Estudio Plasmac

PLATAFORMA EN LA NUBE PARA LA MEJORA DE LA ATENCIÓN SOCIOASISTENCIAL DE LA MACARONESIA

Abril 2019

CARSA

FCF FUNCATRA
FUNDACIÓN CANARIA PARA EL FOMENTO DEL TRABAJO

Interreg
Fondo Europeo de Desarrollo Regional

EUROPEAN UNION

PLASMAC

MAC 2014-2020
Cooperación Territorial

Tabla de contenido

Capítulo 0. Introducción **3**

PLASMAC 3

Capítulo 1. Servicios Sociales **4**

Terminología 4

Introducción 5

Marco legal de PLASMAC 6

Informe de requisitos y requerimientos técnicos de PLASMAC 9

Registro de usuarios y profesionales 12

Información de carácter público 15

Obligaciones de las personas usuarias 21

Información de carácter privado 21

La Historia Social Única y el Plan de Atención Personalizada. 22

Personas que pueden acceder a los Servicios Sociales 24

Unidades familiares y de convivencia 26

Inspección y sanción 27

Capítulo 2. Protección de datos. Requisitos técnicos para el cumplimiento del Reglamento General de Protección de Datos en el marco del proyecto PLASMAC **29**

Terminología 29

Introducción 30

Marco legal de PLASMAC 31

Informe de requisitos y requerimientos técnicos de PLASMAC 33

Principios de PLASMAC para el tratamiento de los datos 35

Cómo PLASMAC garantiza los derechos de las personas 36

Relación entre PLASMAC y los profesionales del servicio 38

Medidas de PLASMAC para una responsabilidad activa 39

PLASMAC y los menores de edad 43

Lista de verificación: 44

Capítulo 3. Ciberseguridad en PLASMAC **45**

Conceptos fundamentales 45

Principales amenazas y riesgos 47

Tecnologías y tendencias en Ciberseguridad a tener en cuenta en PLASMAC. La tecnología conformará el futuro de la plataforma....50
Ciberseguridad en PLASMAC....54
Recomendaciones de ciberseguridad para PLASMAC....57
Capítulo 4. Desarrollo de la plataforma PLASMAC....61
Metodologia aplicada al desarrollo del proyecto....61
Especificación del producto....63
Diseño de la solución....64
Implementación de la solución....66
Anexo I. Carta de derechos y obligaciones....69
Anexo II. Catálogo de servicios y prestaciones....77
Anexo III. Registro de entidades de iniciativa social....85
Anexo IV. Sanciones del sistema público de Servicios Sociales....92
Anexo V. Articulado RGPD correspondiente a PLASMAC....100
Anexo VI. Plantillas para obtener consentimiento....135

Capítulo 0. Introducción

El estudio se estructura en un capítulo introductorio al propio documento y al proyecto PLASMAC, más cuatro capítulos técnicos dedicados al análisis jurídico, normativo y técnico de la plataforma PLASMAC. Concretamente los capítulos en los que se divide el estudio son los siguientes:

Capítulo 0: Introducción al estudio y al proyecto PLASMAC.

Capítulo 1: Estudio de la situación de los Servicios Sociales en Canarias principalmente y su gestión dentro de PLASMAC.

Capítulo 2: Estudio de gestión y protección de datos en PLASMAC.

Capítulo 3: Estudio de la ciberseguridad necesaria para el buen funcionamiento de PLASMAC.

Capítulo 4: Estudio del proceso de desarrollo técnico de la plataforma PLASMAC.

PLASMAC

El proyecto PLASMAC. PLATAFORMA EN LA NUBE PARA LA MEJORA DE LA ATENCIÓN SOCIOASISTENCIAL DE LA MACARONESIA, está liderado por el Servicio Canario de Empleo (SCE) y participan como socios FUNCATRA, Ayuntamiento de San Cristóbal de La Laguna, Instituto Tecnológico y de Energías Renovables, la Universidad de La Laguna y la Universidad de Madeira. Es un proyecto cofinanciado por el Programa de Cooperación Territorial Interreg Madeira-Azores-Canarias (MAC) 2014-2020. Eje 5 – Mejorar la capacidad institucional y la eficiencia de la Administración Pública Conservar y proteger el medioambiente y promover la eficiencia de los recursos.

