en líneas anteriores, el Sector Público Foral está formado no solo por una institución pública dotada de numerosas e importantes competencias como es la Diputación, sino también por **numerosas Entidades Forales** que ejercen su actividad con personalidad jurídica diferenciada, patrimonio y tesorería propios, así como autonomía de gestión. Esto hace que en el Sector Público Foral existan **numerosas y diferentes estructuras organizativas** y que, por tanto, el esquema de trabajo del Plan de Adecuación haya tenido que adaptarse a la totalidad de realidades existentes.

Así, por ejemplo, el Plan ha tenido que desarrollarse con la **flexibilidad** necesaria para que el mismo sea de utilidad para que cumpla con la normativa de protección de datos tanto una Entidad Foral como Sestao Bai, S.A. que trata fundamentalmente datos de contacto de personas trabajadoras de las empresas a las que presta sus servicios, como el Instituto Foral de Asistencia Social (IFAS) que cuenta con 13 centros asistenciales repartidos por todo el Territorio Histórico y presta servicios sociales especializados para personas con discapacidad, mayores, menores y demás colectivos vulnerables, debiendo, por tanto, tratar numerosos **datos de salud**.

Por tanto, las **diferencias organizativas**, las **diversas realidades existentes** en relación a los tratamientos de datos personales, y el funcionalmente **descentralizado** dada la autonomía de gestión de las Entidades Forales, ha planteado importantes desafíos a la hora de lograr que el Plan de Adecuación establezca un **marco estandarizado de cumplimiento de la normativa de protección de datos** dentro del Sector Público Foral. Como se desarrollará a lo largo de los siguientes epígrafes, el rol de la Dirección General de Buen Gobierno y Transparencia del Gabinete de Estrategia Digital y Corporativa de la Diputación Foral de Bizkaia, como referente en materia de protección de datos para todo el Sector Público Foral, unida al firme propósito de la Diputación de mantener un **minucioso respeto por la privacidad** de los datos personales, han sido claves a la hora de diseñar un Plan de Adecuación que se adapta y tiene en cuenta todas las realidades existentes, y **responde a sus necesidades y demandas en materia de protección de datos**.

v. Visibilidad pública y compromiso con la transparencia

Uno de los ejes de actuación en los que se sustenta el *Plan Foral de Transparencia y Datos Abiertos 2020-2022*⁵ de la Diputación Foral de Bizkaia, es **acercar la Diputación a las personas de Bizkaia**, facilitando que estas conozcan la Institución y la labor que desarrolla. El desarrollo de este importante eje de actuación precisa de acciones concretas entre las que se encuentra el **despliegue del modelo de gestión de la privacidad** (la protección de datos y la seguridad de la información) en la Diputación Foral de Bizkaia y en las Entidades Forales, que es objeto de desarrollo en la presente Memoria.

En materia de **protección de datos** este compromiso con la transparencia del Sector Público Foral del Territorio Histórico de Bizkaia **se alinea con el principio de transparencia acuñado por el RGPD** el cual exige que toda información y comunicación

⁵ Diputación Foral de Bizkaia, 2020. *Plan Foral de Transparencia y Datos Abiertos*. Disponible en www.gardentasuna.bizkaia.eus/es/plan-foral-memorias

relativa al tratamiento de los datos personales sea **fácilmente accesible y fácil de entender**, y que se utilice un lenguaje sencillo y claro. En la práctica, este compromiso con la transparencia en el ámbito de la protección de datos se ha traducido en la elaboración de textos en protección de datos que buscan ante todo la **claridad, la sencillez y la transparencia**. Asimismo, como se desarrollará a lo largo de la presente Memoria, tanto la web de la Diputación, como las de todas y cada una de las Entidades Forales, cuentan con un **apartado específico de protección datos** donde se cumplen las **obligaciones de transparencia** que exige la normativa, se da una **información clara** a la ciudadanía en esta materia y se procura que la misma sea **cercana, entendible y precisa**.

Finalmente, en relación a la **visibilidad pública**, cabe mencionar que la Diputación Foral de Bizkaia atiende a la ciudadanía a través de tres canales:



Además de la propia Diputación, también las **Entidades Forales** que integran el Sector Público Foral cuentan con sus propios canales de atención a la ciudadanía por las tres vías mencionadas.

La **pluralidad de vías** a través de las cuales la ciudadanía puede ponerse en contacto con el Sector Público Foral, hace que también sean **múltiples los escenarios** y las formas en las que estas pueden aportar datos personales. Por tanto, el reto para el Sector Público Foral en este ámbito es importante ya que se debe:

- Garantizar el deber de informar estableciendo un sistema **armonizado** de cláusulas informativas que cumplan los requisitos del artículo 13 RGPD.
- **Adecuar** las cláusulas informativas **a todos los canales** a través de los cuales se pueden recabar datos personales.
- Implementar el **principio de minimización de datos** desde la recogida de los mismos.
- **Concienciar y formar** al personal en contacto directo con la ciudadanía para evitar violaciones de seguridad, comunicaciones ilícitas de datos personales, usos no adecuados, quebras de confidencialidad, etc.

- Implementar y revisar de forma continua las **medidas técnicas** de seguridad de los sistemas y soportes a través de los cuales se recaban los datos personales.
- Etc.

Por último, cabe mencionar que la Diputación como gobierno de Bizkaia, ha de ser un **referente** también en materia de privacidad y cumplimiento normativo de la protección de datos dentro del Territorio Histórico para el resto de entidades del sector público y privado. Este deber de ejemplificar unido a la gran exposición pública con la que cuenta el Sector Público Foral, hace que el Plan se haya configurado teniendo en cuenta la estructura y realidad interna de las organizaciones, pero también **el impacto exterior** y la correcta **comunicación** de las actuaciones que la Diputación y las Entidades Forales llevan a cabo en materia de privacidad.

2.2. Marco normativo de la protección de datos en el Sector Público Foral del Territorio Histórico de Bizkaia

Como se ha mencionado en líneas anteriores, el Sector Público Foral cuenta con una serie de **especialidades organizativas y particularidades competenciales derivadas de los derechos históricos forales que reconoce la Constitución**.

Con el objeto de adaptar el cumplimiento de la normativa de protección de datos a las especificidades del Sector Público Foral, se han aprobado una serie de **disposiciones normativas** cuyo objetivo es la organización interna para el cumplimiento normativo en esta materia, así como la aprobación de una serie de herramientas, procedimientos y normas de actuación que permitan abordar el cumplimiento normativo en materia de protección de datos de forma satisfactoria.

Entre las disposiciones normativas aprobadas por la Diputación en materia de protección de datos y que se mencionarán a lo largo de la presente Memoria, **destacan** las siguientes:



- Crea los siguientes roles en materia de protección de datos y seguridad de la información:
 - Personas dinamizadoras.
 - Comisión Interdepartamental de Dirección en materia de protección de datos de carácter personal.



- Modifica el Decreto Foral 173/2013.
- Se modifican las atribuciones competenciales en materia de protección de datos que en el Decreto Foral 173/2013 se hacían al Departamento de Presidencia, por la mención genérica a la Dirección General que ostente la competencia de implantación de medidas organizativas, de infraestructura, aplicaciones y servicios en materia de protección de datos de carácter personal.



- Aprueba la Política de seguridad de la información del Sector Público del Territorio Histórico de Bizkaia.
- La Comisión Interdepartamental de Dirección en materia de protección de datos de carácter personal, ejercerá también funciones en materia de seguridad de la información denominándose Comité de Dirección cuando actúe en este ámbito.
- El Comité de Dirección ejercerá diversas funciones en materia de seguridad de la organización entre las que destacan la coordinación de todas las competencias en esta materia.



- Norma Interna que establece los requisitos de seguridad que ayuden a las personas usuarias de Diputación a utilizar adecuadamente la infraestructura y recursos informáticos dispuestos por la Institución.



- Designa formalmente y regula la figura de la persona Delegada de protección de datos del Sector Público del Territorio Histórico de Bizkaia.
- Establece las tareas y acciones a desempeñar por la persona Delegada de protección de datos.
- Identifica a las personas componentes de la Sección de Asesoramiento Jurídico, Seguridad de la información y Protección de la Dirección General de Buen Gobierno y Transparencia como personal de apoyo a la persona Delegada de protección de datos.



- La Comisión Interdepartamental de Dirección en materia de protección de datos y el Comité de Dirección en seguridad de la información proceden a identificarse de manera unívoca y conjunta con el nombre de Comité de Dirección en materia de protección de datos y seguridad de la información del Sector Público Foral y aglutina las funciones correspondientes a la materia de protección de datos y a la de seguridad de la información.



- Aprueba la creación, regulación y publicación del Registro de Actividades de Tratamiento de datos personales de la Diputación Foral de Bizkaia (en adelante, RAT).
- Aprueba que el RAT sea objeto de mantenimiento y revisión periódica de manera transversal y conjunta entre Responsables de tratamiento de cada Departamento Foral (Direcciones Generales) y el Gabinete de Estrategia Digital y Corporativa, y que las modificaciones, correcciones y actualizaciones que se produzcan sean comunicadas para dación en cuenta al Comité de Dirección en Materia de protección de datos y seguridad de la información del Sector Público Foral.
- Aprueba que el RAT, además de ser el Inventario de tratamiento de datos personales, constituya la 2.ª capa de Información completa y necesaria de cada actividad de tratamiento de datos personales.



- Aprueba que durante el proceso de elaboración y mantenimiento del RAT se implementen las medidas técnicas y organizativas apropiadas y necesarias para garantizar el cumplimiento de la normativa de protección de datos en lo que respecta a la materia de seguridad y en especial de seguridad de la Información en el ámbito del Esquema Nacional de Seguridad (ENS), de modo que se minimicen los riesgos para los derechos y libertades de las personas físicas durante el tratamiento de datos personales.
- Instrucción para la incorporación en los Decretos por los que se regula la estructura orgánica de los Departamentos Forales y los Gabinetes, las funciones y responsabilidades que desempeñan:
 - Las personas dinamizadoras en materia de protección de datos y seguridad de la información;
 - Las Direcciones Generales en calidad de Responsables de tratamiento en materia de protección de datos y en calidad de Responsables de información en materia de seguridad de información.

2.3. Situación del Sector Público Foral del Territorio Histórico de Bizkaia en relación a los tratamientos de datos personales realizados antes de la aplicación del RGPD

Antes de la efectiva aplicación del RGPD en mayo de 2018, el Sector Público Foral cumplía con las exigencias de la normativa existente en la realidad anterior a la actual normativa en todos los actos y disposiciones que trataban datos personales.

En primer lugar, la derogada *Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de Carácter Personal* y el *Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal* establecían el marco del cumplimiento de las obligaciones que se imponían a los Responsables del Fichero.

La creación de los ficheros se realizaba mediante Orden Foral aprobada por el Departamento o Gabinete correspondiente, y **publicada en el Boletín Oficial de Bizkaia** y comunicada a la Agencia Vasca de protección de datos para la incorporación a su Registro de Ficheros. Los Responsables del Fichero eran las diferentes **Direcciones Generales** de los correspondientes Departamentos o Gabinetes de Diputación Foral de Bizkaia.

En la Diputación Foral de Bizkaia y el organismo autónomo foral IFAS contaban respectivamente con **107** y **7 ficheros** inscritos en el Registro de protección de datos de la **Agencia Vasca de protección de datos (AVPD)**.

Nombre del fichero	Descripción de la finalidad
BFA 02031 - ORIENTACIÓN A PERSONAS MAYOR...	RECOGER LOS DATOS BÁSICOS PARA LA IDENTIFICACIÓN DE LA PERSONA MAYOR Y SU PROBLE...
BFA 03301 - CARPETA SOCIAL	GESTIÓN INTEGRAL EN LA PRESTACIÓN DE SERVICIOS SOCIALES.
BFA 09105 - SERVICIOS GENERALES EN EL DE...	GESTIÓN DE SERVICIOS INTERNOS EN EL DEPARTAMENTO. OTROS REGISTROS ADMINISTRATIVO...
BFA013001 PARTICIPANTES PROCESOS E INICI...	FACILITAR INFORMACIÓN A LAS PERSONAS PARTICIPANTES EN LOS PROCESOS DE PARTICIPAC...
BFA02001 - GESTIÓN DEL LABORATORIO ANIMA...	CONTROL SANITARIO DE GANADO
BFA02031022 - PROMOCIÓN DEL ENVEJECIMIEN...	PROMOCIÓN DEL ENVEJECIMIENTO ACTIVO Y DE LA PARTICIPACIÓN SOCIAL DE LAS PERSONAS...
BFA02100 - EXPEDIENTES SANCIONADORES EN ...	GESTIÓN DE LOS EXPEDIENTES SANCIONADORES DE LA DIRECCIÓN GENERAL DE AGRICULTURA...
BFA02101 - COMPENSACIONES	GESTIÓN DE PROGRAMAS DE COMPENSACIONES
BFA02105 - REGISTRO Y CONTROL DE ACTIVID...	REGISTRO Y CONTROL DE ACTIVIDADES DE CAZA Y PESCA E INTERACCIONES CON EL MEDIO N...
BFA02106 - PLAN TERRITORIAL SECTORIAL AGR...	GESTIÓN DE PROCEDIMIENTOS ADMINISTRATIVOS

Registro de Ficheros de la AVPD

Asimismo, las restantes 20 Entidades Forales también cumplían con la normativa aplicable y contaban con ficheros, que, por su diferente naturaleza jurídica, se inscribían en el Registro General de la Agencia Española de Protección de datos (AEPD).

En segundo lugar, cabe mencionar que estos ficheros, en su mayoría, eran de nivel **medio y alto** y su legitimación se encontraba en el consentimiento de las personas interesadas y en el ejercicio de las competencias atribuidas a la Diputación dada su condición de Administración Pública.

Destaca también el cumplimiento del **derecho de información** de las personas interesadas al cual se daba cumplimiento mediante la incorporación de los pertinentes avisos legales en los soportes de recogida de datos, los cuales contenían la información exigida por el artículo 5 de la Ley 15/1999.

En tercer lugar, el Sector Público Foral realizaba **auditorias bienales formales** en las que se revisaba el cumplimiento de las disposiciones normativas establecidas en ambos textos normativos y, especialmente, la correcta implementación de las medidas de seguridad detalladas por el citado Real Decreto en función del nivel de seguridad de los ficheros.

Por último, con relación a la **estructura de seguridad**, las medidas de seguridad se diseñaban en función del nivel de protección establecido por el *Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999*, en cuanto a la atribución de los niveles de seguridad: básico, medio, alto.



3. PLAN DE ADECUACIÓN

3.1. Alcance y objetivos del Plan de Adecuación

Tal y como se ha descrito en anteriores epígrafes, el alcance principal del Plan de Adecuación son todas aquellas **entidades que forman parte del Sector Público Foral del Territorio Histórico de Bizkaia**, el cual está compuesto por la propia Diputación Foral y sus Entidades Forales.

En relación a los objetivos del Plan que es objeto de desarrollo en la presente Memoria, cabe indicar que el objetivo fundamental y último es el cumplimiento por parte del **Sector Público Foral** de **la normativa** de protección de datos (RGPD y LOPDGD). Este objetivo principal se divide a su vez en una serie de objetivos individualizados cuya consecución permite alcanza el objetivo principal. Dichos objetivos son los siguientes:



No obstante lo anterior y teniendo en cuenta que una de las competencias que ejerce la Diputación Foral de Bizkaia es prestar **ayuda y asesoramiento en materia jurídica**, económica y técnica a las **Entidades Locales** del Territorio Histórico de Bizkaia, cabe destacar que en el marco del Plan de Adecuación llevado a cabo se ha tenido en cuenta la realidad de estas Entidades y, aunque no han sido objeto del Plan de Adecuación descrito en la presente Memoria, si se han promovido diferentes actuaciones por parte de la Diputación orientadas a **facilitar el cumplimiento normativo** en protección de datos de las mismas. Y es que, ante la necesidad de afrontar las modificaciones recogidas en el nuevo marco jurídico de protección de datos, se antojaba necesario que estas Entidades Locales tuviesen un **soporte, asesoramiento y asistencia de tipo técnico y jurídico** en la materia. Atendiendo a esta necesidad, la Central de Contratación Foral de Bizkaia aprobó un **Acuerdo marco de asesoramiento jurídico y de medidas técnicas y organizativas en materia de protección de datos** para resolver las dificultades que se plantean durante la implantación y el seguimiento de los controles establecidos para la protección de datos y el cumplimiento de la normativa, que les permita continuar avanzando en su adecuación a la legislación vigente en esta materia.



El citado Acuerdo Marco está dividido en varios lotes y su objeto es la adecuación de las Entidades de Bizkaia adheridas al mismo a la normativa de protección de datos, así como la contratación de la figura de Delegado/a de Protección de datos. Concretamente, además de la propia Diputación y de sus Entidades Forales, se adhirieron **31 entidades locales** a las que las empresas adjudicatarias prestarán los servicios indicados. Las entidades adheridas son las siguientes:

Ayuntamiento de Areatza	Ayuntamiento de Loiu
Ayuntamiento de Arrigorriaga	Ayuntamiento de Mallabia
Ayuntamiento de Artzentales	Ayuntamiento de Mungia
Ayuntamiento de Bermeo	Ayuntamiento de Murueta
Ayuntamiento de Busturia	Ayuntamiento de Nabarniz
Ayuntamiento de Derio	Ayuntamiento de Sondika
Ayuntamiento de Durango	Ayuntamiento de Valle de Trápaga - Trapagaran
Ayuntamiento de Ereño	Ayuntamiento de Zaldibar
Ayuntamiento de Etxebarri	Ayuntamiento de Zamudio
Ayuntamiento de Fruiz	Consorcio de Transportes de Bizkaia (CTB)
Ayuntamiento de Galdakao	Mancomunidad Busturialdea
Ayuntamiento de Galdames	Mancomunidad Durango
Ayuntamiento de Iurreta	Mancomunidad Lea Artibai
Ayuntamiento de Kortezubi	Mancomunidad Mungialde
Ayuntamiento de Larrabetzu	Mancomunidad Txorierrri
Ayuntamiento de Lezama	

Por tanto, como se puede comprobar la envergadura de las labores llevadas a cabo por la Diputación Foral de Bizkaia para lograr el cumplimiento de la normativa de protección de datos no solo en el Sector Público Foral, sino en todo el Territorio Histórico de Bizkaia, es de importante consideración. Todo ello fruto del compromiso que tiene la Diputación en respetar la privacidad de la ciudadanía y de hacer de Bizkaia un territorio transparente y respetuoso con la intimidad de las personas.

3.2. Contenido, fases y acciones

Los citados objetivos del Plan de Adecuación han sido estructurados en **seis fases** de trabajo las cuales están a su vez compuestas por una serie de **acciones** cuyo desarrollo ha permitido alcanzar los mismos. Las fases son:

- Fase I. Análisis del estado de situación
- Fase II. Diseño del plan de acción
- Fase III. Creación del modelo de gobernanza corporativa para la protección de datos y seguridad de la información
- Fase IV. Implementación del Plan de Adecuación
- Fase V. Formación y concienciación
- Fase VI. Control, revisión y mejora continua

Las **diferentes realidades** existentes dentro del Sector Público Foral, unidas a los diferentes **retos** que se han expuesto y que debe afrontar el cumplimiento de la normativa de protección de datos en las organizaciones que lo integran, han sido claves a la hora de diseñar el Plan de Adecuación cuyo contenido es objeto de detalle en las siguientes líneas.

Asimismo, cabe destacar que este Plan de Adecuación se ha sustentado fundamentalmente en **cuatro pilares** que han inspirado el diseño, ejecución e implementación de las diferentes acciones desarrolladas dentro de cada una de las seis fases identificadas dentro del Plan.