Está previsto que se desarrolle una solución piloto que se implemente en el Ayuntamiento de San Cristóbal de La Laguna.

Capítulo 1. Servicios Sociales

El primer capítulo de este estudio evalúa la situación de los Servicios Sociales en Canarias principalmente.

TERMINOLOGÍA

APL: Anteproyecto de Ley

Servicios sociales: El conjunto de recursos, medios o acciones organizados técnica y funcionalmente para realizar, de manera habitual, prestaciones sociales.

Necesidad personal básica: Las circunstancias en que se puedan encontrar personas sin hogar o sin soporte familiar, entendiendo como tales a las personas en situación de exclusión social o riesgo de estarlo, que carezcan de alojamiento estable, adecuado, habitable y adaptado, así como de redes de apoyo personal o familiar.

Necesidad social: las requeridas para mantener unas relaciones interpersonales y de grupo normalizadas, con integración y participación en la comunidad o, al menos, apoyo social sostenido en los casos de personas con patologías crónicas en el ámbito de la atención sociosanitaria.

Situación de exclusión social: Situación de pérdida de inclusión de las personas en el conjunto de la sociedad, que incluye no solo la falta de ingresos económicos y su alejamiento del mercado de trabajo, sino también un debilitamiento de los lazos sociales, un descenso de la participación social y una pérdida de derechos sociales.

Tercer sector de acción social: Las organizaciones privadas de carácter voluntario y sin ánimo de lucro, legalmente constituidas, que mediante la participación ciudadana desarrollan actividades en áreas de interés social, con criterios de solidaridad, autonomía y transparencia, a través de programas o proyectos encaminados a impulsar el reconocimiento y el ejercicio de los derechos sociales y lograr la cohesión y la inclusión social de todas las personas.

Personas en situación de riesgo de exclusión social: Aquellas que se encuentran en situación de vulnerabilidad o fragilidad social que puede derivar hacia situaciones de exclusión en caso de que se produzca alguna alteración en los mecanismos de integración ya debilitados, como ingresos, empleo, familia, educación o sanidad, entre otros.

Urgencia social: Aquella situación de necesidad de carácter excepcional o que surja de forma extraordinaria y puntual de las personas y que requiera de una actuación inmediata de los servicios sociales, sin la cual podría producirse un deterioro o agravamiento de la situación de necesidad acaecida.

Perspectiva o análisis de género: La consideración sistemática, en el conjunto de la actividad política, social e institucional de las diferentes situaciones y condiciones de vida, obstáculos o limitaciones, participación, recursos, derechos, prioridades o necesidades, valores y comportamientos de mujeres y hombres, determinados por los roles tradicionales de género, que provocan desigualdades sociales o discriminaciones reales y efectivas entre ambos sexos.

Principio de igualdad de trato entre mujeres y hombres: Supone la ausencia de toda discriminación, directa o indirecta, por razón de sexo en los sectores público o privado y, especialmente, las derivadas de la maternidad, la asunción de las obligaciones familiares, el estado civil y cualquier otra vinculada a la condición de género.

Identidad de género: Implica la vivencia interna e individual del género tal como cada persona la siente, pudiendo corresponder o no con el sexo asignado al nacer, y comporta el derecho de las personas que adoptan socialmente el sexo contrario al de su nacimiento a recibir de las administraciones públicas canarias una atención integral y adecuada a sus necesidades médicas, psicológicas, jurídicas y de otra índole, en igualdad de condiciones que el resto de la ciudadanía.

Derecho a la autotutela: La posibilidad que tiene una persona capaz de obrar de adoptar las disposiciones que estime convenientes en previsión de su propia futura incapacitación en los casos de pérdida de su autogobierno en los términos señalados en el Código Civil.

Familias y demás unidades de convivencia: Núcleo familiar constituido por los progenitores y, en su caso, las demás personas que convivan con ellos en una misma vivienda o espacio habitacional, ya sea por unión matrimonial por cualquier otra forma de relación estable análoga a la conyugal, por parentesco civil de consanguinidad o afinidad, hasta el segundo grado en línea recta y colateral, o por adopción, tutela o acogimiento familiar, que se hallaren empadronados y con residencia en Canarias.

Organizaciones de ayuda mutua: A los efectos de la presente ley, se entenderá por organizaciones de ayuda mutua aquellas entidades de carácter no lucrativo cuyos asociados sean, principalmente, las personas que afrontan directamente una necesidad o dificultad o sus familiares.

Producto de apoyo y ayuda técnica: Se entenderá por producto de apoyo y ayuda técnica, todo producto, instrumento, equipamiento o sistema técnico, fabricado especialmente o existente en el mercado, destinado a prevenir, compensar, aliviar o eliminar limitaciones para la promoción de la autonomía personal.

INTRODUCCIÓN

Los servicios sociales son uno de los sistemas públicos del estado del bienestar y constituye aquellas intervenciones que tienen como objetivo garantizar las necesidades básicas de los/as canarios/as, poniendo atención en el mantenimiento de su autonomía personal y promoviendo el desarrollo de las capacidades personales, en un marco de respeto por la dignidad de las personas.

No obstante, el crecimiento demográfico acelerado de los últimos años sufrido en Canarias, el envejecimiento de la población, la diversidad de las familias y los núcleos de convivencia, las nuevas bolsas de pobreza, el riesgo de desigualdades personales, colectivas o territoriales, las situaciones de dependencia que viven muchas personas y la complejidad que comporta para las familias, y los cambios en el mercado laboral son algunos ejemplos de necesidades sociales que un sistema público de servicios sociales debe atender. Por todo ello, se hace necesario ofrecer un sistema que permita gestionar

el ejercicio efectivo de los servicios sociales de acuerdo con las necesidades de la región y en el nuevo marco normativo.

Por último, teniendo en cuenta el aumento de la exigencia de la ciudadanía sobre los servicios públicos que se ha traducido en una mayor presencia de modelos de gestión basados en la calidad, las nuevas tecnologías adquieren un papel relevante, ya que permiten una mayor eficacia de las prestaciones sociales, lo que ha impactado de manera muy significativa en el actual sistema de servicios sociales.

En este sentido, PLASMAC constituye una plataforma en la nube que permite a las administraciones regionales mejorar los procesos de valoración, atención y prestación de servicios a los ciudadanos. En el presente informe se introduce la definición de los servicios sociales, la situación en Canarias y las novedades previstas en la nueva ley de Servicios Sociales de Canarias. Todo ello, pone en contexto las necesidades que la plataforma de gestión de los servicios sociales como PLASMAC, deberá reunir para que se adapte lo más fielmente a la normativa recientemente vigente y cumpla con las expectativas para una gestión integral, eficiente y lógica de los Servicios Sociales a nivel de los Ayuntamientos canarios, y en el futuro, a nivel insular y regional.

Con este objetivo, en el presente informe se analiza cómo PLASMAC deberá estructurarse desde sus cimientos para hacer efectiva la gestión de los servicios y prestaciones que constituyen el Sistema Público de Servicios Sociales, asegurando su escalabilidad en el resto de instituciones públicas canarias en el futuro, siendo fiel reflejo en este nuevo marco normativo.