En los siguientes epígrafes se expondrá en detalle el contenido del Plan de Adecuación, desarrollando cada una de las acciones principales llevadas a cabo para lograr los objetivos pretendidos e indicados en el presente epígrafe.

Tal y como se detalla en el epígrafe relativo al Modelo de Gobernanza Corporativa, las acciones identificadas dentro de cada una de las fases en las que se divide el Plan de Adecuación descrito, están lideradas por un equipo de personas **especializadas** en la materia que integran la **Sección de Asesoramiento Jurídico, seguridad de la información y protección de datos** de la Dirección General de Buen Gobierno y Transparencia perteneciente al Gabinete de Estrategia Digital y Corporativa y la persona Delegada de protección de datos del Sector Público Foral. Estas personas asesoran y apoyan de forma directa a cada una de las personas Responsables del Tratamiento designadas dentro de cada una de las Direcciones Generales de Diputación y las Entidades Forales.

3.2.1. Fase I. Análisis del estado de situación

Para el diseño de un Plan de Adecuación que permita alcanzar los objetivos indicados con eficacia y eficiencia, la Diputación Foral de Bizkaia considera fundamental conocer la **situación** en la que se encuentran la propia Diputación y sus Entidades Forales en relación al cumplimiento de las novedades normativas que introdujo el RGPD. Por ello, el Plan de Adecuación descrito en la presente Memoria, se inició con esta **primera fase de análisis del estado de situación**. Tal y como se ha detallado en anteriores epígrafes, este análisis concluyó que el Sector Público Foral contaba con un **estado óptimo de cumplimiento de la anterior normativa** de protección de datos, así como una estructura de seguridad sólida formada por diferentes roles que se responsabilizaban en garantizar el cumplimiento normativo.

El conocimiento de la situación permitió identificar aquellas labores prioritarias que se precisaban implementar para **adecuar la Diputación y sus Entidades Forales a las numerosas novedades normativas impuestas por la norma europea**. Así, se identificaron una serie de acciones cuyo inicio y desarrollo era necesaria bien por ser novedosas, o bien por ser consecuencia directa del cambio de enfoque de la nueva normativa.

Una de las acciones prioritarias que se iniciaron con esta fase de análisis, es la aplicación y despliegue del **principio de responsabilidad proactiva**. La Diputación Foral de Bizkaia considera necesario analizar **qué datos personales se tratan**, con qué **objetivos** y **qué tipo de operaciones de tratamiento** se llevan a cabo y, a partir de esta realidad e infraestructura de datos, **decidir las medidas a adoptar** para asegurar su cumplimiento en función de los riesgos detectados y asumidos. Cumplir con este principio, esto es, ser **proactivo y organizado** supone evidenciar los pasos que se han dado para su cumplimiento.

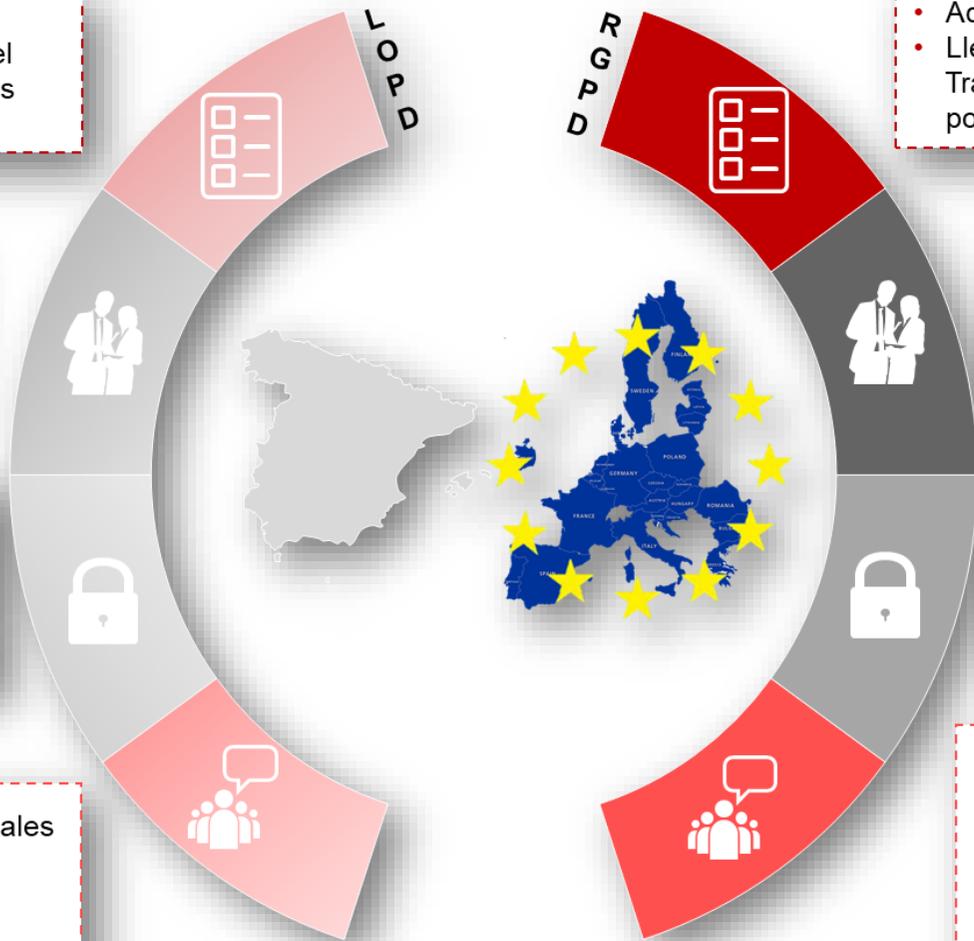
En la siguiente infografía se resumen los principales cambios que se identificaron como necesarios, que se **priorizaron** con objeto de adecuar al Sector Público Foral a la nueva normativa, y que han sido desplegados mediante las fases que forman el citado Plan.

- Existencia de ficheros
- Obligación de inscribir los ficheros en el Registro de Ficheros gestionado por las Autoridades de Control

- Responsable del Fichero
- Responsable de Seguridad

- Listado de medidas de seguridad detallado en el *RD 1720/2007, de 21 de diciembre* en función del nivel de seguridad de los ficheros (básico, medio y alto)

- Las personas titulares de datos personales ostentan los siguientes derechos: información, acceso, rectificación, cancelación, oposición



- Actividades de Tratamiento
- Llevanza de un Registro de Actividades de Tratamiento y publicación para que sea accesible por medios electrónicos

- Responsable del Tratamiento
- Responsable de Seguridad: seguridad de la información
- Delegado/a de Protección de Datos: protección de datos

- Se deberán adoptar las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado

- Las personas titulares de los datos ostentan los siguientes derechos: información, acceso, rectificación, supresión, oposición, olvido, portabilidad, limitación del tratamiento, a no ser objeto de decisiones individuales automatizadas incluida la realización de perfiles

Como se puede observar, son múltiples los cambios cuyo desarrollo era necesario para garantizar la adecuación a la nueva normativa. Cambios que, en muchos casos, requerían de una dotación de recursos, medios y personas y, por tanto, la gestión de los mismos debía ser abordada desde un **enfoque transversal** y con la intervención de personas responsables.

En primer lugar, con objeto de **analizar el estado de situación** y dada la multitud de realidades existentes en el Sector Público Foral en relación a la protección de datos, se consideró fundamental **conocer la realidad de los tratamientos de datos** que se estaban realizando y poder adecuar los mismos a las nuevas exigencias normativas. Para ello, se procedió a **identificar y analizar el contenido de los antiguos ficheros** para la creación de las actividades de tratamiento llevadas a cabo por cada Dirección General y Entidad Foral. Una vez identificados estos, se procedió a revisar los tratamientos de datos realizados y a **documentar el ciclo de vida** de los mismos con el objeto de poder analizar la legalidad de dichos tratamientos y documentar debidamente el Registro de Actividades de Tratamiento de la Diputación y de las Entidades Forales.

En segundo lugar, para lograr el citado objetivo, el personal de la **Sección de Asesoramiento Jurídico, seguridad de la información y protección de datos**, liderado por la persona DPO, mantuvo las necesarias reuniones de toma de datos con aquellas personas identificadas por cada Dirección y entidad Responsable del Tratamiento por conocer la realidad de los tratamientos de datos personales a revisar. Dichas reuniones de toma de datos permitieron **documentar una ficha para cada Actividad de Tratamiento** identificada donde se recogían, entre otras cuestiones, el **ciclo de vida de los datos**. La información recopilada en estas fichas es fundamental no solo para conocer el estado de situación y analizar el mismo, sino también para la elaboración del **Registro de Actividades de Tratamiento**, para realizar los perceptivos **análisis de riesgos**, así como para la **mejora y análisis continuo** de los tratamientos de datos realizados por las organizaciones.



6

3.2.2. Fase II. Diseño del plan de acción

Una vez conocido el estado de situación en materia de protección de datos y recopilada la información necesaria de cada una de las actividades de tratamiento llevadas a cabo por las diferentes Direcciones Generales y Entidades Forales Responsables del Tratamiento, se procedió a **identificar las principales acciones a acometer** para cumplir con las obligaciones de la nueva normativa. Una vez identificadas estas, se procedió a elaborar un **plan de acción** en el que se detallaban las acciones a implementar y se planificaba la ejecución de las mismas en función de la prioridad asignada a cada una de ellas.

Este plan de acción, por tanto, es **la hoja de ruta básica** que ha permitido el desarrollo y ejecución del presente Plan de Adecuación.

Las acciones identificadas dentro del plan de acción permitieron dividir el mismo en las fases que se detallan en el presente documento, lo cual supuso una mejora en la organización y efectiva aplicación del mismo. A continuación, se detallan las **acciones identificadas** dentro del plan de acción, así como su **encaje dentro de las fases** que forman el presente Plan de Adecuación:

⁶ Por motivos de espacio no se recoge el contenido completo de la Ficha.

Fases

I

II

III

IV

V

VI

Diseño del plan de acción:

- Identificación y **priorización** de acciones para acometer el cumplimiento normativo:
- Despliegue del **principio de protección de datos desde el diseño y por defecto**: se ha de tener en cuenta la privacidad desde el origen de cualquier nuevo desarrollo tecnológico y nuevo servicio a prestar a la ciudadanía.
- Creación de una cultura de prevención de riesgos.

Implementación del Plan de Adecuación:

- Revisión de las **bases legitimadoras** de los diferentes tratamientos de datos personales.
- Revisión del cumplimiento del **deber de informar**.
- Actualización de los procedimientos de ejercicio de **derechos** e introducción de los nuevos derechos.
- Elaboración y publicación de los **Registro de Actividades de Tratamiento**.
- Realización de los **análisis de riesgos**, y se regulan, incorporan y realizan los procedimientos para las **evaluaciones de impacto**.

Análisis del estado de situación:

- Despliegue del **principio de responsabilidad proactiva**: conocer qué datos personales se tratan, con qué objetivos y qué tipo de operaciones de tratamiento se llevan a cabo y, a partir de esta realidad e infraestructura de datos, decidir las medidas a adoptar para asegurar su cumplimiento en función de los riesgos detectados y asumidos.

Creación del modelo de gobernanza corporativa:

- Creación y nombramiento del rol de persona **Delegada de Protección de Datos**.
- Diseño y alcance de los roles de **Responsable de Tratamiento y Encargados de tratamiento**.
- Diseño de roles dentro de la **organización** del Sector Público Foral en materia de protección de datos:
 - Capa de dirección y gobierno.
 - Capa operativa.
 - Capa de supervisión y control.
- Determinar las funciones y obligaciones de los diferentes roles.

Formación y concienciación:

- Diseño de **planes formativos y de concienciación específicos** para todo el personal empleado foral con el objetivo de generar una cultura de compromiso y concienciación.

Control, revisión y mejora continua

A lo largo de los siguientes epígrafes se detallan las acciones principales que se han llevado a cabo dentro de cada una de las fases indicadas, así como el detalle de las mismas y su especificidad en relación a su aplicación a la particularidad realidad del Sector Público Foral del Territorio Histórico de Bizkaia.

3.2.3. Fase III. Creación del modelo de gobernanza corporativa para la protección de datos y seguridad de la información

Analizada la organización y estructura de protección de datos y seguridad de la información que existía se identificó como labor prioritaria la **creación y refuerzo de una serie de nuevos roles**, comités y órganos a los que se dotaron de recursos humanos y competencias específicas relacionadas con la protección de datos y la seguridad de la información.

El modelo de gobernanza corporativa está formado por los roles que se muestran en la siguiente imagen y que serán analizados en los siguientes apartados:

MODELO ORGANIZATIVO DE LA DIPUTACIÓN FORAL DE BIZKAIA Y ENTIDADES FORALES (SECTOR PÚBLICO FORAL) PARA LA PROTECCIÓN DE DATOS Y LA SEGURIDAD DE LA INFORMACIÓN



La creación y nombramiento de los diferentes roles que forman parte del modelo de gobernanza corporativa para la protección de datos y seguridad de la información se ha realizado mediante la aprobación de diferentes **disposiciones normativas de carácter organizativo** cuya aprobación comenzó en el 2013 y que han continuado una vez aprobado el RGPD.

Tal y como se detalla en la presente Memoria, una de las principales características de los roles creados a través de las correspondientes disposiciones normativas es que todos ellos son desempeñados por personas que han sido **formadas de forma**

específica en materia de protección de datos. Asimismo, estos roles han sido nombrados teniendo en cuenta la pluralidad de realidades y la organización interna existente dentro del Sector Público Foral, de manera que todos los roles puedan ser nombrados en cada una de las entidades recogidas en el alcance del presente Plan de Adecuación y se les dote de los recursos necesarios para ejercer sus funciones con eficacia y eficiencia.

A destacar también, la existencia de una **estructura de seguridad sólida, formada por personas especializada en la materia** y con conocimiento del funcionamiento interno de la Diputación y de las diferentes Entidades Forales, es clave en el éxito de este Plan de Adecuación y en el logro de los objetivos marcados al inicio del mismo.

A continuación, se detallan los roles existentes en materia de protección de datos dentro del Sector Público Foral, junto con las competencias, funciones y responsabilidades de cada uno de ellos.

i. Comité de Dirección en materia de protección de datos y seguridad de la información del Sector Público Foral

Órgano directivo de carácter colegiado que **coordina** las actuaciones del Sector Público Foral en materia de protección de datos y seguridad de la información, y que ostenta la máxima capacidad para la adopción de decisiones en estas materias.

Entre sus **funciones** destacan las siguientes:

- **Supervisar, impulsar y coordinar** la aplicación efectiva por parte del Sector Público Foral de la normativa y planes vigentes en materia de protección de datos y seguridad de la información.
- **Coordinar** las medidas a adoptar por el Sector Público Foral en la aplicación del cumplimiento de la legislación aplicable y buenas prácticas en materia de protección de datos.
- **Dirigir y supervisar** el trabajo de las personas dinamizadoras designadas en cada departamento y Entidad Foral, encargadas de realizar labores de interlocución e impulso de acciones en esta materia.
- Atender inquietudes de la **alta dirección** y transmitirselas a las personas Responsables del Tratamiento pertinentes, para recabar respuestas y soluciones que se comunicarán de nuevo a la alta dirección.
- Recabar de las personas responsables de seguridad del Sector Público Foral los informes sobre el estado de la seguridad y resumirlos para la alta dirección.
- Aprobar el **Análisis de Riesgos** y establecer el Nivel de Riesgo no Aceptable.

Este Comité está integrado de la siguiente manera:



ii. Persona Delegada de protección de datos

La designación formal y la regulación de la figura de la persona Delegada de protección de datos del Sector Público Foral del Territorio Histórico de Bizkaia, se llevó a cabo mediante el **Acuerdo 11/2018, de 15 de mayo, de la Diputación Foral de Bizkaia citado en anteriores epígrafes.**

Las funciones y el cargo de la persona Delegada de protección de datos (en adelante, DPO) son ejercidas por la **Jefatura de la Sección de Asesoramiento Jurídico, Seguridad de la información y Protección de datos**, adscrita directamente a la Dirección General de Buen Gobierno y Transparencia del Gabinete de Estrategia Digital y Corporativa de la Diputación Foral de Bizkaia.

Además de las **funciones** que tanto el RGPD como la LOPDGDD atribuyen a esta figura, la persona Delegada de protección de datos realiza las tareas específicas detalladas en el citado Acuerdo 11/2018, de 15 de mayo. A continuación, se recoge un listado no exhaustivo de dichas funciones:

Respecto a las operaciones de tratamiento

- **Detectar y revisar, asesorar y auditar** las posibles novedades, cambios, modificaciones o supresiones de actividades de tratamiento de datos de carácter personal realizados por los Responsables y/o Encargados del Tratamiento.
- Revisar, asesorar y auditar con precisión los **principios del tratamiento**, las **finalidades y la base jurídica** o la compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos de los tratamientos, que llevan a cabo los Responsables y/o Encargados del Tratamiento.
- Revisar, asesorar y auditar las **disposiciones y normativas reguladoras** que amparen los tratamientos basados en el ejercicio de potestades o intereses públicos realizados por los Responsables y/o Encargados del Tratamiento. En concreto, detectará normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
- Revisar, asesorar y auditar los **análisis de los riesgos** asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento realizados por los Responsables y/o Encargados del Tratamiento.

Respecto al cumplimiento normativo

- Informar, asesorar y emitir **recomendaciones** a los diferentes Responsables y/o Encargados del Tratamiento.
- Revisar y asesorar sobre las **normas y procedimientos** que en materia de seguridad afecten a las actividades de tratamiento de los datos, incluida la asignación de responsabilidades de los diferentes Responsables y/o Encargados del Tratamiento.
- Participar en la planificación y ejecución destinada a **concienciar y formar** en materia de protección de datos.
- Participar de forma adecuada y en tiempo oportuno **en todas las cuestiones relativas a la protección de datos personales** mediante reuniones con las diferentes Áreas, Direcciones o Secciones de los diferentes Responsables y/o Encargados del Tratamiento
- Asesorar en la valoración de la adhesión a **códigos de conducta** o certificaciones/sellos/marcas que acrediten el cumplimiento de la organización.

Respecto a la evaluación de impacto y medidas de seguridad

- Revisar, asesorar y auditar los **análisis de riesgo** realizados por los diferentes Responsables y/o Encargados del Tratamiento, que pondere los peligros a los que se someten los derechos y libertades de los ciudadanos de los diferentes tratamientos de datos que se desarrollen.
- Asesoramiento ante si se debe llevar a cabo o no una **evaluación de impacto** de la protección de datos en los diferentes tratamientos.
- Asesorar en la **definición de la metodología** a llevar a cabo ante una evaluación de impacto.
- **Revisar, asesorar y auditar** la ejecución de una evaluación de impacto de la protección de datos.
- Revisar, asesorar y auditar las **salvaguardas** (incluidas medidas técnicas y organizativas) a aplicar para mitigar cualquier riesgo para los derechos e intereses de los afectados, así como que garanticen la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento, así como la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico. En concreto, revisará las medidas de **privacidad desde el diseño y por defecto** adecuadas a los riesgos y naturaleza de los tratamientos.
- Revisar, asesorar y auditar los procesos de verificación, evaluación y valoración reguladores de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento. En concreto, supervisará el **diseño e implantación de políticas de protección de datos** en la organización.