MARCO LEGAL DE PLASMAC

Numerosas normativas avalan y protegen el derecho de todas las personas a un nivel de vida que le asegure a ella y a su familia, la salud y el bienestar, y en especial la alimentación, el vestido, la vivienda, la asistencia médica y los servicios sociales necesarios. Ejemplos de estas normativas son:

- La Declaración Universal de los Derechos Humanos de las Naciones Unidas de 1948 (en el art. 25),
- La Carta Social Europea (en el art. 14),
- La Convención Internacional de los Derechos de las Personas con Discapacidad de las Naciones Unidas,
- La Estrategia Europa 2020 (siendo una de sus prioridades, la contribución al empleo, la productividad y la cohesión social),
- La Constitución Española (en los art. 9.2, 148.1.20 y 149.1.17), etc.

En este marco competencial, la Comunidad Autónoma de Canarias aprobó la Ley 9/1987, de 28 de abril, de Servicios Sociales, una norma de largo recorrido, pero que, sin menoscabo del valioso papel desempeñado hasta la fecha a través de esta ley, los profundos cambios operados en la realidad social de la población canaria y los cambios económicos producidos, incluida la actual situación de recesión de la crisis y los elevados

indicadores de desempleo, justifican la necesidad de revisar y analizar en profundidad la regulación contenida en el proyecto de ley, elaborada por la Consejería de Empleo, Políticas Sociales y Vivienda.

Con la nueva ley se pretende incluir una serie de mejoras que la ley de 1987 no contemplaba, para cubrir las nuevas necesidades de la sociedad implicando no solo a los/as residentes canarios/as, sino también a la población nacional y extranjera visitante o transeúnte.

Las principales novedades que aporta la nueva normativa, que consta de 108 artículos (agrupados en un título preliminar y siete títulos, además de catorce disposiciones adicionales, cuatro transitorias, una derogatoria y seis finales), con respecto a la ley 9/1987 de Servicios Sociales de Canarias (con tan solo 26 artículos, agrupados en 5 títulos más el preliminar, y tres disposiciones transitorias y cinco finales) **se describirán a continuación agrupándolos por títulos y capítulos.** Es necesario aclarar, que la nomenclatura y disposición de los títulos, capítulos y artículos, están sujetos a posibles modificaciones hasta que no salga publicado oficialmente en el BOC.

A través de los tres capítulos que configuran el Título II, se define la estructura del Sistema público en cuanto a las prestaciones de servicio y económicas, y el acceso a dichas prestaciones. Detallándose los que tienen la consideración de servicios esenciales y las prestaciones económicas garantizadas, así como la **cartera de servicios** y el **catálogo de prestaciones**. En general, las premisas son:

- El establecimiento de otras prestaciones de servicio del Sistema público de servicios sociales de Canarias.
- El acceso a las prestaciones de servicio y económicas
- La organización de los servicios de atención a las personas
- La determinación de los servicios de atención primaria
- La Cartera de Servicios y Prestaciones económicas
- El catálogo de prestaciones del Sistema Público de Servicios Sociales

El Título III se dedica a la distribución de competencias entre tres niveles: (1) Consejo de Gobierno de la Comunidad Autónoma de Canarias, (2) Cabildos Insulares, y por otro lado (3) las que corresponden a los ayuntamientos de cada municipio. También se describe la necesaria participación de tres órganos nuevos colegiados:

- la Conferencia Sectorial de Servicios Sociales,
- el Consejo General de Servicios Sociales y
- el Observatorio Canario de los Servicios Sociales.

De este título podemos destacar la importancia de:

- El papel de colaboración de los Cabildos Insulares con el Gobierno de Canarias.

- El acceso efectivo a los servicios residenciales y de día del Sistema para la Autonomía personal y Atención a la Dependencia y la asignación de prestaciones de servicios especializados que correspondan a los usuarios.
- La aportación y actualización de los datos que deba integrar el Sistema de Información de Servicios Sociales relativos a las la Historia social de los usuarios del Sistema público, prestaciones y servicios en su ámbito de actuación territorial y competencial.
- La colaboración de los municipios con la Comunidad Autónoma de Canarias y el correspondiente cabildo insular en la coordinación, el control y la inspección de las actividades en materia de servicios sociales.
- La composición, organización y régimen de funcionamiento del **Consejo General de Servicios Sociales**.
- El Observatorio Canario de los Servicios Sociales.
- Y el Consejo de Atención Sociosanitaria.

El Título IV se refiere a la organización funcional y sistemas de gestión y de información del SPSS, mediante el uso de los siguientes sistemas de información: el portal Web del Sistema, la Historia Social Única y el Registro de Entidades y Servicios.

El Título V se dedica la calidad y a la mejora continua del Sistema público de servicios sociales con el fin de asegurar la eficacia de las prestaciones, actividades y servicios. Para ello, se contempla una serie de medidas para garantizar la calidad y los planes estratégicos de calidad. También se regula el régimen de inspección y evaluación de las entidades y establecimientos de los servicios sociales. Estos aspectos son una de las nuevas aportaciones que se hacen a la ley de 1987, en concreto con:

- La participación de las personas en la elaboración del Plan estratégico de calidad de los servicios sociales
- La metodología para la evaluación del Sistema Público de SS de Canarias
- La participación económica del beneficiario en el coste de los servicios y, en su caso, la exención a esa obligación, a efectos de cubrir el coste de las prestaciones por parte de la persona usuaria en los servicios públicos o concertados

El Título VI se refiere a la financiación del Sistema público de servicios sociales, indicando la cooperación financiera entre las distintas AAPP canarias, y a su vez, de éstas con la iniciativa privada. También se describe la participación económica de las personas usuarias.

En cuanto a la gestión de los servicios, el Título VII del APL está dedicado a regular la iniciativa social, el régimen general del Tercer Sector y su participación en el Sistema público a través de los conciertos sociales, nueva figura de gestión que ahora se crea. En general, se detectan las siguientes novedades:

- La participación de las entidades de iniciativa social.
- El régimen de registro, autorización o acreditación de las entidades privadas.
- El régimen de concertación la gestión por entidades de iniciativa social.
- La gestión integral de prestaciones, servicios o centros objeto de concierto social.
- Los méritos preferentes para suscribir los conciertos sociales.
- Los requisitos para la formalización de los conciertos.

El Título VIII regula el régimen sancionador, enumerando las infracciones en materia de servicios sociales y las sanciones que, por la comisión de dichas infracciones correspondan, dentro del marco de la normativa estatal básica, en la normativa que la desarrolle y en el resto de la normativa aplicable al ámbito de los servicios sociales y todo ello con el objeto de procurar el correcto funcionamiento del Sistema público.

- La determinación de los órganos competentes para imponer las sanciones
- La actualización de las cuantías de las sanciones previstas en la Ley
- La regulación del procedimiento sancionador

Finalmente, la ley establece varias disposiciones adicionales, transitorias y finales:

- Las adicionales tratan de las cláusulas sociales en la contratación pública; las políticas de inclusión activa para promover mercados de trabajo inclusivos; la regulación específica del Sistema para la autonomía y atención a la dependencia; el régimen peculiar del manejo de los datos de carácter personal en el ámbito de los servicios sociales; la gestión de la red de las escuelas infantiles adscritas a la Consejería con competencias en materia de infancia y familia;
- Las transitorias se ocupan del primer diagnóstico del **Observatorio Canario de los Servicios Sociales**; el régimen transitorio de las disposiciones vigentes de carácter reglamentario; el momento de exigibilidad de las prestaciones garantizadas; y, asimismo, la culminación del proceso de transferencias de competencias en materia de servicios sociales a los Cabildos Insulares.

De este modo, el presente informe analiza qué artículos de la nueva ley intervienen directamente en la estructura y planificación de PLASMAC, y que condiciones y requisitos técnicos deberá incluir para ser un referente a nivel regional en la gestión de los servicios sociales en Canarias.