Respecto a las relaciones con terceros

- Revisar, asesorar y auditar las **cláusulas y avisos legales** utilizados para informar a las personas interesadas cuando se recaban sus datos personales.
- Diseñar y ordenar la implantación de **medidas de información** a los afectados por los tratamientos de datos.
- Revisar, asesorar y auditar las cláusulas y modelos de contratos, convenios, encomiendas o cualquier otro instrumento jurídico que articule las relaciones jurídicas con **encargados de tratamiento** o terceras personas de acuerdo a lo previsto en la normativa de protección de datos.
- **Evaluación de las garantías** ofrecidas por potenciales encargados de tratamiento en el ámbito del cumplimiento de la normativa de protección de datos.

- Recomendar las **instrucciones y medidas de seguridad** concretas a aplicar por las personas encargadas del tratamiento.
- Control y supervisión de las **medidas de seguridad efectivamente implantadas** por las personas encargadas del tratamiento.
- Revisar, asesorar y auditar los **procedimientos de atención de ejercicios de derechos de la ciudadanía**, implantados tanto por los responsables como por las personas encargadas del tratamiento.
- Valoración previa de **transferencias internacionales de datos** y la necesidad de requerir autorización de las autoridades de protección de datos.

La persona Delegada de protección de datos desempeña estas funciones con el **apoyo** principal de las personas componentes de la **Sección de Asesoramiento Jurídico, Seguridad de la información y protección de datos** objeto de análisis en el siguiente apartado. Asimismo, también se **apoya** para el ejercicio de sus funciones en las personas dinamizadoras en materia de protección de datos y de seguridad de la información designadas por cada Departamento y Gabinete Foral, y en las personas Responsables en protección de datos designada por las Entidades Forales.

Respecto a su cualificación y competencias, habiendo sido designada como DPO a la persona que ocupe el puesto de Jefatura de la Sección, y considerando que dicho puesto se ha de cubrir necesariamente con personal específicamente capacitado por su titulación, se ha cubierto el mismo en este sentido. Con el objetivo de mantener un nivel adecuado de conocimientos y poder desempeñar sus funciones de manera adecuada a su perfil, tanto el DPO como su equipo realizan formaciones periódicas para mantener y actualizar sus conocimientos respecto a las novedades en protección de datos.

Finalmente, cabe mencionar que el criterio jurídico de la persona DPO respecto a sus funciones y tareas, se manifiesta con imparcialidad ya que en su posición jurídica está dotada de independencia respecto a las decisiones de otros órganos, no pudiendo recibir instrucciones de carácter político ni técnico para el desempeño de su puesto. Sus opiniones no se someterán ni será tutelada ni deberá acompañarse **ni refrendarse por otros órganos superiores** de la Diputación Foral de Bizkaia.

Se muestra imagen de la publicación en Bizkaia.eus de la figura:



NORMATIVA Y DPO

NORMATIVA

PERSONA DELEGADA DE PROTECCIÓN DE DATOS (DPO)

PERSONA DELEGADA DE PROTECCIÓN DE DATOS (DPO)

PERSONA DELEGADA DE PROTECCIÓN DE DATOS (DPO)

La creación, designación y regulación de la **PERSONA DELEGADA DE PROTECCIÓN DE DATOS** de la Diputación Foral de Bizkaia y Entidades Forales del sector público se aprobó mediante Acuerdo del Consejo de gobierno el día 15 de mayo de 2018. La publicación de este nombramiento se realizó en el Boletín Oficial de Bizkaia en el **R.O.R.** Núm 99 de 24 de mayo de 2018 y se realizó su comunicación oficial a la Agencia Vasca de Protección de Datos (AVPD).

Contacto

Para todas las consultas en materia de protección de datos relativas a los tratamientos que realice la Diputación Foral de Bizkaia y sus Entidades Forales, pueden dirigirse [AQUÍ](#)

iii. Sección de Asesoramiento Jurídico seguridad de la información y protección de datos

Como ya se ha mencionado, la Sección de Asesoramiento Jurídico, seguridad de la información y protección de datos ostenta la importante función de ser el **principal equipo de apoyo de la persona DPO**. Además, esta Sección es la Responsable de Seguridad en el ámbito de la Diputación Foral de Bizkaia tal y como consta en la Política de Seguridad aprobada mediante el ya citado *Acuerdo de Consejo de Gobierno de 21 de marzo de 2017*.

Esta Sección está adscrita a la Dirección General de Buen Gobierno y Transparencia del Gabinete de Estrategia Digital y Corporativa de la Diputación Foral de Bizkaia. Las personas que forman parte de esta Sección son personas **especializadas** en materia de protección de datos y seguridad de la información.

Asimismo, cabe mencionar que esta Sección es la unidad administrativa a la que corresponde las funciones de participar y colaborar, **asistiendo en Derecho**, en los proyectos y planes liderados por el Gabinete de Estrategia Digital y Corporativa, así como las de elaborar y proponer los proyectos de las disposiciones administrativas generales en las materias de protección de datos y seguridad de la información. Asimismo, se le atribuye con carácter general el ejercicio de funciones orientadas al impulso, programación, asesoramiento, diseño, gestión y evaluación de las políticas y programas de actuación en los ámbitos de protección de datos y seguridad de la información.

Entre otras, son **funciones** específicas que desempeña esta Sección las siguientes⁷:

- Emitir **informes y dictámenes** en las materias de protección de datos y seguridad de la información, a instancias de la Jefatura del Gabinete, así como de las Direcciones Generales que lo componen.
- Atender las **consultas internas y externas** que demanden asistencia jurídica en materia de protección de datos y seguridad de la información.
- Analizar, informar y realizar el **seguimiento de las disposiciones normativas** comunitarias, estatales y autonómicas que se dicten en materia de protección de datos y seguridad de la información.
- Prestar **asistencia** a los Departamentos y Gabinetes Forales que deban elaborar propuestas normativas o propuestas de resoluciones administrativas para la adecuación de las materias específicas o sectoriales de su competencia a las nuevas necesidades en materia de protección de datos y seguridad de la información.
- Asesorar al Gabinete en la definición de criterios comunes de ponderación de las **limitaciones, criterios de disociación y publicación parcial** de datos personales.
- Realizar el seguimiento de las **resoluciones de los órganos de supervisión y vigilancia** estatales y autonómicos existentes en materia de transparencia y protección de datos.
- Definir e impulsar iniciativas de **formación, sensibilización y cooperación** de los diferentes Departamentos Forales y entidades del Sector Público Foral para el **desarrollo y promoción de buenas prácticas** en materia de seguridad de la información y protección de datos personales, concienciación al personal del Sector Público Foral sobre el modelo de gobierno y gestión preventivo del riesgo con enfoque en el principio de Responsabilidad Proactiva y de Privacidad desde el diseño y por defecto desde las fases iniciales de la planificación de los procedimientos y servicios.

⁷ Decreto Foral 11/2020, de 4 de febrero, de la Diputación Foral de Bizkaia, por el que se aprueba el Reglamento que regula el Gabinete del Diputado General y el Gabinete de Estrategia Digital y Corporativa. Disponible en: https://www.bizkaia.eus/lehendakaritza/Bao_bob/2020/02/07/1-100_cas.pdf?hash=1cae9d8b317e311b4a6b926578538075

- **Asistir** en Derecho a los Responsables del Tratamiento sobre el correcto ejercicio de sus funciones en materia de protección de datos.
- **Centralizar las relaciones técnicas e intermediar con las Autoridades de Control** de protección de datos europeas, estatales y autonómicas, así como con los organismos de similares características que se creen en materias propias del Gabinete.
- **Coordinar, dinamizar y mantener la interlocución** con las personas dinamizadoras designadas por las distintas Direcciones Generales y Servicios de la Diputación Foral de Bizkaia en materia de protección de datos y seguridad de la información.
- Elaborar, publicar electrónicamente y gestionar el mantenimiento del **Registro de Actividades de Tratamiento (RAT)** de la Diputación Foral de Bizkaia y ayudar a las Entidades Forales para la creación de sus correspondientes RAT.

iv. Responsables del Tratamiento

El rol de Responsable del Tratamiento lo desempeñan, con carácter general, en el ámbito de la Diputación Foral de Bizkaia, las **Direcciones Generales** y, en el ámbito de las Entidades Forales, las **Direcciones Gerentes de cada Entidad**.

Las personas Responsables del Tratamiento, tal y como establece el RGPD, ostentan las siguientes **funciones**:

- Determinar los fines y medios del tratamiento.
- Cumplir las obligaciones del RGPD y LOPDGDD.
- Tomar las decisiones finales en materia de protección de datos.
- Responder en caso de incumplimiento.

v. Personas dinamizadoras en materia de protección de datos y seguridad de la información en Diputación de Foral de Bizkaia y las Entidades Forales

Las personas dinamizadoras en materia de protección de datos son personas nombradas **por cada Departamento y Gabinete Foral** para el **impulso, coordinación y colaboración** con las distintas Direcciones y Servicios de su Departamento o Gabinete, para la información, interlocución, dinamización y **coordinación con la Dirección de Buen Gobierno y Transparencia**, Dirección que, como se ha indicado, ostenta la competencia de implantación de medidas organizativas, de infraestructura, aplicaciones y servicios en materia de protección de datos. Asimismo, estas personas también realizan funciones de **información, interlocución, dinamización y coordinación** departamental en materia de seguridad de la información.

En cada uno de los Departamentos y Gabinetes Forales deberá haber, **como mínimo, una persona** que ostente el rol de persona dinamizadora en materia de Protección de datos y seguridad de la información.

Por su parte, las Entidades Forales también designan una persona dinamizadora que también ejercen las mismas funciones que las personas dinamizadoras, pero en el ámbito de las **Entidades Forales**. A destacar que estas personas dinamizadoras ejercen una importante labor dado que actúan como **personas de contacto y de referencia** entre sus Departamento, Gabinetes y Entidades Forales, con la Dirección de Buen Gobierno y Transparencia, la cual emite las diferentes instrucciones y recomendaciones en materia de protección de datos y seguridad de la información para todo el Sector Público Foral.

Finalmente, estas personas son, por tanto, las **principales interlocutoras** de la Dirección que lidera todo lo relativo al cumplimiento normativo en las materias indicadas, y su rol es fundamental para la actuación coordinada y homogénea.

vi. Administrador de Seguridad

El rol de Administrador de la Seguridad lo desempeña la Entidad Foral **Lantik, S.A.M.P.** Entre sus **funciones** destacan las siguientes:

- Implementación, gestión y mantenimiento de las medidas técnicas de seguridad.
- Gestión, configuración y actualización de hardware y software de seguridad TI.
- Monitorizar el estado de la seguridad y el cumplimiento de los controles TI.
- Informar a los responsables de seguridad y de sistema de cualquier anomalía.
- Colaborar en la investigación de incidentes de seguridad TI.
- Gestión de autorizaciones TI.

3.2.4. Fase IV. Implementación del Plan de Adecuación

Esta fase tiene como objeto la implementación de aquellas labores identificadas en el plan de acción como **fundamentales para lograr la adecuación** del Sector Público Foral a las nuevas obligaciones normativas impuestas por el RGPD y la LOPDGDD.

Como bien se ha analizado a lo largo de la presente Memoria, una de las principales novedades introducidas por la norma europea es el **cambio de enfoque** en el cumplimiento de la normativa de protección de datos. Este nuevo enfoque basado en la **responsabilidad proactiva**, conlleva la necesidad no solo de modificar algunas de las cuestiones formales que con el RGPD y la LOPDGDD han quedado obsoletas (como, por ejemplo, la inscripción de ficheros), sino también la modificación del modo en que la Diputación y las Entidades Forales abordaban el cumplimiento normativo. Así, mediante este Plan se **evolucionó** de un enfoque reactivo del cumplimiento normativo en protección de datos basado principalmente en el cumplimiento de obligaciones formales, a un enfoque **proactivo** basado principalmente en la adopción de procedimientos y normas que permitan tener en cuenta la protección de datos **desde las fases iniciales** de cualquier nuevo tratamiento de datos personales, y en ser capaz de **demostrar** que se está cumpliendo con las obligaciones normativas aplicables.

A continuación, se detallan las principales **labores** que conforman este Plan de Adecuación al RGPD y la LOPDGDD, así como las **acciones** llevadas a cabo por el Sector Público Foral del Territorio Histórico de Bizkaia para su implementación.

Las labores indicadas se engloban en siete grandes **ejes de actuación**:

Ejes de actuación para la implementación del Plan de Adecuación



Estos siete grandes **ejes de actuación** se dividen a su vez en **líneas de trabajo** formadas por las **acciones concretas** que se han desarrollado y que permiten implementar el Plan de Adecuación de forma satisfactoria.

A continuación, se analizan en detalle las líneas de trabajo y las principales acciones llevadas a cabo dentro de cada uno de los siete ejes de actuación.

i. Revisión de los tratamientos de datos realizados

El **objetivo** de las labores llevadas a cabo dentro de este primer eje de actuación es analizar que los tratamientos de datos identificados y documentados durante la fase inicial de análisis del estado de situación **cumplan con las diferentes obligaciones normativas** recogidas tanto en el RGPD como en la LOPDGDD.

Las principales **líneas de trabajo** llevadas a cabo dentro de este eje de actuación son las siguientes:



A continuación, se describen cada una de líneas de trabajo que forman este eje, así como las principales acciones implementadas dentro de cada una de ellas.

➤ **Revisión de las bases legitimadoras del tratamiento:**

El RGPD regula en su artículo 6.1 **seis bases de licitud** que no mantienen entre sí ninguna relación de prioridad, a diferencia de lo que sucedía con la anterior normativa en la cual se establecía que los tratamientos solo podían llevarse a cabo con el consentimiento de las personas interesadas, con una serie de excepciones entre las que se encontraba el que los datos fuesen tratados por las administraciones públicas para el ejercicio de sus funciones.

Asimismo, cabe mencionar que la nueva normativa no solo elimina la preferencia por el consentimiento como base de licitud, sino que también introduce un importante refuerzo de los requisitos para obtener el mismo estableciendo que este ha de ser **libre, específico, informado, inequívoco** y otorgado mediante una **clara acción afirmativa**⁸. Esto supone que los consentimientos **tácitos** permitidos por la LOPD **ya no son válidos**. Además, el hecho de que el consentimiento, entre otros requisitos, deba ser **libre** supone que, con carácter general, en aquellos supuestos en los que no haya una situación de equilibrio entre la persona Responsable del Tratamiento y la persona interesada, el consentimiento no se considerará libre y, por tanto, no será una base de licitud adecuada. Este requisito es directamente aplicable a la mayor parte de los tratamientos de datos realizados por las administraciones públicas en el ejercicio de sus funciones dado que, con carácter general, existe un desequilibrio entre la administración y la ciudadanía.

Este importante cambio trajo la necesidad de revisar la base legitimadora de los tratamientos de datos personales realizados por el Sector Público Foral para encajar los mismos dentro de las bases de licitud introducidas por el RGPD. Para ello, se comenzó identificando de forma precisa las **finalidades de los tratamientos** que se llevan a cabo. Una vez hecho esto, se comenzó a revisar las bases de licitud indicadas y su encaje dentro de la nueva normativa.

En el caso del **Sector Público Administrativo** formado por la Diputación Foral de Bizkaia y el Organismo Autónomo Foral IFAS, se partió de que, como regla general, los tratamientos de datos realizados por las administraciones públicas están legitimados de forma mayoritaria por el cumplimiento de una obligación legal, por cumplimiento de una misión realizada en interés público o por el ejercicio de poderes públicos. Es decir, por las **letras c y e del artículo 6 RGPD**. Asimismo, se revisaron aquellos tratamientos de datos legitimados por el consentimiento de las personas interesadas para verificar que los mismos seguían siendo una base de licitud válida y, en caso afirmativo, revisar que el mismo reuniese los requisitos establecidos por el RGPD para su validez.

Respecto a los tratamientos legitimados por las letras c y e del artículo 6 RGPD y en cumplimiento de lo establecido por el 8 LOPDGDD, se procedió a identificar aquellas **normas con rango de ley** que legitimasen cada tratamiento de datos realizado. Fruto de esta labor de investigación se concluyó que las normas con rango de ley que en su mayoría dan soporte y legitiman los tratamientos de datos personales son las siguientes:

- *Ley Orgánica 3/1979, de 18 de diciembre, de Estatuto de Autonomía para el País Vasco.*
- *Ley 27/1983, de 25 de noviembre, de Relaciones entre las Instituciones Comunes de la Comunidad Autónoma y los Órganos Forales de sus Territorios Históricos* y demás disposiciones de delegación o transferencia.
- *Ley 12/2002, de 23 de mayo, por la que se aprueba el Concierto Económico con la Comunidad Autónoma del País Vasco*, adaptado al Impuesto sobre el Valor Añadido y otras disposiciones de carácter tributario y demás normas que en este sentido se establezcan.

⁸ Art. 4.11. RGPD.

- Las disposiciones legales que establecen el marco competencial en el que actualmente se desenvuelven las Diputaciones de Régimen Común y en particular según lo dispuesto en la Disposición Adicional 2ª de la Ley 7/85, de 2 de abril, reguladora de las Bases de Régimen Local.
- Norma Foral 3/1987, de 13 de febrero, sobre Elección, Organización, Régimen y Funcionamiento de las Instituciones Forales del Territorio Histórico de Bizkaia.
- Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público

En el caso del **Sector Público Empresarial** formado por las Entidades Forales, se revisaron también las bases de licitud identificadas en cada tratamiento de datos. Se comprobó que en el caso de estas entidades eran muchos los tratamientos de datos legitimados por el **consentimiento**. Se procedió, por tanto, a verificar que el consentimiento seguía siendo la base de licitud más adecuada para el tratamiento de los datos, procediendo a modificar gran parte de las bases de licitud existentes al comprobar que estas Entidades Forales prestaban servicio o realizaban actividades reguladas por normativa de carácter público. En aquellos supuestos en los que se verificó que el consentimiento seguía siendo una base de licitud adecuada al no existir desequilibrio entre las partes, se procedió a verificar que los mismos cumplieren los **requisitos** exigidos por el RGPD y, en su caso, a modificar los medios a través de los cuales se recababan los mismos.

En relación con los tratamientos de **datos de categoría especial**, se procedió a realizar una verificación exhaustiva de las condiciones y requisitos del cumplimiento de cuantos supuestos dispone el artículo 9.2. del RGPD habilitadores de esta categoría.

➤ **Aplicación de los principios relativos al tratamiento:**

Otra importante línea de trabajo es la consistente en aplicar a todos los tratamientos de datos que realiza tanto Diputación como las Entidades Forales, los principios relativos al tratamiento.

Concretamente, las acciones ejecutadas en relación con dichos principios son principalmente las siguientes:

- Principio de licitud, lealtad y transparencia (art. 5.1.a RGPD).

El cumplimiento de este principio está estrechamente relacionado con la línea de trabajo expuesta anteriormente, ya que su cumplimiento conlleva, en primer lugar, verificar que el mismo se lleva a cabo bajo la premisa de alguna de las **bases de licitud** del artículo 6.1 y 9.2 RGPD. Asimismo, como se verá en detalle en el desarrollo del tercer eje de actuación, la aplicación de este principio ha supuesto también la revisión y/o implementación de las pertinentes **cláusulas que informen** a las personas titulares de los datos de forma clara y transparente del tratamiento de sus datos que se efectuará.

- Principio de limitación de la finalidad (art. 5.1.b RGPD).

La aplicación de este principio ha supuesto revisar todas y cada una de las actividades de tratamiento identificadas durante la fase de análisis del estado de situación para verificar que, para cada una de ellas, se recoge una **finalidad del tratamiento adecuada y específica**.

Asimismo, dado que la mayor parte de tratamientos de datos que lleva a cabo el Sector Público Foral están legitimados en el cumplimiento de obligaciones legales o en el ejercicio de poderes públicos, se ha verificado que, en cada caso, se traten los datos personales para las **finalidades recogidas en las normas con rango de ley**

legitimadoras de cada tratamiento, y que no se tratan los datos personales para finalidades distintas a aquellas para las que fueron recogidos.

Todas estas acciones se han realizado teniendo siempre presente que las finalidades deben ser **lo más precisas posibles**, de manera que permitan informar del tratamiento de datos que se va a realizar de forma transparente y comprensible. Así, se ha procurado que las personas titulares de los datos entiendan de forma sencilla el alcance de dichos tratamientos, y lo que la persona Responsable del Tratamiento realizará con sus datos personales, manteniendo así el **control y el poder de disposición** sobre los mismos. Consecuencia de ello es la **eliminación de las finalidades del tratamiento genéricas** que se ha llevado a cabo.

La aplicación de este principio ha supuesto también el análisis de la **compatibilidad** de determinadas finalidades del tratamiento que, si bien no son las que se informaron a las personas titulares de los datos en el momento de su recogida, el RGPD establece en su art. 6.4 que pueden llevarse a cabo si son compatibles con dicha finalidad inicial. Así, se ha analizado la compatibilidad de tratamientos de datos que de forma ulterior se han destinado para finalidades relacionadas con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos.

- Principio de minimización de datos (art. 5.1.c RGPD)

Dado el **gran volumen de datos personales** que el Sector Público Foral trata, la aplicación de este principio ha adquirido especial importancia durante la implementación del Plan de Adecuación.

Concretamente, se ha revisado que los datos personales que se tratan en el marco de cada actividad de tratamiento sean **adecuados, pertinentes y limitados** a lo necesario en relación con los fines para los que sean tratados. Una labor muy importante ha sido la de examinar las normas con rango de ley que, en la mayoría de supuestos legitiman el tratamiento, para identificar aquellos datos personales cuyo tratamiento podría estar amparado en dicha norma.

Asimismo, se han mantenido **reuniones** con las personas dinamizadoras en protección de datos identificadas dentro de Diputación y de las Entidades Forales, para verificar con ellas si se trataban para cada actividad de tratamiento únicamente los datos adecuados, pertinentes y limitados. Esto permitió comprobar que, en algunos casos, se recababan datos personales que ya no eran necesarios y se procedió a eliminar los mismos de las correspondientes solicitudes y procedimientos, lo que resultó en una agilización de los procedimientos administrativos asociados.

El mantenimiento de las citadas reuniones junto con las **acciones formativas y de concienciación** llevadas a cabo en el marco del presente Plan y que serán expuestas en posteriores epígrafes, permitió concienciar al personal foral de que no es posible recabar datos personales no pertinentes por si en el futuro fuesen útiles o necesarios.

- Principio de exactitud (art. 5.1.d RGPD).

La Diputación, en cumplimiento de este principio, ha considerado adecuado tomar una serie de medidas para garantizar que los datos personales que se tratan sean **exactos** y se encuentren **actualizados**.

Una de las principales medidas que permiten cumplir con el principio de exactitud, es la **formación y concienciación** del personal sobre la importancia de mantener los datos personales actualizados y acordes a la realidad, estableciendo la obligación de actualizar aquellos que se tiene constancia de que no son correctos.

Asimismo, también cabe mencionar la existencia de **aplicativos informativos** cuya seguridad es gestionada por la Entidad Foral Lantik, S.A.M.P, administrador de

seguridad del Sector Público Foral, que permiten actualizar y agilizar la revisión de los datos inexactos de forma segura.

Especialmente en el caso de la Diputación Foral de Bizkaia, es fundamental contar con datos personales actualizados y exactos para poder prestar debidamente el servicio público que le encomiendan las leyes.

- Principio de limitación del plazo de conservación (art. 5.1.e RGPD).

Este principio ha supuesto la revisión y, en su caso, la **definición de plazos y criterios** de conservación de los datos personales que se tratan.

Como regla general se ha establecido que, en el Sector Público Foral, los datos personales se conservan durante el **tiempo necesario para la tramitación del procedimiento** correspondiente a la actividad o servicio, y, además, se extiende durante el cumplimiento del plazo de **prescripción o caducidad** posterior para la extinción de las posibles responsabilidades ulteriores que pudieran acaecer derivadas del propio tratamiento. Asimismo, se han tenido en cuenta los **plazos específicos** que la LOPDGDD incorpora en su Título IV para los tratamientos de datos personales concretos que en el mismo se dispone, así como la **legislación aplicable** en cada caso para verificar si existe o no un plazo de conservación legalmente establecido.

En particular, destacamos los plazos de conservación específicos:

- **Archivo Administrativo General:** la Comisión de Valoración, Selección y Eliminación de Documentos, regulada en el capítulo VI del Decreto Foral de la Diputación Foral de Bizkaia 90/2011, de 24 de mayo (BOB núm. 103, de 31 de mayo) determina, conforme a sus funciones, el plazo de conservación y el criterio de expurgo de cada documentación con datos personales que se somete a su valoración.
- **Control médico-sanitario y prevención de riesgos laborales:** se establecen plazos de conservación en función de la especificidad de cada norma concreta del sector de prevención:
 - Documentación clínica: plazo mínimo de 5 años desde la fecha de alta de cada proceso asistencial, dando cumplimiento a la Ley 41/2002 de 14 noviembre, de autonomía del paciente y al Decreto 38/2012, de 13 de marzo, País Vasco, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica.
 - Agentes biológicos: plazo mínimo de 10 años desde que finalice la exposición, que podrá ser ampliado hasta 40 años, dando cumplimiento al Real Decreto 664/1997, sobre la protección de los trabajadores contra los riesgos relacionados con la exposición a agentes biológicos durante el trabajo.
 - Agentes cancerígenos: plazo de 40 años desde que finalice la exposición, dando cumplimiento al Real Decreto 665/1997, sobre la protección de los trabajadores contra los riesgos relacionados con la exposición a agentes cancerígenos durante el trabajo.
 - Exposición amianto: plazo mínimo 40 años desde que finalice la exposición, dando cumplimiento al Real Decreto 396/2006, por el que se establecen las disposiciones mínimas de seguridad y salud aplicables a los trabajos con riesgo de exposición al amianto.
 - Protección de radiaciones ionizantes: hasta que la persona trabajadora cumpla 65 años y siempre respetando un mínimo

30 años, dando cumplimiento al Real Decreto 783/2001, por el que se aprueba el Reglamento sobre protección sanitaria contra radiaciones ionizantes.

- Plomo metálico y componentes iónicos: plazo de 30 años, dando cumplimiento a la Orden Ministerial de 9 de abril de 1986, que aprueba el reglamento de prevención de riesgos y protección de la salud por la presencia de plomo metálico y sus componentes iónicos en el ambiente de trabajo. BOE de 6/5/1986.
- **Videovigilancia y control de accesos:** el tiempo de conservación de la imagen será de 1 mes, dando cumplimiento al artículo 22.3 de la LOPDGDD.
- Principio de integridad y confidencialidad (art. 5.1.f RGPD).

La aplicación de este principio está estrechamente relacionada con el cumplimiento de las medidas de seguridad establecidas en el anexo II del *Real Decreto 3/2010, de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad** en el ámbito de la Administración Electrónica* dado que el Sector Público está **obligado a observarlo**.

Asimismo, respecto al deber de secreto y confidencialidad del personal empleado cabe mencionar que tal y como se recoge tanto en la *Ley 6/1989, de 6 de julio, de la Función Pública Vasca*, como en el *Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público*, este está **sujeto a la obligación legal de confidencialidad y secreto profesional** pudiendo ser constitutivo de falta disciplinaria la utilización indebida de la documentación o información a que tengan o hayan tenido acceso por razón de su cargo o función y la falta del debido sigilo respecto a los asuntos que conozca por razón de su cargo.

Respecto a la aplicación de medidas organizativa de seguridad, cabe mencionar las **labores de formación y concienciación** que se han llevado a cabo y que serán objeto de análisis en el epígrafe correspondiente a la fase V del Plan de Adecuación.

- Principio de responsabilidad proactiva (art. 5.2 RGPD).

Como se ha expuesto a lo largo de la presente Memoria, este principio ha sido uno de los **principales inspiradores** del Plan de Adecuación llevado a cabo. Su aplicación ha promovido un cambio de enfoque en el modo de afrontar el cumplimiento normativo de la protección de datos. Así, Diputación ha establecido un modelo de cumplimiento que tiene en cuenta la protección de datos en todos y cada uno de los procesos que se llevan a cabo, siendo una pieza que ayuda a la mejora y **eficiencia** de los mismos, consolidándose como una **garantía del respeto a la confidencialidad** de los datos personales y, en definitiva, de la **privacidad** de las personas que tratan con el Sector Público Foral.

Como **ejemplos** de la aplicación de este principio de responsabilidad proactiva, destaca la **publicación del Registro de Actividades de Tratamiento** de la Diputación y de las Entidades Forales como se verá en los siguientes epígrafes; la modificación de los procedimientos para solicitar y conservar los **consentimientos** teniendo siempre como principal premisa la posibilidad de **demostrar** que ese consentimiento se ha obtenido y que, además, el mismo es lícito; la actualización de las cláusulas para el cumplimiento del **deber de informar**; la mejora en la **transparencia** y **claridad** de la información sobre protección de datos aportada a la ciudadanía mediante apartados webs muy didácticos y específicos sobre esta materia; la realización de **análisis de riesgos y evaluaciones de impacto** para poder establecer las adecuadas medidas de seguridad en función al riesgo detectado; la actualización de los procedimientos internos para

garantizar que, **por defecto**, siempre se tiene en cuenta la protección de datos ante cualquier nuevo servicio o procedimiento llevado a cabo, etc.

➤ **Identificación de las personas Responsables del Tratamiento**

Como se ha indicado en el epígrafe relativo al modelo gobernanza corporativa, el rol de persona Responsable del Tratamiento en el Sector Público Foral, lo desempeñan, con carácter general:

- a. En la Diputación Foral de Bizkaia: las **Direcciones Generales**;
- b. En las Entidades Forales: las **Direcciones Gerentes de cada Entidad**.

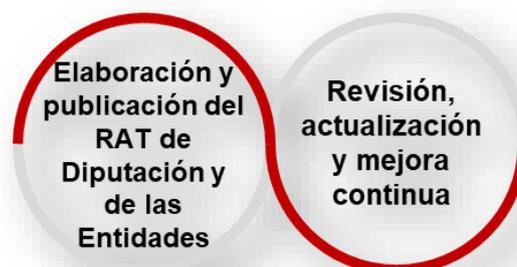
Dadas las **funciones y la responsabilidad** que en materia de protección de datos ostentan las personas Responsables del Tratamiento, se identificó como una **acción fundamental** dentro de este Plan de Adecuación la correcta identificación de las personas que debían ostentar el rol de Responsables del Tratamiento de cada una de las actividades del tratamiento identificadas. La identificación de la persona o personas Responsables del Tratamiento es fundamental ya que las mismas son las que deciden los **fines y medios del tratamiento**, y son a las que se **exigirán responsabilidades** en caso de que exista un cumplimiento no adecuado de la normativa.

La ejecución de esta línea de trabajo ha tenido especial relevancia y complejidad en el ámbito de la **Diputación** dado el gran número de Direcciones Generales que forman la misma. Así, para aquellas actividades de tratamiento en las que existían dudas acerca de qué Dirección General debía ostentar el rol de Responsable del Tratamiento, se procedió a analizar de forma detallada no solo los reglamentos de estructura orgánica que establecen competencias y funciones, sino también la información detallada que se había recopilado de cada actividad de tratamiento en su correspondiente ficha. Este análisis permitió determinar quién era la Dirección que decidía para qué se tratan los datos personales (fin del tratamiento) y mediante qué medios se llevaba a cabo dicho tratamiento (medios del tratamiento). Estos análisis pormenorizados permitieron identificar las adecuadas Direcciones Responsables del Tratamiento para cada caso, así como identificar actividades de tratamiento transversales cuya responsabilidad recae en más de una Dirección General.

ii. Elaboración y publicación de los Registros de Actividades de Tratamiento

Una vez identificados y revisados de forma exhaustiva los tratamientos de datos realizados por el Sector Público Foral, se procedió a elaborar y publicar los diferentes Registros de Actividades de Tratamiento (en adelante, RAT) que el artículo 30 del RGPD exige.

Las principales **dos líneas de trabajo** llevadas a cabo dentro de este eje de actuación son las siguientes:



A continuación, se describen cada una de líneas de trabajo y sus acciones:

➤ **Elaboración y publicación del RAT de Diputación y de las Entidades Forales**

Para la elaboración de los RAT se partió de los ficheros que en su día se declararon a las autoridades de control. Estos ficheros sirvieron como **base** sobre la que partir para la creación y, mediante reuniones mantenidas con las diferentes Direcciones responsables, con las personas interlocutoras identificadas para cada tratamiento y con la sección de Asesoramiento Jurídico, seguridad de la información y protección de datos, se procedió a **revisar** si los tratamientos identificados se seguían realizando y a **identificar y documentar nuevos tratamientos** que no estaban identificados.

Así se procedió a **identificar las actividades de tratamiento** que conforman los diferentes RAT y a recoger para cada una de ellas la información que exige el artículo 30 RGPD y 31 LOPDGDD. Además, se completó la información que componía cada actividad de tratamiento recabando los elementos que establece el art. 30 del RGPD.

Por su parte, en el ámbito de la **Diputación Foral de Bizkaia** se procede a exponer la información que se facilita a la ciudadanía en la página web Bizkaia.eus, con texto y un vídeo explicativo, respecto a las características del RAT de la institución foral. A continuación, procedemos a exponer las características que incluye:

1. ¿Qué es el Registro de Actividades de Tratamiento (RAT) de la Diputación Foral de Bizkaia y por qué es importante conocerlo?

Es un inventario en el que la Diputación recoge y detalla todas las Actividades de Tratamiento de datos personales que realiza. Es importante que todas las personas, como titulares de datos personales que son, conozcan este Registro que permitirá identificar de forma detallada y transparente toda la información relativa a los tratamientos de datos personales que lleva a cabo la Diputación, controlar qué hace en cada caso con los datos personales, y asegurar de que los mismos se tratan de manera adecuada.

2. ¿Dónde se puede consultar el RAT?

El RAT de la Diputación está publicado en el apartado de protección de datos dentro de la sección Bizkaia Abierta de la web bizkaia.eus.

Documentar y publicar este RAT es una obligación legal para la Diputación, regulada en el artículo 30 del Reglamento de la Unión Europea 2016/679 General de protección de datos y en el 31 de la Ley Orgánica 3/2018 de protección de datos Personales y garantía de los derechos digitales.

3. ¿Qué estructura tiene el RAT?

La normativa de protección de datos regula el contenido que ha de tener el Registro de Actividades de Tratamiento y que la Diputación publica en su web. Para dar una mayor claridad y transparencia a dicha información, la Diputación ha estructurado la publicación de su RAT en dos partes: una parte general y una parte específica.

La parte general está formada por aquella información que es común para todas las Actividades de Tratamiento que realiza la Diputación, y en la parte específica se muestra la información detallada e individualizada de cada una de dichas Actividades de Tratamiento.

3.1. Parte general

En primer lugar, se recoge información acerca de **las bases jurídicas que legitiman** el tratamiento de datos personales que realiza la Diputación. ¿Qué son estas bases jurídicas? Son las condiciones que legitiman los tratamientos de

datos personales que se realizan. No obstante, y con carácter general, de acuerdo con el art 6.1 letras e) y c) del RGPD las bases legitimadoras por las que la Diputación Foral de Bizkaia trata los datos personales son el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, y para el cumplimiento de una obligación legal. A modo indicativo se señalan las disposiciones normativas con rango de ley habilitadoras de la actividad competencial de la Diputación: Estatuto de Autonomía para el País Vasco, Ley de Territorios Históricos, Ley del Concierto Económico, Ley reguladora de las Bases del Régimen Local, Carta Europea de Autonomía Local, Ley de Procedimiento Administrativo Común de las Administraciones Públicas y Ley de Régimen Jurídico del Sector Público.

Por ejemplo, el tratamiento por parte de la Diputación del nombre y apellidos de las personas físicas para conceder o denegar una determinada subvención tendría como base jurídica habilitadora el ejercicio por parte de la Diputación de los poderes públicos que le confiere la Ley de Territorios Históricos y la Norma Foral de 5/2005 por la que se regula el régimen jurídico general de las subvenciones otorgadas por la Administración Foral. Para desarrollar las competencias que le atribuyen los citados textos normativos, la Diputación debe tratar los datos que sean estrictamente necesarios para tramitar una determinada subvención.

En segundo lugar, se indican **las medidas de seguridad** que la Diputación aplica a las Actividades de Tratamiento que realiza y que impiden que los datos sean conocidos por personas no autorizadas, que sean utilizados para finalidades no permitidas y, en definitiva, que impiden los usos no adecuados de los mismos. La Diputación está obligada a cumplir con las exigencias del Esquema Nacional de Seguridad en cuyo Anexo II se detallan las medidas de seguridad que se han de aplicar y que la Diputación aplica sobre los tratamientos de datos personales que realiza. Por ejemplo, esta normativa obliga a implementar controles de accesos a los aplicativos informáticos, formar y concienciar al personal en materia de seguridad, instalar cortafuegos, mecanismos de autenticación, trazabilidad, etc.

En tercer lugar, se informa del **tiempo durante el cual la Diputación conservará** los datos personales que trata. Como regla general, los datos personales se conservan durante el tiempo necesario para la tramitación del procedimiento correspondiente a la actividad o servicio y además se extiende durante el cumplimiento del plazo de prescripción o caducidad posterior para la extinción de las posibles responsabilidades que pudieran darse derivadas del propio tratamiento, siempre teniendo en cuenta los plazos específicos que la LOPDGDD incorpora en su Título IV para los tratamientos de datos personales concretos que en el mismo se disponen. Por ejemplo, la Diputación únicamente conserva las imágenes que capta mediante sus sistemas de videovigilancia durante un mes.

En cuarto lugar, se informa de que la **Diputación no realiza tratamientos automatizados de datos que permitan elaborar perfiles sobre los cuales se tomen decisiones con efectos jurídicos sobre las personas o les afecten significativamente**. En todos los tratamientos de datos personales que realiza la Diputación que implican la toma de decisiones con efectos jurídicos, participa personal de la institución foral. Por ejemplo, si se solicita una subvención será una persona empleada de la Diputación la que revisará la solicitud y los datos personales que se han consignado en la misma, y analizará si se cumple o no los requisitos legales para conceder dicha subvención. Nunca será un algoritmo

el que decida estas cuestiones y, en caso de que en un futuro sea así, se informará debidamente antes de que se aporten los datos.

En quinto lugar, se detalla cómo gestiona la Diputación las relaciones con **las personas encargadas del tratamiento** que son terceras personas físicas o jurídicas (empresas u organismos públicos) que prestan un determinado servicio para el cual precisan tratar datos personales de los que es responsable la Diputación (por ejemplo, Lantik, Entidad Foral, es una entidad encargada del tratamiento de la Diputación dado que presta a la misma un servicio de soporte informático y, para ello, debe tratar datos personales de los que es responsable la Diputación). En este apartado se informa además que la Diputación, en cumplimiento de las obligaciones legales, únicamente mantiene relaciones con personas encargadas del tratamiento que ofrezcan garantías suficientes del cumplimiento normativo en materia de protección de datos, que apliquen medidas técnicas y organizativas de seguridad adecuadas, y que cumplan con las instrucciones emanadas por la Diputación. Asimismo, las relaciones que la Diputación mantiene con las personas encargadas del tratamiento, los instrumentos jurídicos a través de los cuales regula su relación con ellas, así como el detalle de las personas que actualmente ostentan el rol de encargadas del tratamiento de la Diputación.