INFORME DE REQUISITOS Y REQUERIMIENTOS TÉCNICOS DE PLASMAC

Con el fin de extraer un listado de requisitos y requerimientos técnicos que PLASMAC debe cumplir para satisfacer la legislación vigente, se ha realizado un estudio y análisis de dos de los principales documentos que han sido referentes para la creación y aprobación de la nueva ley de servicios sociales:

1) el Boletín Oficial del Parlamento de Canarias, informe de ponencia de Servicios

Sociales de Canarias (**BOPC, núm. 182/2, sobre el Proyecto de Ley de Servicios Sociales de Canarias, del 20 de marzo de 2019**), y

2) el Anteproyecto de Ley de Servicios Sociales de Canarias, varias actualizaciones de informe sobre la oportunidad, objetivos y principios generales del anteproyecto de ley de servicios sociales de Canarias, por la Consejería de empleo, políticas sociales y vivienda.

En cualquier caso, es necesario destacar que solo se tendrá en cuenta la información referida al proyecto de ley de servicios sociales de canarias más vigente posible, que a fecha de creación de la última versión de este informe corresponde con el BOPC núm. 182/2. Mientras que la información recogida en versiones anteriores, figurando la normativa como anteproyecto de ley, será tenida en cuenta para ampliar y orientar en mayor profundidad los aspectos relacionados con PLASMAC.

Además, el presente informe **no supone un resumen general de la norma**, sino un estudio específico para orientar a PLASMAC para que gestione de forma correcta según la última normativa aprobada, los servicios sociales a nivel local y regional, y garantizando su perdurabilidad y eficiencia en el tiempo.

Como resultado, se debe tener en cuenta dos aspectos relevantes:

- La nueva ley contempla hasta 108 artículos, donde se tratan disposiciones generales y aspectos generalistas que no son de aplicación directa a PLASMAC. Estos artículos se han obviado para facilitar el trabajo técnico a los responsables, tratando directamente aquellos aspectos que sí influenciarán en PLASMAC, resultando un estudio de la normativa más práctico, efectivo y menos engorroso.
- La anterior ley de 1987 dejó en un vacío legal muchos aspectos que, por fin, se tratan en la nueva ley. Es por ello que la nueva ley, contempla diferentes casos y aspectos que no afectan a PLASMAC.

Por ello, se contemplan unas posibles **hipótesis**, que podrían orientar PLASMAC hacia una herramienta especialmente dirigida a la gestión de los servicios sociales no solo a nivel local, sino también poderse conectar en el futuro, a nivel regional.

Estas hipótesis podrían ser modificadas y no deben ser tomadas como "únicas verdades", es decir, PLASMAC tiene ese carácter trasmutable que le permitirá adaptarse a las necesidades del futuro, pues toda la normativa sobre la que se ha basado este estudio es bastante reciente y no ha tenido tiempo suficiente para materializarse y/o madurar.

Estas hipótesis son:

1. En principio, PLASMAC estaría concebido como una plataforma de gestión de servicios sociales. En el futuro, podría incorporar otros servicios municipales que estén asociados a los servicios sociales, por ejemplo, con Urbanismo, Viviendas

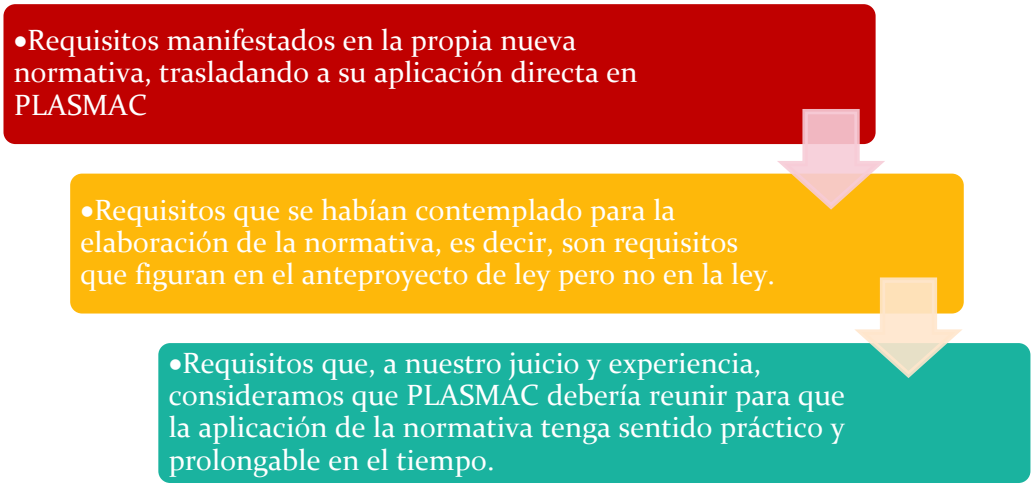
e Infraestructuras, etc.