La **parte general** está formada por aquella información que es **común** para todas las actividades de tratamiento que realizan cada una de las Direcciones Generales Responsables del Tratamiento en Diputación.



REGISTRO DE **ACTIVIDADES DE TRATAMIENTO DE DATOS PERSONALES**

Introducción

La Diputación Foral de Bizkaia publica su Registro de Actividades de Tratamiento de datos personales (en adelante **RAT**). El **RAT** es el Inventario o Registro interno de la información completa referente al conjunto estructurado de datos personales que tiene lugar en las actividades de tratamiento de datos personales que se lleva a cabo en cada Departamento Foral de la propia Institución Foral con relación a las personas que contactan o que hacen uso de los diversos servicios, actividades y prestaciones forales.

La Diputación Foral de Bizkaia, dada su condición de Administración Pública, resulta Responsable de los tratamientos de datos personales que realiza y es por ello que se aprueba la creación y posterior actualización y revisión de su **RAT** Foral, en cumplimiento de lo dispuesto en el artículo 30 del Reglamento (UE) 2016/679, (RGPD), y artículos 31 y 77 de la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDD-GDD).

La creación y publicación de este Inventario de actividades de tratamiento de datos personales es accesible por medios electrónicos y se pone a disposición de la **AVPD**, en cuanto autoridad de control competente.

Acuerdo

Anuncio en el **BOE** del Acuerdo de Consejo de Gobierno de **DFF** de 18 de febrero de 2020, por el que se procede a la creación, regulación, mantenimiento y publicación del Registro de Actividades de Tratamiento de Datos Personales del acuerdo.

[DESCARGAR PDF \(123 KB\)](#)

Video Explicativo **RAT**



3.2. Parte específica

En la denominada parte específica del RAT de la Diputación, se muestra la información detallada e individualizada relativa a cada una de las Actividades de Tratamiento que realizan, en su mayor parte, las Direcciones Generales de los diferentes Gabinetes y Departamentos Forales que forman parte de la Diputación.

Las Actividades de Tratamiento se han ordenado por Gabinetes y Departamentos Forales, de manera que si clicamos sobre cualquiera de ellos nos aparecerá un listado de las Actividades de Tratamiento que cada uno de ellos realiza. Además del listado de todas las Actividades de Tratamiento, se muestra un primer resumen informativo y un enlace que permite acceder a una información concreta y detallada de la actividad de tratamiento y que permitirá conocer con exactitud todo lo relativo a una actividad de tratamiento concreta que realiza la Diputación sobre los datos personales. Se muestra a través de desplegados, de forma transparente y mediante un lenguaje claro, toda la información que la normativa vigente en materia de protección de datos exige que contenga el RAT.

En primer lugar, se informa de **la identidad y los datos de contacto de la persona o personas Responsables del Tratamiento de los datos**, que, con carácter general, son las direcciones generales.

En segundo lugar, se informa acerca de la **finalidad** para la cual la persona Responsable del Tratamiento precisa tratar los datos personales en cuestión. Es decir, para qué necesitan las Direcciones Generales tratar los datos personales y porqué se están recabando.

En tercer lugar, se informa acerca del **tipo de datos** que la Diputación trata para cumplir la finalidad, así como de las **categorías de personas titulares de los datos**. Las categorías de datos permiten informar del tipo de datos personales que la Diputación precisa tratar, englobándolos por categorías. Asimismo, las categorías de personas interesadas permiten conocer las personas titulares de los datos que tratan.

En cuarto lugar, se informa del **origen de los datos**, es decir, de dónde ha obtenido la Diputación los datos. Normalmente, los datos los aportará la propia persona titular de los mismos, pero hay ocasiones en las que la Diputación los obtiene de terceras personas. En este apartado se aporta también información acerca de los orígenes más frecuentes de los que la Diputación obtiene los datos.

En quinto lugar, se informa de si la Diputación **comunicará los datos a terceras personas o entidades ajenas a ella** y, en caso de que lo haga, se identifican las mismas. Se recoge también en este apartado, las comunicaciones de datos que con más frecuencia suele realizar la Diputación. En cualquier caso, es importante mencionar que la Diputación Foral de Bizkaia únicamente comunica los datos a terceras personas o entidades cuando tenga obligación legal de hacerlo o cuente con el consentimiento.

En sexto lugar, se indica las disposiciones legales de aplicación a la específica actividad de tratamiento y que hacen que el tratamiento de datos que se realiza sea conforme a la norma.

En séptimo lugar, se recogen **los derechos** que todas las personas físicas, por el mero hecho de serlo, ostentan sobre sus datos personales y que reconocen la normativa de protección de datos. Así, en este apartado se detalla en qué consisten cada uno de los derechos y cómo se pueden ejercitar ante la Diputación, así como su procedimiento. Estos derechos permiten conocer qué datos personales trata la Diputación, pedir que los suprima, oponerse a que los trate, solicitar que los modifique o corrija, que limite su tratamiento debido a determinadas circunstancias y pedir no ser objeto de decisiones individuales automatizadas.

En octavo lugar, se informa del **tiempo de conservación** específico en aquellas actividades de tratamiento que bien por disposición legal o por decisión de la unidad administrativa competente de su tramitación, dispongan de plazo de conservación concreto y determinado, por ejemplo: imágenes grabadas por cámaras de videovigilancia se suprimen en el plazo de 1 mes desde su captación de acuerdo con el art 22. 3 LOPDGDD.

Finalmente, se recoge información acerca del **nombramiento y la identidad de la persona Delegada de protección de datos del Sector Público Foral de Bizkaia** que comprende la Diputación Foral de Bizkaia y sus Entidades Forales, así como la forma de contactar con la persona que ostenta dicho rol. Esta persona es la encargada de informar, asesorar y supervisar el cumplimiento de la normativa de protección de datos dentro del Sector Público Foral, y también es el punto de contacto con las autoridades.

Registro de actividades de tratamiento

GABINETE DEL DIPUTADO GENERAL	▼
GABINETE DE ESTRATEGIA DIGITAL Y CORPORATIVA	▼
SOSTENIBILIDAD Y MEDIO NATURAL	▼
ACCIÓN SOCIAL	▼
EUSKERA, CULTURA Y DEPORTE	▼
HACIENDA Y FINANZAS	▼
TRANSPORTES Y MOVILIDAD SOSTENIBLE	▼
ADMINISTRACIÓN PÚBLICA Y RELACIONES INSTITUCIONALES	▼
PROMOCIÓN ECONÓMICA	▼
EMPLEO, INCLUSIÓN SOCIAL E IGUALDAD	▼
INFRAESTRUCTURAS Y DESARROLLO TERRITORIAL	▼

Ejemplo de la actividad de tratamiento “Gestión de los Contratos que formalicen los Órganos de Contratación de la Diputación Foral de Bizkaia”:

GESTIÓN DE LOS CONTRATOS QUE FORMALICEN LOS ÓRGANOS DE CONTRATACIÓN DE LA DIPUTACIÓN FORAL DE BIZKAIA

¿Quién es la persona responsable de este tratamiento?

Responsable del Tratamiento	Dirección General a la que esté adscrito el servicio promotor del contrato y Dirección General a la que esté adscrito el Servicio de Contratación, en función de los tratamientos de datos personales de los que sean responsables, respectivamente.
Departamento/Gabinete	Departamento/Gabinete competente al que estén adscritas la/s persona/s Responsable/s de Tratamiento
Datos de Contacto	Datos de contacto de la Dirección General a la que esté adscrito el servicio promotor del contrato y de la Dirección General a la que esté adscrito el Servicio de Contratación. Gran Vía, 25 - 48009 Bilbao

¿CUÁL ES LA FINALIDAD DE ESTE TRATAMIENTO?

¿QUÉ TIPO DE DATOS MANEJAMOS?

¿DE DÓNDE PROCEDEN LOS DATOS?

¿CEDEMOS TUS DATOS A TERCEROS?

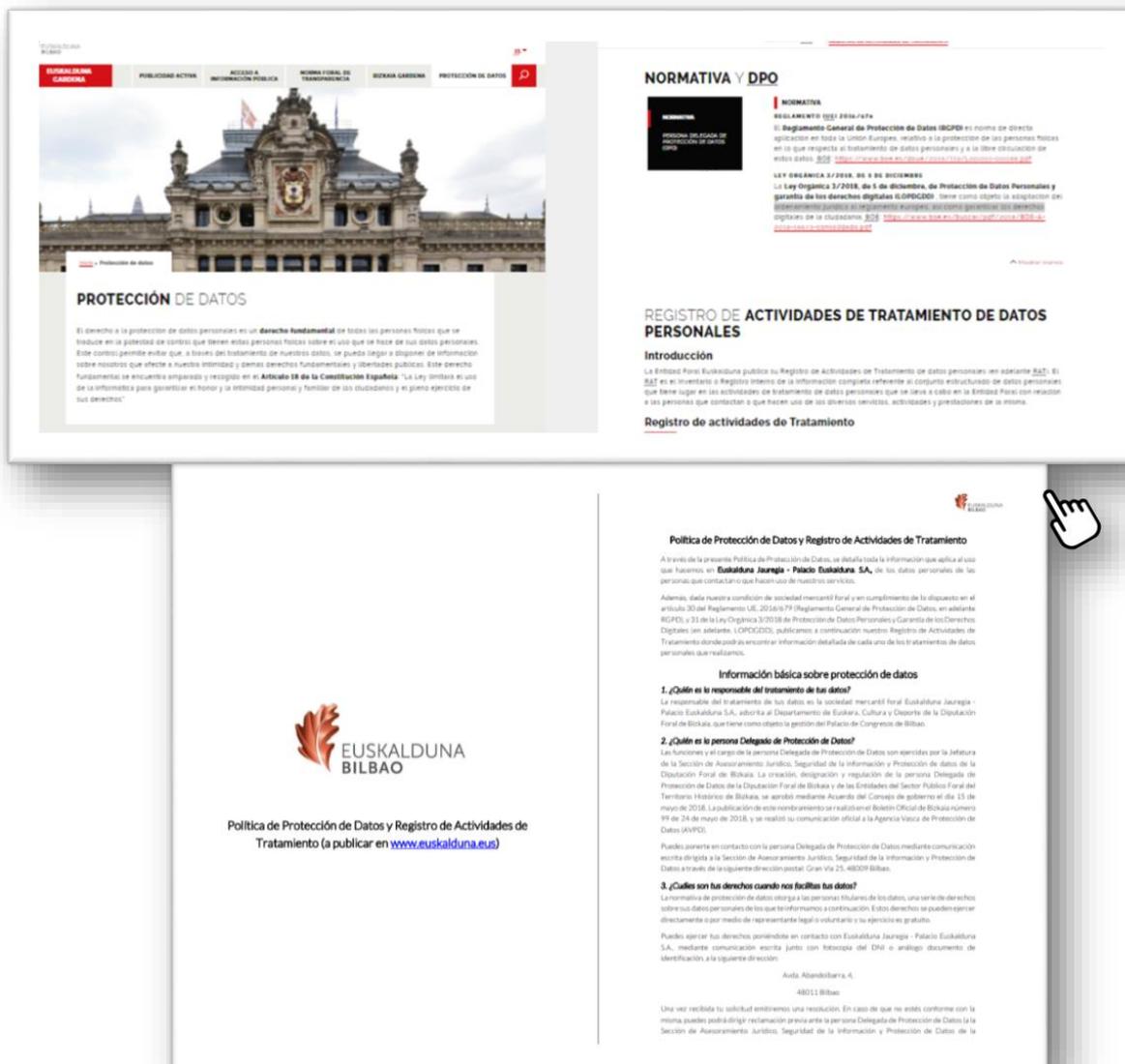
¿QUÉ NOS HABILITA PARA TRATAR TUS DATOS?

¿QUÉ DERECHOS PERSONALES PUEDES EJERCITAR EN ESTE?

¿QUIÉN ES LA PERSONA DELEGADA DE PROTECCIÓN DEL SECTOR PÚBLICO FORAL?

En el ámbito de las **Entidades Forales**, cada una de ellas ha creado un RAT en el que se identifican las actividades de tratamiento que cada una de ellas realiza, junto con la información que exigen los citados artículos. En cumplimiento de la obligación de transparencia que el artículo 31.2 LOPDGDD exige a las administraciones públicas, las Entidades Forales procedieron a **publicar** sus correspondientes RAT en sus páginas web. Dada la diferente realidad que cada Entidad Foral tiene en materia organizativa y con el principal objetivo de **armonizar el cumplimiento normativo** en materia de protección de datos, se procedió a publicar los RAT de las Entidades Forales en el apartado de **transparencia** de la Diputación Foral de Bizkaia. Además, estos RAT parten todos de un **formato común** que garantiza el cumplimiento de los criterios mínimos que la normativa exige para estos inventarios.

Se reproduce a continuación un **ejemplo** del RAT de la Entidad Foral “Palacio Euskalduna S.A.” publicado en el portal de Transparencia de Diputación Foral de Bizkaia:



RAT de Palacio Euskalduna, S.A.

➤ **Revisión, actualización y mejora continua**

En cumplimiento del principio de responsabilidad proactiva y dada la voluntad de **mejora continua** que tiene el Sector Público Foral, se trabaja de forma constante en la **actualización de los RAT elaborados**. Así, entre las funciones de las personas responsables departamentales y responsables en protección de datos está la **detección y documentación** de aquellos tratamientos de datos que realice su Departamento, Gabinete o Entidad Foral de forma novedosa, así como **actualizar** aquellos que ya estaban identificados pero que han sufrido algún tipo de cambio.

Esta información se debe **remitir de forma periódica** a la Sección de Asesoramiento Jurídico, seguridad de la información y protección de datos de la Diputación Foral de Bizkaia encargada de **revisar** que los nuevos tratamientos cumplan las disposiciones normativas y se hayan documentado de forma debida y, finalmente, de **actualizarlos** en los RAT publicados.

Respecto a los RAT de las Entidades Forales, en cumplimiento del principio de responsabilidad proactiva y la voluntad de **mejora continua** que tiene el Sector Público Foral, se trabaja de forma constante en la **actualización de los RAT**. Así, entre las funciones de las personas responsables de protección de datos identificadas por cada Entidad Foral está la **detección y documentación** de aquellos tratamientos de datos que realice su entidad de forma novedosa, así como **actualizar** aquellos que ya estaban identificados pero que han sufrido algún tipo de cambio. Esta información se debe **remitir de forma periódica** a la Sección de Asesoramiento Jurídico seguridad de la información y protección de datos de la Diputación Foral de Bizkaia encargada de **revisar** que los nuevos tratamientos cumplan las disposiciones normativas y se hayan documentado de forma debida y, finalmente, de **actualizarlos** en el RAT publicado.

A continuación, se expone el procedimiento para la identificación y documentación de nuevas actividades de tratamiento.

Este procedimiento se dirigirá y será **conocido e implementado**, principalmente, por todas las personas Responsables del Tratamiento, así como el resto de personas que forman parte del **modelo de gobernanza corporativa** en materia de protección de datos y seguridad de la información.



Como ya se ha expuesto a lo largo de la presente Memoria, este procedimiento exigirá que ante un nuevo tratamiento de datos o ante una modificación de un tratamiento ya identificado:

1. Se analice por la persona Responsable del Tratamiento la **licitud** del tratamiento de datos que se pretende realizar.
2. Se cumplimente la correspondiente **ficha de actividad de tratamiento**.
3. Se dé traslado a la Sección de Asesoramiento Jurídico, seguridad de la información y protección de datos de la ficha cumplimentada para que se **asesore** a la persona responsable acerca de la licitud de dicho tratamiento.
4. Se lleve a cabo un análisis básico de riesgos y se implementen las adecuadas **medidas de seguridad**.
5. Se lleve a cabo, en su caso, la pertinente **EIPD**.

6. Se registre el nuevo tratamiento de datos en el **RAT** y se de **publicidad** al mismo.

iii. Revisión del cumplimiento del deber de informar

Este eje de actuación ha consistido en la adecuación de las cláusulas informativas de protección de datos a las **nuevas exigencias** impuestas por el RGPD y la LOPDGDD. Así, durante el mismo se han ejecutado diferentes líneas de trabajo compuestas por acciones orientadas a elaborar modelos de cláusulas informativas que puedan ser empleadas por cada Responsable del Tratamiento del Sector Público Foral.

Las principales **líneas de trabajo** llevadas a cabo dentro de este eje de actuación son las siguientes:



Con el objetivo de, por un lado, abordar el cumplimiento normativo de protección de datos de manera **común y armonizada** para todo el Sector Público Foral y, por otro, **facilitar** a las personas Responsables del Tratamiento el **cumplimiento normativo**, la Sección de Asesoramiento Jurídico, seguridad de la información y protección de datos de la Diputación, trabajó con las personas responsables para el **diseño de modelos normalizados de cláusulas informativas** que permitiese cumplir con el deber de informar y que se adaptasen a la realidad foral.

Dada la **pluralidad de realidades** existentes y los diversos canales a través de los cuales se obtienen los datos personales de las personas interesadas, se ha trabajado en elaborar **varios modelos** de cláusulas informativas que se adaptan a cada una de las realidades existentes en el Sector Público Foral.

A continuación, se exponen las principales cláusulas informativas elaboradas en el Sector Público Foral en el marco del Plan de Adecuación y el uso que en cada caso se hace de las mismas:

- Cláusulas informativas por capas:

Estos modelos de cláusulas informativas se han elaborado en aplicación de las recomendaciones emanadas por las autoridades de control⁹ que, con objeto de poder aportar toda la información exigida por el RGPD de forma **concisa y clara**, recomiendan adoptar un modelo de información por capas.

Así, Diputación ha elaborado un modelo de cláusula informativa por capas distribuido de la siguiente forma:

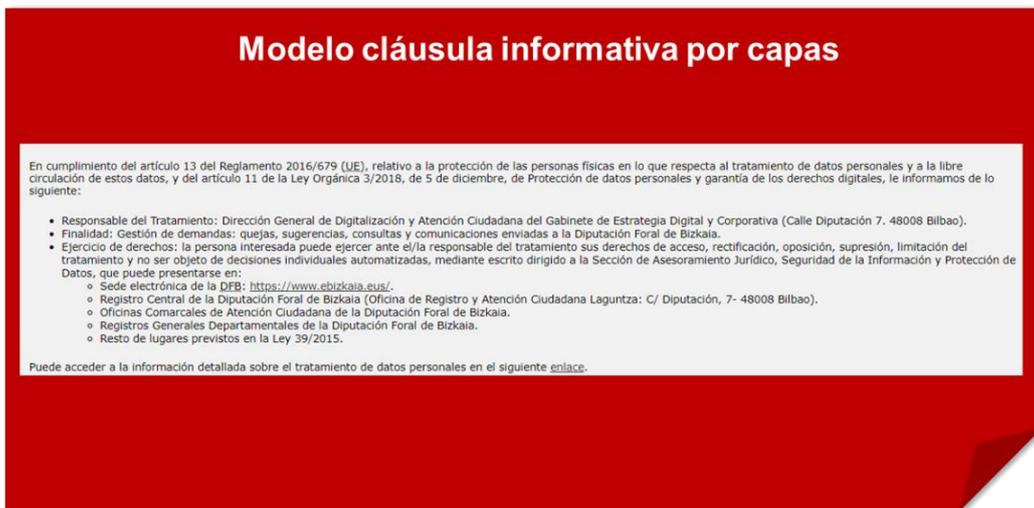
- **Primera capa:** se aporta **en el mismo momento** y en el mismo medio en que se recojan los datos. Tiene la información **básica** establecida por

⁹ AEPD, ApdCAT, AVPD, *Guía para el cumplimiento del deber de informar*.

el artículo 11 LOPDGDD. Esta información se recoge de forma **concisa y resumida** y remite a la segunda capa informativa.

- **Segunda capa:** recoge de forma **detallada** el resto de información que el artículo 13 y 14 RGPD exige que se ha de aportar a las personas interesadas. Esta segunda capa se ubica en la **web** de Diputación o, en su caso, de las Entidades Forales. Además, con carácter general, el **RAT** publicado actúa como segunda capa informativa dado que el contenido reflejado para cada una de las diferentes actividades de tratamiento coincide con el que el RGPD exige para las cláusulas informativas.

Este modelo de cláusula informativa es empleado principalmente en **medios electrónicos**.



Modelo cláusula informativa por capas

En cumplimiento del artículo 13 del Reglamento 2016/679 (UE), relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y del artículo 11 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de datos personales y garantía de los derechos digitales, le informamos de lo siguiente:

- Responsable del Tratamiento: Dirección General de Digitalización y Atención Ciudadana del Gabinete de Estrategia Digital y Corporativa (Calle Diputación 7, 48008 Bilbao).
- Finalidad: Gestión de demandas: quejas, sugerencias, consultas y comunicaciones enviadas a la Diputación Foral de Bizkaia.
- Ejercicio de derechos: la persona interesada puede ejercer ante el/la responsable del tratamiento sus derechos de acceso, rectificación, oposición, supresión, limitación del tratamiento y no ser objeto de decisiones individuales automatizadas, mediante escrito dirigido a la Sección de Asesoramiento Jurídico, Seguridad de la Información y Protección de Datos, que puede presentarse en:
 - Sede electrónica de la DFB: <https://www.ebizkaia.eus/>.
 - Registro Central de la Diputación Foral de Bizkaia (Oficina de Registro y Atención Ciudadana Laguntza: C/ Diputación, 7- 48008 Bilbao).
 - Oficinas Comarcales de Atención Ciudadana de la Diputación Foral de Bizkaia.
 - Registros Generales Departamentales de la Diputación Foral de Bizkaia.
 - Resto de lugares previstos en la Ley 39/2015.

Puede acceder a la información detallada sobre el tratamiento de datos personales en el siguiente [enlace](#).

- Cláusulas informativas en una única capa:

Estos modelos de cláusulas recogen toda la información exigida por los **artículos 13 y 14 RGPD**, en un único lugar. Por tanto, su uso es posible tanto para los tratamientos de datos cuyo origen es la propia persona interesada, como para aquellos supuestos en los que los datos personales provienen de terceras personas.

Su uso está previsto para aquellos tratamientos de datos personales cuyos titulares son **personas que no cuentan con los conocimientos adecuados** para acudir a la web de Diputación y acceder a la segunda capa informativa (por ejemplo, personas mayores, colectivos vulnerables, etc.). También se recomienda su uso como anexo en los pliegos administrativos, así como para aquellas Entidades Forales que no desean redirigir a la web para más información.

Con objeto de armonizar el cumplimiento del deber de informar, y facilitar su cumplimiento por las personas responsables, este modelo cuenta con ciertos apartados **previamente cumplimentados**, como los datos de contacto de la persona DPO o el procedimiento para el ejercicio de los derechos de las personas interesadas, por ser estos comunes al Sector Público Foral y para facilitar el cumplimiento. El resto de los apartados deben ser cumplimentados por las personas responsables en función del tratamiento de datos que se vaya a realizar. En todo caso, se recogen ayudas para la cumplimentación de cada apartado.

Asimismo, dadas las **dos realidades** existentes en el Sector Público Foral, se ha elaborado **dos modelos de cláusulas diferentes** para que sean empleadas por Diputación y por las Entidades Forales. La única diferencia entre ambos modelos es que los apartados pre-cumplimentados están **adaptados a la realidad de cada**

organización lo cual facilita la correcta cumplimentación de estas cláusulas y, en definitiva, el adecuado cumplimiento del deber de informar.

Modelo cláusula informativa en una capa

- Cláusulas informativas para el canal telefónico:

Como ya se ha comentado a lo largo de la presente Memoria, uno de los principales canales de atención del Sector Público Foral es el canal telefónico. La Diputación y las entidades atienden numerosas llamadas de la ciudadanía en las que, en ocasiones, se recaban datos personales. Por tanto, es de vital importancia establecer procedimientos que permitan cumplir de forma adecuada con el deber de información en aquellos supuestos en los que se recaban datos personales mediante este canal.

El cumplimiento del deber de informar en las locuciones telefónicas está en **continuo cambio y mejora** con el fin de garantizar que se aporta la debida información sin que ello vaya en detrimento de la calidad del servicio público prestado.

Como regla general y dadas las limitaciones del formato telefónico, las cláusulas informativas empleadas en este medio adoptan también un sistema de **doble capa informativa**:

- **Primera capa:** se aporta **en el mismo momento** de la llamada antes de que la persona aporte ningún dato o, en su caso, se comience la grabación de la llamada. Recoge la información **básica** establecida por el artículo 11 LOPDGDD. Esta información se aporta de forma **concisa y resumida** y remite a la segunda capa informativa.
- **Segunda capa:** recoge de forma **detallada** el resto de información que el artículo 13 y 14 RGPD exige que se ha de aportar a las personas interesadas. En función del teléfono de atención la segunda capa se ubica en la **web** de Diputación o, en su caso, de las Entidades Forales, o en una nueva locución.

Además de la elaboración de los diferentes modelos de cláusulas informativas indicados, durante este eje de actuación se ha trabajado también en **formar**, principalmente, a las personas responsables para que cuenten con los conocimientos básicos que les permitan cumplir de forma óptima con el deber de informar. Asimismo, se trabaja de forma **constante** en la **adecuación de las cláusulas informativas** a los

nuevos formatos expuestos de manera que la información se aporte siempre de forma **armonizada, clara, transparente y adecuada** a las exigencias normativas.

iv. Elaboración de guías y procedimientos para dar respuesta a las solicitudes de ejercicio de derechos en materia de protección de datos

La implementación de este eje de actuación está directamente relacionada con la voluntad de **transparencia** con la que la Diputación aborda el cumplimiento normativo en protección de datos. Por ello, dentro de este Plan de Adecuación se han implementado una serie de **líneas de trabajo** orientadas a garantizar que las personas titulares de los datos pueden **ejercer** de manera adecuada los derechos que ostentan sobre los mismos ante las personas Responsables del Tratamiento del Sector Público Foral, y que se dé la debida respuesta dentro del plazo legalmente establecido.

Las principales líneas de trabajo llevadas a cabo dentro de este eje de actuación son las siguientes:



En primer lugar, con objeto de que ante solicitudes de ejercicio de derechos las personas Responsables del Tratamiento sepan identificar las mismas y darlas la debida respuesta, se han elaborado una serie de guías y modelos documentales. Así, se crearon los siguientes modelos documentales:

- **Guía para el ejercicio de derechos en materia de protección de datos:**

Esta Guía está dirigida y debe ser conocida e implementada por las personas que forman parte del modelo de gobernanza corporativa en materia de protección de datos y seguridad de la información y, especialmente, por las personas que tratan a diario datos personales y que están en directo contacto con la ciudadanía.

En la Guía se recoge de forma detallada, entre otras cuestiones, las siguientes:

- Roles que han de participar ante un ejercicio de derechos y funciones de cada uno.
- Condiciones generales para el ejercicio de derechos.
- Procedimiento a seguir ante una solicitud de ejercicio de derechos.
- Contenido y explicación de cada uno de los derechos que ostentan las personas interesadas, con especial mención de cuando se debe, como regla general, estimar o desestimar una solicitud.

- **Anexo I - Modelos de respuesta a las solicitudes de ejercicio de derechos en materia de protección de datos:**

Este Anexo contiene **modelos de respuesta** que las personas Responsables puede utilizar en caso de que deban responder a una solicitud de derechos. Recoge modelos con varias opciones que la persona Responsable, en cada caso, deberá seleccionar para que la respuesta esté en todo caso **motivada** y cumpla los requisitos normativos. Estos modelos pretenden servir de ayuda para facilitar la elaboración de las respuestas

y procurar responder a las personas solicitantes **en el plazo de un mes** que establece la normativa.

Este procedimiento está dirigido y debe ser conocido e implementado por las personas que forman parte del modelo de gobernanza corporativa en materia de protección de datos y seguridad de la información y, especialmente, por las personas que tratan a diario datos personales y que están en directo contacto con la ciudadanía.



Dentro de este eje de actuación, destaca también el procedimiento interno que se ha rotulado para permitir que las personas ejerzan sus derechos. Así, tanto en las **cláusulas informativas** como en el apartado de protección de datos de la **web** de Diputación, se recogen los **diferentes canales** habilitados para poder ejercer los derechos, así como el procedimiento a seguir para hacerlo.

¿QUÉ DERECHOS PERSONALES PUEDES EJERCITAR EN DFB? ∨

PROCEDIMIENTO PARA EL EJERCICIO DE DERECHOS PERSONALES EN DFB ∧

- 1. Presentación:** Las solicitudes se presentan mediante escrito dirigido a la Sección de Asesoramiento Jurídico, Seguridad de la Información y Protección de Datos en los lugares que se indican:
 - Sede electrónica de la DFB: <https://www.ebizkaia.eus> (procedimiento: ejercicio derechos datos personales)
 - Registro Central de la Diputación Foral de Bizkaia (Oficina de Registro y Atención Ciudadana Laguntza: C/ Diputación, 7- 48008 Bilbao)
 - Oficinas Comarcales de Atención Ciudadana de la Diputación Foral de Bizkaia
 - Registros Generales Departamentales de la Diputación Foral de Bizkaia
 - Lugares previstos en la Ley 39/2015
- 2. Tramitación y Resolución:** La sección indicada tramita la solicitud ante el Responsable de tratamiento, en cada caso competente dentro de la Diputación Foral de Bizkaia y éste responde y notifica en el plazo de 1 mes desde la recepción. Este plazo es prorrogable otros 2 meses más, teniendo en cuenta la complejidad y número de solicitudes, los motivos de la prórroga serán debidamente informados.
- 3. Impugnación:** En caso de desestimación, expresa o presunta, de la solicitud del ejercicio de derechos en materia de protección de datos correspondiente, pueden recabar la tutela del derecho ante la AVPD mediante la presentación de reclamación ante la propia AVPD, o en su caso, de conformidad con el art 37 LOPDGDD dirigir reclamación previa ante la persona delegada en protección de datos de la Diputación Foral de Bizkaia (DPO) para su tramitación correspondiente dentro de la DFB, entidad contra la que dirige la reclamación.

Una vez recibida la solicitud por parte de la Dirección General Responsable del Tratamiento, esta deberá dar **respuesta** en el plazo de 1 mes tras la recepción de la misma. En la elaboración de la respuesta motivada se contará con el **sopORTE** de los documentos indicados anteriormente y con el **apoyo** de la Sección de Asesoramiento Jurídico, Seguridad de la Información y Protección de Datos.

v. Elaboración, revisión y suscripción del clausulado con personas encargadas del tratamiento

La implementación de este eje de actuación ha supuesto también una evolución en el modo en el que el Sector Público Foral abordaba su cumplimiento.

Las principales **líneas de trabajo** llevadas a cabo dentro de este eje de actuación son las siguientes:



En primer lugar, se han ejecutado las acciones necesarias para suscribir con las personas encargadas del tratamiento instrumentos jurídicos que las vinculen con las personas responsables y que los mismos contengan los requisitos establecidos por el **artículo 28 RGPD**. En el ámbito foral son **varios los instrumentos jurídicos** empelados para formalizar jurídicamente las relaciones con entidades del sector público o privado que, en materia de protección de datos, son encargadas del tratamiento de alguna de las Direcciones Generales responsables de Diputación o de alguna Entidad Foral. Por ello, la Sección de Asesoramiento Jurídico, seguridad de la información y protección de datos junto con las personas responsables, trabajaron en la elaboración de modelos de clausulado a suscribir con las personas encargadas del tratamiento, cuyas características son **diferentes** en función del **medio jurídico** empleado para formalizar las relaciones. Así, se han elaborado **modelos normalizados** para suscribir con aquellas personas encargadas del tratamiento que se relacionan con el Sector Público Foral mediante contratos administrativos, contratos menores, convenios, encargos a medios propios y encomiendas de gestión. Todos estos modelos normalizados se han distribuido a las personas responsables y se presta de forma continua el **soporte jurídico especializado** requerido para su correcta suscripción e implementación. Asimismo, estos modelos cuentan con apartados de **instrucciones** que facilitan su correcta cumplimentación y adaptación al caso concreto.

- No comunicar ni difundir los datos personales a terceras personas, ni siquiera para su conservación.
- Nombrar, en su caso una persona Delegada de protección de datos, cuando sea necesario según el RGPD, y comunicarlo a la persona responsable incluso cuando la designación sea voluntaria.
- Colaborar con la persona responsable en el cumplimiento de sus obligaciones en materia de medidas de seguridad, comunicación y/o notificación de brechas, a las autoridades competentes o las personas interesadas, y colaborar en la realización de evaluaciones de impacto.
- Comunicar a la persona responsables, de forma inmediata y a más tardar en el plazo de 72 horas, cualquier violación de la seguridad de los datos personales a su cargo de la que tenga conocimiento.

Otra de las particularidades existentes en el Sector Público Foral es la existencia de **medios propios**. Mediante *Acuerdo de Consejo de Gobierno de la Diputación Foral de Bizkaia de 22 de mayo de 2018* se establece que son medios propios de la Diputación Foral de Bizkaia las siguientes Entidades Forales:

- Interbiak, S.A.M.P.
- Azpiegiturak, S.A.U.M.P.
- Lantik, S.A.M.P.
- Zugaztel, S.A.M.P.
- Garbiker, S.A.M.P.
- Basalan, S.A.M.P.

A estas Entidades con la calificación jurídica de medio propio se les encarga por parte de la Diputación Foral de Bizkaia y/u otras Entidades Forales la realización de trabajos por razones de eficiencia. Para ello, se suscriben los correspondientes **encargos a medio propio** que también han de contar con las pertinentes **cláusulas de protección de datos** que regulen la relación jurídica existente entre la persona responsable y el medio propio Encargado del Tratamiento.

Finalmente, cabe mencionar que, con objeto de dar **transparencia** a las contrataciones que Diputación realiza, y siguiendo la voluntad que esta tiene de informar **de forma clara y sencilla** a las personas titulares de los datos del tratamiento de los mismos que la institución foral realiza, se ha incluido en el apartado de “Protección de datos” de la web de Diputación, un **apartado específico sobre las personas encargadas del tratamiento**. En este apartado, mediante un lenguaje sencillo y fácil de entender, se trata de dar respuesta a las siguientes cuestiones:

- “¿Cómo establecemos y regulamos la relación con las personas encargadas del tratamiento?”
- “¿Qué sujetos intervienen en los encargos de tratamiento en la Diputación Foral de Bizkaia?”
- “¿Cómo se formalizan los encargos de tratamiento entre responsable de tratamiento y encargado de tratamiento en la Diputación Foral de Bizkaia?”



vi. Realización de análisis de riesgos y evaluaciones de impacto. Revisión de medidas de seguridad

Este eje de actuación, derivado también del cambio de enfoque normativo, ha supuesto dejar atrás la concepción anterior de la aplicación de las medidas de seguridad identificadas en el Real Decreto que desarrollaba la LOPD, para pasar a un modelo de enfoque proactivo que permite **detectar riesgos antes de que estos se materialicen** y diseñar las **adecuadas salvaguardas y medidas de seguridad** que permitan mitigar y tratar los mismos.

Las principales **líneas de trabajo** llevadas a cabo dentro de este eje de actuación son las siguientes:



En primer lugar, la Sección de Asesoramiento Jurídico, seguridad de la información y protección de datos trabaja de forma coordinada con las diferentes personas responsables y con el personal de la Entidad Foral Lantik, S.A.M.P en su condición de administrador de seguridad del Sector Público Foral, para el diseño de un **procedimiento metodológico** adaptado a la realidad foral para la elaboración de evaluaciones de impacto en protección de datos (en adelante, EIPD) y análisis de riesgos. Con el diseño de esta metodología propia se pretende que todas las EIPD y análisis de riesgos que lleven a cabo las diferentes Direcciones Generales y Entidades Forales Responsables del Tratamiento, utilicen un **formato y lenguaje común** en las mismas. Entre otras, esta metodología recoge las siguientes cuestiones:

- **Intervinientes:** roles que han de intervenir en la elaboración de la EIPD, funciones y responsabilidades de cada una de ellas.

- Apartados que, como mínimo, debe incluir toda EIPD y cuestiones a analizar en cada uno de ellos:
 - Descripción y contextualización del tratamiento.
 - Evaluación de la necesidad y la proporcionalidad del tratamiento.
 - Identificación y análisis de factores de riesgo.
 - Evaluación del nivel de riesgo del tratamiento.
 - Conclusiones y plan de acción.
 - Supuestos en los que procede recabar la opinión de las personas interesadas o de sus representantes.
 - Supuestos en los que procede consulta previa a la autoridad de control.
- Metodología para evaluar el nivel de riesgo del tratamiento:
 - Catálogo de factores de riesgo que afectan a los tratamientos de datos realizados por el Sector Público Foral.
 - Orientaciones para calcular el nivel de impacto y probabilidad.
 - Orientaciones para calcular el nivel de riesgo intrínseco.
 - Listado de medidas y controles mínimos recomendados para gestionar los riesgos detectados.
 - Orientaciones para calcular el nivel de riesgo residual.
 - Establecimiento del nivel de riesgo aceptable.
 - Supuestos en los que procede una revisión del nivel de riesgo.



En segundo lugar, cabe mencionar que como se ha avanzado en el epígrafe relativo a la primera fase del Plan de Adecuación expuesto en la presente Memoria, las **fichas de actividades de tratamiento** que se han de cumplimentar de forma obligatoria para cada uno de los tratamientos de datos que realicen las personas responsables del Sector Público Foral, cuentan con un **apartado** en el que se ha de evaluar si es o no preciso realizar una EIPD. En dicho apartado constan los **criterios** que tanto el RGPD como las autoridades de control han establecido que han de ser tenidos en cuenta para decidir si es o no preciso realizar una EIPD. En caso de que el resultado sea positivo, la persona responsable será la encargada de realizar la correspondiente EIPD con el **asesoramiento** de la persona DPO y su equipo, y siguiendo la metodología desarrollada que se ha expuesto en anteriores líneas.

Como se ha indicado, una consecuencia directa de la realización de análisis de riesgos y EIPD es la implementación de **nuevas medidas de seguridad o el refuerzo** y actualización de las ya existentes. Por tanto, una de las líneas de trabajo desarrollada dentro de este eje de actuación es el diseño, revisión, análisis y actualización de las medidas de seguridad que se aplican a los tratamientos de datos efectuados conforme a los resultados de los análisis de riesgo o EIPD realizadas. Por ello, las personas Responsables del Tratamiento trabajan de forma constante con el apoyo de la Sección de Asesoramiento Jurídico, seguridad de la información y protección de datos de la

Diputación Foral de Bizkaia, liderada por la persona DPO, y la Entidad Foral Lantik, S.A.M.P en el diseño de medidas de seguridad tanto técnicas como organizativas que eviten la pérdida de información, la destrucción involuntaria de datos o el acceso de personas no autorizado, y que a su vez garanticen la confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad de los datos tratados. Asimismo, se analizan de forma constante las medidas de seguridad existentes en los sistemas de información para determinar si las mismas cumplen con lo dispuesto en el RGPD.

vii. Actualización y/o elaboración procedimientos de seguridad y protección de datos.

El objeto de las labores llevadas a cabo dentro de este eje de actuación es facilitar a las personas responsables el cumplimiento normativo, la adecuación a las nuevas exigencias del RGPD y la LOPDGDD y, en definitiva, implementar un **sistema armonizado de cumplimiento normativo en materia de protección de datos** en todo el Sector Público Foral del Territorio Histórico de Bizkaia.