2. Se podría decir que las raíces de PLASMAC es la propia información, es por ello, que debería tener diferentes bases de datos, interconectadas entre sí, actualizables y que deberán estar organizadas de una determinada manera, para que en el futuro, los organismos competentes del Gobierno de Canarias, puedan actualizarlas o se unan a librerías de otros municipios, etc.
3. Debido a que puede resultar complejo la utilización para los profesionales y para los propios usuarios, PLASMAC podría contemplar una sección o módulo de "*Training*" y de "*Support*" para solventar las posibles dudas. Se considera que PLASMAC en sí no sería una plataforma de formación, sino que podría facilitarla, aportando documentación u otros recursos.
4. Se espera que PLASMAC tenga su ámbito de aplicación a nivel local, pero en el futuro, podría conectarse, por ejemplo, entre diferentes ayuntamientos. Es por estos motivos que, se considera que PLASMAC podría tener unos protocolos de conexión que no sean cerrados y/o modificables. Es decir, PLASMAC podría estarse aplicando en dos ayuntamientos diferentes, pero a la vez, podrían establecerse conexiones entre esas dos plataformas.
5. Como se ha comentado, la ley de servicios sociales en Canarias, es muy reciente. Por ello, algunos contenidos no han sido desarrollados en su totalidad, como por ejemplo, el Sistema Canario de Información, los modelos para la Historia Social Única, el plan de atención personalizada, el registro único de centros, entidades y servicios, etc. [1]

No cabe duda que PLASMAC asume un reto importante, cumplir con una serie de requisitos según lo que se manifiesta en la nueva normativa. Y ahí es donde reside la importancia del estudio de PLASMAC, pues la nueva normativa no tiene nada desarrollado y solo se han tenido en cuenta aspectos generalistas que la antigua ley no contemplaba. Por todo ello, será la práctica y la madurez de la normativa, la aplicación de la nueva ley a la vida real la que marque el camino a seguir, y el que deberá seguir PLASMAC. Por ello, con este estudio se pretende que el camino que siga PLASMAC sea lo más **fiel, real, adaptable, práctico y útil** para que no quede "desfasado" en un futuro próximo y sea realmente útil para el desarrollo de este nuevo marco normativo en la sociedad canaria.

Dada la complejidad de este estudio y de la propia normativa, a continuación se detalla un listado de requerimientos técnicos para desarrollar PLASMAC, desde diferentes niveles:

[1] En los anexos se han añadido modelos a modo de propuesta, teniendo en cuenta lo expuesto en el APL. Se recomienda cierta prudencia y que estos sirvan de orientación, pues podrán atravesar diferentes modificaciones, pues en la nueva ley no se han descrito.



Debido a estos niveles de reflejo de la normativa en PLASMAC, se recomienda que los requisitos manifestados en la propia ley sean tenidos en cuenta con máxima prioridad. Mientras que los requisitos expuestos resultado de lo descrito en el anteproyecto de ley, tengan una prioridad intermedia, y finalmente, los requisitos expuestos por los analistas, como recomendaciones leves.