Fundamentalmente, las líneas de trabajo descritas son lideradas por la **Dirección General de Buen Gobierno y Transparencia**, dado que estos procedimientos buscan no solo la actualización y adecuación de los tratamientos de datos que realiza el Sector Público Foral a las novedades y exigencias de la normativa en protección de datos, sino también **a los criterios y directrices emanadas por la persona DPO y su equipo**.

Entre los procedimientos en proceso de elaboración dentro de este eje de actuación, destacan por su importancia los siguientes:



Este procedimiento se dirigirá y será **conocido e implementado**, principalmente, por todas las personas Responsables del Tratamiento, así como el resto de personas que forman parte del **modelo de gobernanza corporativa** en materia de protección de datos y seguridad de la información. Recogerá la **definición, detección y actuación** ante violaciones de seguridad en protección de datos de manera que las personas responsables puedan detectarlas de forma rápida y seguir el protocolo necesario para comunicarlas a la autoridad de control, en su caso, dentro de las 72 horas legalmente establecidas. Además, recogerá los criterios de valoración que permiten **evaluar** de forma rápida la **gravedad** de la misma y determinar la obligatoriedad de comunicar la violación a las autoridades de control, personas titulares de los datos, etc.



Política que se dirigirá, principalmente, a todas las personas Responsables del Tratamiento, así como el resto de personas que forman parte del **modelo de gobernanza corporativa** en materia de protección de datos y seguridad de la información. Establecerá el conjunto de medidas técnicas y organizativas apropiadas para garantizar el cumplimiento de la normativa aplicable al tratamiento de los datos personales, incluyendo, así mismo, los principios básicos y requisitos mínimos que permitan una protección adecuada de la información que se gestiona en el ámbito del Sector Público Foral del Territorio Histórico de Bizkaia.

3.2.5. Fase V. Formación y concienciación

Uno de los principales pilares sobre el que se ha sustentado el presente Plan de Adecuación es la formación y concienciación del personal. El objetivo de esta Fase es que el personal del Sector Público Foral conozca la materia, tome conciencia de las responsabilidades y se les dote de herramientas a utilizar en su día a día para un **cumplimiento óptimo** de la normativa relativa a la protección de datos (y otras normativas de aplicación), evitando de esta manera acciones negligentes que puedan derivar en incumplimientos y/o sanciones.

En base a lo anterior, el Servicio de Formación de Diputación en colaboración con la Dirección General de Buen Gobierno y Transparencia, ha diseñado una serie de labores de concienciación y un importante plan formativo que está en constante evolución y mejora para adecuarse a las necesidades del personal foral. A continuación, se detallan las principales labores formativas y de concienciación llevadas a cabo y cuyo diseño se considera estratégico en el desarrollo del presente Plan de Adecuación:

i. Planes formativos en materia de protección de datos

El conocimiento, implicación y concienciación del personal que a diario trata datos personales, es fundamental para lograr un óptimo cumplimiento normativo. Dada la voluntad que tiene la Diputación de mantener el más elevado nivel de protección de la privacidad de los datos personales de la ciudadanía que son tratados a diario por el Sector Público Foral, la formación de su personal se identificó como uno de los pilares fundamentales y más necesarios de este Plan de Adecuación.

El objetivo general y común de las diferentes acciones formativas diseñadas y desplegadas, es que las personas que forman parte de la Diputación y de las Entidades Forales cuenten con **conocimientos básicos** en materia de protección de datos, garantizando así una adecuada implementación del RGPD y la LOPDGDD en dichas instituciones, así como concienciar al personal e instaurar una óptima cultura de respeto a la privacidad.

El Sector Público Foral está formado por **múltiples personas** empleadas que desempeñan roles, funciones y responsabilidades distintas. Con objeto de que las formaciones se aprovechen de la mejor manera posible, se han diseñado acciones formativas **a medida** para cada uno de estos roles, las cuales se centran en cada caso en la realidad del trabajo diario de cada rol y, principalmente, en los **tratamientos de datos personales** que estos realizan.

Todas las acciones formativas son impartidas por personal experto en la materia y con conocimientos de la organización interna del Sector Público foral, lo que garantiza la buena marcha de las mismas. Además, el sistema metodológico que siguen estas acciones formativas es un sistema dinámico **y práctico** que busca la **participación activa** y la implicación de las personas asistentes.

Asimismo, dado el contexto sanitario existente, se han diseñado acciones formativas en modalidades presenciales, pero también online haciendo uso de la plataforma formativa de *e-learning* de diputación.

A continuación, se detallan las acciones formativas que se han llevado a cabo dentro del Plan de Adecuación y que se **actualizan, retoman y mejoran de forma constante**:

Título de la sesión	Personas destinatarias	Objetivos	Contenido principal
<i>“Responsables en protección de datos de la Diputación Foral de Bizkaia: cuestiones básicas para desempeñar el rol con garantías”</i>	Personas dinamizadoras de Diputación, y Responsables de protección de datos de las Entidades Forales	Asegurar que las personas con responsabilidades en materia de protección de datos conozcan el nuevo marco regulador, con el fin de que puedan aplicar las en sus Departamentos y Entidades las directrices emanadas por la Dirección General de Buen Gobierno y Transparencia de la Diputación.	<ol style="list-style-type: none"> 1. Introducción. Protección de datos, ¿qué es y por qué es tan importante? 2. Marco normativo en protección de datos: conceptos fundamentales para Responsables 3. Protección de datos en la Diputación: cuestiones básicas a conocer por las personas Responsables en protección de datos 4. ¿Qué implica ser Responsable en protección de datos de la Diputación? 5. Buenas prácticas en protección de datos: qué debo hacer para cumplir con la normativa de manera sencilla y para procurar que el resto también cumpla 6. Casos prácticos
<i>“Protección de datos y privacidad en la Diputación Foral de Bizkaia: conceptos básicos, logros y desafíos”</i>	Directores/as y Subdirectores/as de la Diputación, Gerentes de las Entidades Forales	Dar a conocer las principales obligaciones en materia de protección de datos. Trasladar las labores llevadas a cabo dentro de la Diputación para adecuar la misma a la nueva normativa.	<ol style="list-style-type: none"> 1. Introducción. Protección de datos, ¿qué es y por qué es tan importante? 2. Marco normativo en protección de datos: conceptos básicos 3. Protección de datos en la Diputación y en las Entidades Forales 4. Buenas prácticas en protección de datos: pautas a seguir para mantener una adecuada cultura de privacidad 5. Supuestos prácticos relevantes en la materia
<i>“Protección de datos y seguridad de la información: fundamentos básicos”</i>	Jefes/as de Servicio de Diputación	Conocer las principales obligaciones en materia de protección de datos, trasladar las labores llevadas a cabo dentro de la Diputación para adecuar la misma a la nueva normativa e instaurar buenas prácticas.	<ol style="list-style-type: none"> 1. Introducción. Protección de datos, ¿qué es y por qué es tan importante? 2. Marco normativo en protección de datos: fundamentos básicos 3. Protección de datos en la Diputación Foral de Bizkaia 4. Buenas prácticas en protección de datos: pautas sencillas a seguir para mantener una adecuada cultura de privacidad 5. Supuestos prácticos
<i>“Protección de datos en el Sector Público Foral: fundamentos básicos”</i>	Personal de Entidades Forales, Jefaturas de Sección y Técnicos de Diputación	Conocer las principales obligaciones en materia de protección de datos, trasladar las labores llevadas a cabo dentro de la Diputación y de las Entidades Forales para adecuar las mismas a la nueva normativa y concienciar al personal.	<ol style="list-style-type: none"> 1. Módulo I. Introducción y objetivos de la sesión formativa 2. Módulo II. Marco normativo en protección de datos: conceptos básicos 3. Módulo III. Protección de datos en la Diputación y en las Entidades Forales 4. Módulo IV. Buenas prácticas en protección de datos: pautas a seguir para mantener una adecuada cultura de privacidad 5. Módulo V. Supuestos prácticos relevantes en la materia 6. Módulo VI. Conclusiones y cierre
<i>“Protección de datos en la Diputación Foral de Bizkaia: fundamentos básicos y buenas prácticas”</i>	Personal subalterno y personal administrativo de la Diputación	Conocer de forma muy práctica las principales obligaciones en protección de datos, trasladar las labores llevadas a cabo en Diputación para adecuar la misma a la nueva normativa y dar buenas prácticas para contribuir al cumplimiento normativo.	<ol style="list-style-type: none"> 1. Módulo I. Introducción y objetivos de la sesión formativa 2. Módulo II. Marco normativo en protección de datos: fundamentos básicos 3. Módulo III. Protección de datos en la Diputación Foral de Bizkaia 4. Módulo IV. Buenas prácticas en protección de datos: pautas sencillas a seguir para mantener una adecuada cultura de privacidad 5. Módulo V. Supuestos prácticos relevantes en la materia 6. Módulo VI. Conclusiones y cierre
<i>“Protección de datos en datos en la Diputación Foral de Bizkaia: conceptos fundamentales, instrumentos de cumplimiento y aplicación práctica”</i>	Personas funcionarias de carrera de la Diputación.	Conocimientos avanzados en materia de protección de datos.	<ol style="list-style-type: none"> 1. Módulo I. Introducción y objetivos de la sesión formativa. 2. Módulo II. Normativa y conceptos fundamentales. 3. Módulo III. Protección de datos en la Diputación 4. Módulo IV. Buenas prácticas. 5. Módulo V. Supuestos prácticos. 6. Módulo VI. Conclusiones y cierre.

Todas estas acciones formativas, y las que **se siguen desarrollando** de forma constante dentro del Sector Público Foral, buscan **integrar** la protección de datos dentro del día a día de todas las personas que trabajan dentro del Sector Público Foral. La Diputación cree firmemente en que solo mediante el **conocimiento y la concienciación** de su personal se puede lograr una **óptima cultura de cumplimiento normativo** en materia de protección de datos.

Como se ha expuesto en la anterior tabla, estos planes formativos abarcan y se hacen **a medida para todos los roles** que forman parte de la Diputación y de las Entidades Forales. Así, durante el presente año se han impartido sesiones formativas a un total de **830 personas**. Durante el año **2020** y gracias a la adopción del formato online, la cifra de personas formadas ascendió a **1.107**. Finalmente, durante el año **2019** y centrándonos en aquellas acciones formativas dirigidas a formar al personal en las nuevas obligaciones impuestas por el RGPD, se formaron a un total de **1.582 personas**. Todo ello hace notar la voluntad que tiene la Diputación en que todo su personal cuente con **conocimientos básicos en esta materia** y en el interés que la protección de datos suscita en el personal que a diario está en contacto con la ciudadanía.



ii. **Labores de concienciación en materia de protección de datos**

Para lograr un **óptimo cumplimiento de la normativa** en materia de protección de datos, es fundamental que el personal que trata los datos en su día a día laboral, no solo cuente con los conocimientos necesarios, sino que este concienciado en la materia. Únicamente mediante la concienciación del personal y la aportación de consejos y herramientas prácticas que pueden aplicar en su día a día, se conseguirá **crear y mantener una óptima cultura de cumplimiento normativo en materia de protección de datos**. Y es que, el cumplimiento de la normativa y la concienciación del personal, son dos **pilares básicos para garantizar la buena imagen de la organización** en relación al mantenimiento de la privacidad de la información de las personas que a diario tratan con el Sector Público Foral.

Por ello, las labores formativas detalladas en el anterior epígrafe se refuerzan con acciones de concienciación de realización **periódica**. Estas acciones pretenden recordar al personal sus obligaciones en materia de protección de datos, ayudándoles a evitar malas prácticas y **a elevar su grado de concienciación**.

Entre otras, las acciones de concienciación en materia de protección de datos diseñadas son las siguientes:

- **Píldoras formativas.**

Las píldoras formativas son pequeños aportes de información en formato de **vídeos cortos** relativos a la temática de la protección de datos. El planteamiento de las píldoras formativas es el siguiente:

- Se plantea la temática a desarrollar en los vídeos. Se determina la profundidad y duración de los mismos.
- Se elabora el soporte seleccionado y se genera el contenido en texto como apoyo.
- Se elaboran pequeños cuestionarios al finalizar cada píldora.

A continuación, se recogen algunos ejemplos de píldoras formativas diseñadas y difundidas entre el personal del Sector Público Foral:



Vídeo explicativo sobre el RAT publicado en la web de Diputación¹⁰:

Vídeo orientado a acercar el RAT a la ciudadanía y hacer que se comprenda fácilmente. Se recoge no solo la explicación del RAT, sino que también se hace un repaso del contenido del RAT de Diputación, explicando de forma detallada cada uno de los apartados mediante un lenguaje sencillo, claro y sin tecnicismos jurídicos para hacerlo comprensible para la ciudadanía.



Vídeo sobre ciberseguridad en el Sector Público Foral del Territorio Histórico de Bizkaia:

Vídeo dirigido a todo personal del Sector Público Foral y contiene **herramientas y pautas básicas** a implementar en su día a día para prevenir y detectar **problemas de seguridad**, evitar el **phishing** y, en definitiva, hacer un buen uso de los sistemas informáticos y evitar problemas de seguridad.

¹⁰ <https://web.bizkaia.eus/es/proteccion-de-datos>



Decálogo de buenas prácticas en materia de seguridad de la información.

Documento dirigido a todo el personal del Sector Público Foral. Se recogen mediante un lenguaje muy sencillo diez sencillas buenas prácticas que se recomienda aplicar al día a día laboral para respetar la privacidad de los datos personales que se tratan, mantener la seguridad de los mismos y de los equipos informáticos. Además de detallar en qué consiste cada buena práctica, se recogen recomendaciones para su implementación.



Carteles informativos con buenas prácticas en materia de protección de datos y seguridad de la información.

Carteles orientados a todo el personal. En ellos consta un decálogo con buenas prácticas que se recomienda que se apliquen en el trabajo diario y cuya aplicación permitirá lograr una cultura optima de cumplimiento normativo en materia de protección de datos y seguridad de la información en todo el Sector Público Foral. Estos carteles se colocan en zonas estratégicas, como:

- Cerca de los puestos de trabajo.
- En las zonas de descanso.
- Al lado de las impresoras y las destructoras de papel.
- Etc.





Mailings periódicos con recordatorios en materia de protección de datos y seguridad de la información.

Envío de correos electrónicos a todo el personal de forma periódica en los que se recuerda de forma concisa y orientada a la acción, ciertas acciones no recomendadas, buenas prácticas, así como otras cuestiones relacionada con la protección de datos y la seguridad informática y cuyo recordatorio se antoja necesario.



Plataforma formativa online.

Plataforma formativa que recoge conceptos básicos relativos al cumplimiento normativo de la protección de datos dentro de Diputación, así como buenas prácticas y herramientas útiles para que el personal las aplique en su trabajo diario. Sigue el sistema de auto-formación y contiene numerosas actividades que el personal ha de realizar para asimilar conceptos y superar la formación.

3.2.6. Fase VI. Control, revisión y mejora continua

La Fase final de este Plan de Adecuación, como no puede ser de otra manera, consiste en la continua y constante revisión de cada una de las acciones implementadas en las Fases que forman el mismo para su actualización y mejora continua.

Este enfoque metodológico seguido durante todo el Plan de Adecuación consiste en la revisión y mejora continua del mismo, lo cual permite lograr un alto grado de cumplimiento normativo. Como se ha detallado a lo largo de la presente Memoria, este enfoque se logra mediante la instauración de diferentes procedimientos que permitan **detectar posibles incumplimientos, corregirlos** de manera rápida y, en definitiva, llevar a cabo de manera constante **acciones que mejoren la seguridad de la información** en el Sector Público Foral.

Las líneas de trabajo concretas que se desarrollan dentro de esta fase son las siguientes:

- **Planificar:** partiendo del estado de situación, se detectan aquellas actuaciones que son susceptibles de mejora y se establecen los objetivos a alcanzar y las medidas a implementar.
- **Hacer:** ejecución e implantación de las actividades necesarias para las mejoras propuestas y las medidas detectadas de manera continua a medida que se desarrolle el proyecto.

- **Revisar:** se verifica que las medidas, procedimientos y demás actuaciones implementadas, son eficaces y permiten cumplir con los objetivos perseguidos. Se trata de revisar que el plan de trabajo instaurado es óptimo y que las labores llevadas a cabo permiten lograr un adecuado cumplimiento normativo.
- **Actuar:** implementar las medidas y procedimientos que se ha comprobado que son óptimos para lograr un adecuado cumplimiento normativo. Una vez implementadas todas las medidas previstas, se deberá volver de manera cíclica a la etapa primera para estudiar nuevas mejoras a implementar.

Para lograr los citados objetivos, controlar, revisar y mejorar de forma constante este Plan, es fundamental el rol que desempeñan las personas que forman parte del modelo de gobernanza corporativa. Especialmente importantes son las labores de asesoramiento y apoyo que lleva a cabo la Dirección General de Buen Gobierno y Transparencia, y la persona DPO.



4.EJEMPLOS DE PROACTIVIDAD Y BUENAS PRÁCTICAS

4. EJEMPLOS DE PROACTIVIDAD Y BUENAS PRÁCTICAS EN EL CUMPLIMIENTO DEL RGPD Y LA LOPDGDD EN EL SECTOR PÚBLICO FORAL DEL TERRITORIO HISTÓRICO DE BIZKAIA

Una vez expuestas las fases y características principales del Plan de Adecuación a la normativa de protección de datos en el Sector Público Foral del Territorio Histórico de Bizkaia, se recogen en el presente epígrafe una serie de **ejemplos prácticos** mediante los cuales se pretende mostrar cómo se han aplicado a la realidad de las organizaciones forales algunas de las acciones descritas en la presente Memoria

4.1. *Implementación del Plan de Adecuación en el Departamento de Acción Social y en el Departamento de Empleo, Inclusión Social e Igualdad de la Diputación Foral de Bizkaia: mecanismo para el cumplimiento del RGPD y la LOPDGDD en tratamientos de datos de categoría especial*

La implementación del Plan de Adecuación descrito en la presente Memoria, ha supuesto un especial reto en aquellos tratamientos de datos que, por su naturaleza o contexto entrañan un mayor riesgo para la privacidad de las personas titulares de los datos. Entre estos tratamientos de datos destacan la mayor parte de los realizados por las diferentes Direcciones Generales, Responsables del Tratamiento dentro del Departamento de Acción Social y del Departamento de Empleo, Inclusión Social Igualdad de la Diputación.

Estos Departamentos desarrollan funciones relacionadas con la protección de personas **menores de edad**, la atención a la problemática social específica de la **mujer y de la familia**, y la definición y ejecución de la política de prevención, detección, diagnóstico, tratamiento, orientación e integración de las personas en situación de **dependencia**. El correcto desempeño de estas funciones legalmente encomendadas, hacen que se deban tratar numerosos **datos de categoría especial** y, además, titularidad de **colectivos vulnerables**. Estos dos factores unidos al mandato legal recogido, entre otras, en la *Ley 12/2008, de 5 de diciembre, de Servicios Sociales*, que fomentan el desarrollo de modalidades alternativas e innovadoras de atención, hace que los tratamientos de datos realizados por este Departamento deban ser objeto de exhaustivos controles.

La implementación del Plan de Adecuación en estos Departamentos comenzó con el análisis de situación inicial donde se comprobó, como ya se ha mencionado, la gran cantidad de datos personales de categoría especial que las diferentes Direcciones trataban. Esto evidenció la necesidad de aplicar de forma exhaustiva, entre otros, el principio de **minimización de datos** y fomentar la **interoperabilidad** en aquellos supuestos en los que la misma es posible para **reducir la carga administrativa** de las personas usuarias y la circulación de estos datos fuera de redes seguras.

Asimismo, otra cuestión importante que se detectó es la existencia de numerosos **consentimientos** que legitimaban algunos de los tratamientos de datos personales realizados y que con el RGPD dejan de ser válidos. Así, se realizaron los correspondientes análisis para encuadrar dichos tratamientos dentro de alguna de las **bases legitimadoras** de los artículo 6.1 y 9.2 RGPD (fundamentalmente las letras c y e del artículo 6.1. y la b del artículo 9.2 RGPD).

Posteriormente, se procedió al nombramiento de una persona que asuma el rol de **Persona Dinamizadora en cada Departamento**. Personas que debían tener no solo mayores conocimientos en materia de protección de datos, sino que también debía conocer los tratamientos realizados por el propio Departamento. Esta persona es

fundamental para **detectar tratamientos nuevos** que no están identificados en el RAT, o aquellos que sus características o el uso de **nuevas tecnologías** hacen que deban ser objeto de análisis detallados.

Dadas las características que, como se ha expuesto, ostentan una gran parte de los tratamientos de datos personales realizados por las Direcciones Generales de estos Departamentos, son muchos los tratamientos que precisan ser objeto de una **EIPD**. Así, se han realizado múltiples evaluaciones de impacto sobre tratamientos de datos que:

- Implican el uso de **categorías especiales de datos** a las que se refiere el artículo 9.1 del RGPD.
- Las personas titulares son pertenecientes a **colectivos vulnerables** o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, personas con discapacidad, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que están bajo su guardia y custodia.
- Uso de datos a **gran escala**.
- Implican la utilización de **nuevas tecnologías** que suponen nuevas formas de recogida y utilización de datos.

Asimismo, al igual que en el resto del Sector Público Foral, se aplica de forma activa el **principio de protección de datos desde el diseño y por defecto** de manera que, ante un nuevo tratamiento de datos personales, un nuevo servicio o un nuevo desarrollo informático, se tiene en cuenta la protección de datos **desde el inicio del mismo** y el cumplimiento normativo se realice **por defecto**. Para ello:

- Se solicita el **asesoramiento de la persona DPO** desde las fases iniciales del proyecto;
- Se cumplimenta la **ficha de actividad de tratamiento** lo cual obliga a, entre otras cuestiones, analizar debidamente cual es la **base legitimadora** más adecuada y, en su caso, se identifica la norma con rango de ley habilitante;
- Se aplica el principio de **minimización de datos** verificando que no se solicitan datos no pertinentes. Asimismo, se habilitan mecanismo para permitir que las personas interesadas ejerzan su **derecho a no aportar documentos** que ya obran en poder de las Administraciones Públicas;
- Se elaboran las pertinentes **cláusulas informativas** teniendo en cuenta las características de las personas titulares de los datos y adaptando el lenguaje de las cláusulas a la realidad de las mismas.;
- Se realizan los pertinentes **análisis de riesgo** o, en su caso, **EIPD** y se aplican las **adecuadas medidas técnicas y organizativas** de seguridad en función del riesgo detectado.
- En su caso, se actualiza el **RAT**.

Finalmente, cabe indicar que los datos de categoría especial son **custodiados de forma segura** en los sistemas de Diputación. Así, además de las medidas de seguridad implementadas por defecto en todos los sistemas informáticos de Diputación y que son obligatorias para el cumplimiento del ENS, entre otras medidas, y dependiendo la tipología de tratamientos y de datos con carácter general, se procede a **seudonimizar** las bases de datos para evitar su uso no autorizado o comunicación indebida, se **cifran los archivos** que se comparten fuera de la red segura de Diputación, en ningún caso se recaban ni se aportan datos de categoría especial por teléfono o mediante cualquier medio que **no permita conocer la identidad** de la persona solicitante, los datos de categoría especial se encuentran guardados **en carpetas en red** a las que solo tienen acceso las personas con permisos específicos de la Dirección **autorizadas** para tal fin y que precisan acceder a ellos para el ejercicio de sus funciones, etc.

Respecto a los datos de categoría especial en **soporte papel**, estos se almacenan en **armarios cerrados con llave** que se encuentran en las oficinas de la Dirección correspondiente, que debe tratar los mismos en ejercicio de sus funciones profesionales. La llave la custodia la persona responsable de la Dirección y su acceso es controlada para evitar fugas de información o accesos no debidos. Además, la **política de mesas limpias** es de obligado cumplimiento en toda Diputación y la misma exige que no se dejen documentos ni cualquier soporte que contenga datos personales en la mesa o zona de trabajo, una vez terminada la jornada laboral o durante ausencias prolongadas del lugar de trabajo. Por tanto, una vez terminada la jornada laboral, o en caso de ausencia, vacancia o enfermedad, estos soportes se han de almacenar en los armarios habilitados al efecto.

En el caso de datos personales de expedientes ya cerrados y mientras no se procede al expurgo de los mismos, se procede a su almacenamiento en el archivo general de Diputación el cual cuenta con **adecuadas y especiales medidas de seguridad física** como sistemas de videovigilancia, personal de seguridad, registro de accesos, etc. que cuenta, además con una regulación específica sobre el derecho de acceso a los expedientes custodiados.

4.2. Protección de datos desde el diseño y por defecto en los sistemas de información

Otro ejemplo de proactividad y buenas prácticas en el cumplimiento de la normativa de protección de datos es el modo en el que se aplica el principio de protección de datos desde el diseño y por defecto en los **sistemas de información de Diputación**.

Como ya se ha mencionado, la seguridad informática dentro del Sector Público Foral es gestionada por la Entidad Foral **Lantik, S.A.M.P**, que es la encargada de aplicar en los sistemas las medidas de seguridad aplicables de las recogidas por el Anexo II del ENS y aquellas que las personas responsables del tratamiento consideran adecuadas en función del riesgo detectado. La aplicación del principio de protección de datos desde el diseño y por defecto es una de las **principales medidas** de refuerzo que se han aplicado en los sistemas informáticos como consecuencia de la aplicación del RGPD. Medidas que, en muchos casos, ya venían aplicándose pero que con la aplicación del RGPD y la LOPDGDD se han visto **reforzadas e incrementadas**.

Una de las principales medidas adoptadas es la obligación de cumplimentar **una ficha de actividad de tratamiento** cada vez que se realiza un nuevo desarrollo informático para un nuevo servicio gestionado por el Sector Público Foral. Así, la Sección de Asesoramiento Jurídico, seguridad de la información y protección de datos en colaboración con **Lantik, S.A.M.P**, solicita la correspondiente ficha a la persona responsable del tratamiento y el aplicativo tiene en cuenta las **particularidades del tratamiento** de datos identificado. Por ejemplo, **desde el diseño**, el aplicativo únicamente permitirá registrar los datos personales que se han indicado en la ficha y que son los **pertinentes, adecuados y necesarios** para la finalidad prevista. Además, en caso de que el desarrollo informático en cuestión conlleve el tratamiento de datos de **categoría especial**, se aplicarán **por defecto** medidas de seguridad determinadas, como el cifrado de los datos personales que se extraigan del aplicativo.

Asimismo, respecto a la realización de aquellas EIPD que en su caso sean necesarias de acuerdo con el art. 35 del RGPD, en su mayoría supuestos de tratamientos de datos realizados mediante tratamiento automatizados o desarrollos tecnológicos novedosos, Lantik, S.A.M.P. prestará el soporte técnico necesario para analizar, diseñar y desplegar las adecuadas medidas técnicas de seguridad en función del riesgo detectado.

Otra de las medidas aplicadas en cumplimiento del principio de protección de datos desde el diseño y por defecto, es la inclusión de un **apartado de protección de datos** en las fichas a cumplimentar para dar de alta un nuevo servicio de tramitación electrónica en la sede electrónica de Diputación¹¹. Este apartado debe ser cumplimentado **siempre** que se dé de alta un nuevo servicio de tramitación electrónica que implique un tratamiento de datos personales. Entre otras cuestiones, en este apartado se deberán cumplimentar las cuestiones relativas al tratamiento necesarias para elaborar las **cláusulas informativas** y que éstas aparezcan **por defecto** de forma automática en las tramitaciones electrónicas.

4.3. Rol de la Sección de Asesoramiento Jurídico seguridad de la información y protección de datos de la Diputación Foral de Bizkaia como impulsora, supervisora y asesora para la implementación del Plan de Adecuación

Uno de los ejemplos más claros de buenas prácticas en el cumplimiento de la normativa de protección de datos, es el rol que desempeña la Dirección General de Buen Gobierno y Transparencia mediante su Sección de Asesoramiento Jurídico, seguridad de la información y protección de datos. Esta Sección, como se ha indicado en el epígrafe dedicado a la exposición del modelo de gobernanza corporativa, está formada por **personal especializado** en materia de protección de datos y seguridad de la información y, además, la persona que ostenta el cargo de Jefe/a de dicha Sección desempeña también el rol de persona Delegada de protección de datos del Sector Público Foral del Territorio Histórico de Bizkaia.

Tal y como se ha descrito a lo largo de la presente Memoria, esta Sección **apoya** de forma directa a las personas responsables y al resto de personas que forman parte del modelo de gobernanza corporativa, no solo en el diseño del presente Plan, sino también en su implementación. Así, esta Sección actúa como **punto de referencia** dentro del Sector Público Foral en todo lo relativo a la protección de datos y la seguridad de la información, participando en reuniones en las que presta la **asistencia** necesaria a las personas Responsables del Tratamiento, o respondiendo a las consultas internas en materia protección de datos y seguridad de la información que reciben a través del **buzón electrónico específico** que gestiona la Sección. Esta función es especialmente importante para lograr el adecuado cumplimiento normativo en todo el Sector Público Foral, y para **armonizar** el mismo.

También el rol de la Sección es muy importante como asesora para la elaboración de los diferentes **modelos y soportes documentales** que permiten el cumplimiento normativo como los modelos de cláusulas informativas, el contenido y formato del RAT, los procedimientos de seguridad, las cláusulas a suscribir con las personas Encargadas del Tratamiento, la elaboración de **informes y dictámenes** que le sean solicitados, mantener al Sector Público actualizado en relación a los cambios y novedades relacionadas con las **disposiciones normativas** comunitarias, estatales y autonómicas, etc.

Cabe destacar también el importante rol que la Sección ocupa como **equipo de apoyo** a la persona DPO, lo cual garantiza que las **directrices** emanadas por esta persona son **difundidas** a todo el Sector Público y se presta el **soporte** necesario para su correcta implementación.

Por tanto, es claro que el hecho de contar con una unidad administrativa con funciones específicas en materia de protección de datos y seguridad de la información, y que actúa como **punto de referencia** en dichas materias, es clave para lograr un **grado elevado**

¹¹ <https://www.ebizkaia.eus/es/inicio>

de cumplimiento normativo y para poder **armonizar** el modo en el que se aborda el mismo dada la pluralidad de realidades existentes dentro del Sector Público Foral. Esta Sección participa además de forma activa en la **revisión y mejora continua de este Plan**, detectando aquellas oportunidades de mejora que trasladan las personas responsables y adaptándolas a la realidad foral.

4.4. Información sobre protección de datos en bizkaia.eus: transparencia, lenguaje claro y cercanía como principios inspiradores

Como ya se ha mencionado anteriormente, el compromiso de la Diputación Foral de Bizkaia con la transparencia del Sector Público Foral del Territorio Histórico de Bizkaia, va íntimamente relacionado con el principio recogido por la normativa de protección de datos por el que se establece la obligación de ofrecer a la ciudadanía información sobre el tratamiento de sus datos de una manera **fácilmente accesible, clara y sencilla de entender y comprender**. Es por este motivo que tanto en la web de la propia Diputación (bizkaia.eus), como las respectivas de cada Entidad Foral, tienen un apartado específico de protección de datos, donde se detalla la información pertinente de una manera **clara, cercana, entendible y precisa**.

Concretamente, respecto al apartado de protección de datos de la web de Diputación¹² este se ha diseñado con dos objetivos principales:

1. Aportar la información de forma **rigurosa** y cumplir así con las **exigencias formales** del RGPD en relación, principalmente, al deber de informar, derechos de las personas interesadas y publicación del RAT.
2. Trasladar a la ciudadanía de forma **transparente** la información **precisa, detallada y sencilla** acerca de lo que la Diputación hace con sus datos personales cuando tratan con ella.

Como se puede apreciar en la citada web, a través de un **lenguaje didáctico, sencillo y mediante un formato visualmente atractivo** se informa a la ciudadanía sobre las siguientes cuestiones:

- **Qué es la protección de datos.** En qué consiste este derecho fundamental y cuál es su regulación.
- Quién es la persona **Delegada de protección de datos** del Sector Público Foral del Territorio Histórico de Bizkaia y cómo se puede **contactar** con ella de forma sencilla.
- Los diferentes **derechos** que ostentan las personas titulares de los datos, en qué consiste cada uno de ellos, cuándo se pueden ejercer y el procedimiento a seguir para ejercerlos.
- **Registro de Actividades de Tratamiento** de la Diputación Foral de Bizkaia. Este RAT está dividido en dos partes:
 - **Parte general:** cuestiones comunes a todas las actividades de tratamiento. Concretamente, de forma muy sencilla y con información enlazada, se da respuesta a las siguientes **preguntas**:
 - “¿Cuál es la base que legitima los tratamientos de datos que realiza Diputación?”
 - “¿Qué medidas de seguridad aplica Diputación al tratamiento de los datos?”

¹² <https://web.bizkaia.eus/es/proteccion-de-datos>

- “¿Durante cuánto tiempo se almacenan los datos en la Administración Pública?”
- “¿Se elaboran perfiles en la Diputación Foral de Bizkaia?”
- “¿Cómo se relaciona la Diputación Foral de Bizkaia con las personas Encargadas de Tratamiento?”
- **Parte específica:** detalle de las actividades de tratamiento de las que es Responsable cada Dirección General organizadas por Departamentos y Gabinetes. Dentro de cada actividad de tratamiento, además, se detalla la siguiente información de forma muy clara en formato de **respuesta a preguntas:**
 - “¿Quién es la persona Responsable de este Tratamiento?”
 - “¿Cuál es la finalidad de este tratamiento?”
 - “¿Qué tipo de datos manejamos?” Se recoge detalle de las categorías de datos personales y de personas interesadas que utiliza Diputación.
 - “¿De dónde proceden los datos?” Se recoge detalle de las categorías de los orígenes de los datos personales que utiliza Diputación.
 - “¿Cedemos tus datos a terceros?” Se recoge detalle de las categorías de personas destinatarias de los datos personales que utiliza Diputación.
 - “¿Qué nos habilita para tratar tus datos?” Se recoge detalle de las normas con rango de ley que, en su caso, habilitan cada tratamiento.
 - “¿Qué derechos personales puedes ejercitar en Diputación?”
 - “¿Quién es la persona Delegada de Protección del Sector Público Foral?”

Con respecto al RAT y dado su carácter posiblemente más complejo de comprender, se ha reforzado además las explicaciones recogidas con un **vídeo explicativo** en el que de una manera muy visual y comprensible se explica qué es y qué tipo de información se podrá encontrar en el mismo, así como una explicación de cómo navegar por sus diferentes secciones y todo ello utilizando un vocabulario accesible y comprensible.

Este apartado web, por tanto, es fiel reflejo de la voluntad de **transparencia** que tiene Diputación en esta materia que tan importante es para la ciudadanía y que, en ocasiones, desconocen o les es muy difícil de entender. La Diputación continuará trabajando en **mejorar la información** que se aporta a las personas titulares de los datos para garantizar que, en todo caso, conocen y están informadas de forma transparente de qué hará Diputación con sus datos personales una vez que los comuniquen a la Institución Foral.



5. CONCLUSIONES Y VALORACIÓN DEL PLAN DE ADECUACIÓN EN LA ACTUALIDAD

La Diputación Foral de Bizkaia entiende el cumplimiento normativo de la protección de datos como una **cuestión capital** en todo su Sector Público Foral. Así, la institución foral entiende que garantizar el respeto a esta normativa no conlleva únicamente adecuarse a un mandato legal, sino también tomar las medidas necesarias para **garantizar la privacidad** de los datos personales de las personas que a diario tratan con Diputación y con las Entidades Forales. Y es que, dado el rol que, principalmente, la Diputación Foral de Bizkaia desempeña como Administración de referencia en Bizkaia, se considera fundamental **fortalecer el modelo de cumplimiento de la normativa de protección de datos como tractor para una gestión foral responsable y transparente**.

El diseño, implementación y mejora continua del Plan de Adecuación descrito en la presente memoria, se ha enmarcado dentro de la voluntad que tiene la Diputación Foral de Bizkaia de **construir y desplegar un modelo de gestión** de la protección de datos y la seguridad de la información corporativo, que garantice el **derecho fundamental** de la ciudadanía de Bizkaia a la protección de sus datos personales y la garantía de sus derechos digitales en todas sus relaciones con la Diputación Foral de Bizkaia.

En la actualidad, se ha podido constatar que el diseño que se ha dado a este Plan y la forma en la que se ha abordado el mismo han permitido que las labores que forman parte del Plan no sean meras formalidades, sino que se apliquen de forma **activa, continua y constante** en la totalidad de acciones desarrolladas por el Sector Público Foral. La **formación de todo el personal foral** a través de planes transversales de formación en materia de protección de datos, el **acompañamiento y soporte continuos** a los diferentes Departamentos, Gabinetes y Entidades Forales, e incluso la **implicación de los roles del más alto nivel jerárquico**, son claros ejemplos del **papel central y transversal** que la protección de datos ocupa actualmente en todas las actuaciones llevadas a cabo por la Diputación y sus Entidades Forales. Y es que, la protección de datos ha dejado de ser una obligación meramente formal, para ser uno de los **principales principios rectores** de las actuaciones que lleva a cabo el Sector Público Foral fruto de su **compromiso con la privacidad** de la ciudadanía vizcaína.

Dado que el cumplimiento de la protección de datos ha de ser una **constante** en la actuación foral, la Diputación trabaja en varias **líneas de acción** destinadas a **mejorar y robustecer** el modelo foral de gestión de la protección de datos. Entre las líneas de acción cuya implementación está prevista para lograr el citado fin, destacan las siguientes:

- Fortalecimiento del **nodo Diputación Foral de Bizkaia - Entidades Forales** en materia de políticas corporativas en protección de datos para una gestión **integrada y eficiente**. Así, se prevé dotar a las Entidades Forales de un espacio de conocimiento y colaboración para la compartición de información entre las mismas y la propia Diputación, que contribuya a una mayor cohesión del Sector Público Foral en un entorno de trabajo digital.
- Seguir estableciendo nuevas **políticas corporativas** en protección de datos que profundicen en la forma en la que la Diputación articula su **sistema de integridad y funcionamiento institucional** en ámbitos como el control y la gestión de riesgos.
- Diseño de nuevas **acciones formativas y de concienciación** a medida en función de las necesidades de cada Departamento, Gabinete o Entidad Foral. Especialmente, se trabajará en el **refuerzo** de las acciones formativas destinadas a personas responsables departamentales.
- Identificar de manera permanente y con la implicación de los diferentes Departamentos y Gabinetes de la Diputación y las Entidades Forales, **oportunidades y proyectos** encaminados a la mejora en el cumplimiento normativo de la protección de datos.

Por tanto, la Diputación continuará llevando a cabo las labores adecuadas para seguir **mejorando y evolucionando de forma continua** su modelo foral de gestión de la protección de datos, teniendo como objetivo principal el **respeto al derecho fundamental a la protección de datos** de la ciudadanía de Bizkaia.

Dirección General de Buen Gobierno y Transparencia