Aspectos en los que la nueva ley de servicios sociales hace especial hincapié:

REGISTRO DE USUARIOS Y PROFESIONALES

Según los derechos de las personas usuarias, recogidos en la nueva ley del sistema público de servicios sociales, incluyen el derecho al acceso y seguimiento, vía telemática, de su expediente. También tienen derecho a participar en la toma de decisiones, y a escoger libremente el tipo y modalidad de servicio más adecuado a su caso, según disponibilidad.

Requisito:
PLASMAC deberá permitir que las personas puedan acceder a información general sobre los tipos de servicios que existen y su correspondiente información privada.

Recomendación:
Se recomienda introducir una jerarquía de acceso a información de PLASMAC, pues existen datos sensibles e información de interés para el público en general. Para ello, se recomienda gestionar el acceso desde diferentes perfiles, con diferentes autorizaciones:

- Perfil "usuario"
- Perfil "Profesional de los servicios sociales"
- Perfil "Administración"

Se recomienda añadir el perfil de "Profesional de Referencia", a un/a Trabajador/a Social, que tenga un equipo interdisciplinar de Profesionales de servicios sociales, y que cada usuario tenga uno asignado.

De esta manera, el perfil "usuario" solo podrá tener acceso a aquellos datos que le atañen directamente. Y la diferencia entre los perfiles de "profesionales de los servicios sociales" y el de "administración" implica el uso de esa información.

Es decir, los profesionales, son personas que intervienen en áreas específicas (dependencia, discapacidad, etc.) y hacen una "valoración especializada" social, psicosocial, sociosanitaria o socioeducativa, y una "valoración de seguimiento" del plan de intervención de cada persona.

Mientras que los de "administración" simplemente, gestionan los recursos y acceden a información, por ejemplo, anonimizada, para realizar estadísticas, informes, inspecciones, etc.

Sugerencia:
Se sugiere que para los perfiles de "Profesional de servicios sociales" y de "Administración", se reproduzca la jerarquía interna de los propios organismos hasta definir las diferentes unidades operativas.
Podrán ser, dentro del grupo de "profesionales de los servicios sociales" aquellas personas que formen parte de la iniciativa social, pero que estén debidamente identificadas y su participación y el acceso a PLASMAC, esté condicionado por la vigencia de la "Autorización Administrativa Definitiva de Funcionamiento".
Se sugiere asignar a cada profesional de los servicios sociales, un segundo rol dentro del equipo de trabajo.
Se recomienda incluir dentro del perfil "Administración" el perfil de "Personal de Inspección".

A modo de nota aclaratoria, se entiende que estos requisitos están estrechamente vinculados con el módulo de «**Gestión de la seguridad**» de PLASMAC, para limitar la visibilidad de la información según el encargo de los operadores dentro de la organización y con el papel o rol que tengan dentro de los servicios sociales.

Sugerencia:

En cuanto a los profesionales de los servicios sociales, se deben distinguir hasta tres niveles:

- Nivel 1:

Son profesionales de intervención en su nivel más básico, solo pueden recogen información (datos y documentos) y son los que hacen la "valoración inicial" de sus usuarios: en si una situación es urgente o no. Si es urgente derivan a otros profesionales de nivel 2. Además, rellenan estos dos modelos para cada persona, unidad familiar o de convivencia:

  - Modelo de Historia Social Única
  - Modelo del Plan de Atención Personalizada

- Nivel 2:

Son profesionales de intervención de áreas específicas (dependencia, discapacidad, etc.) y hacen una "**valoración especializada**" social, psicosocial, sociosanitaria o socioeducativa, y una "**valoración de seguimiento**" del plan de intervención de cada persona. Existe un "**Profesional de Referencia**" que tiene asignado un grupo de personas según un área determinada.

- Nivel 3:

Son profesionales de administración que acceden a la información según las necesidades para elaborar informes (acceso a datos anonimizados o semi anonimizados de las personas beneficiarias, pero que puedan filtrarlos por localidad, género, edad...) o datos específicos de expedientes de personas en concreto.

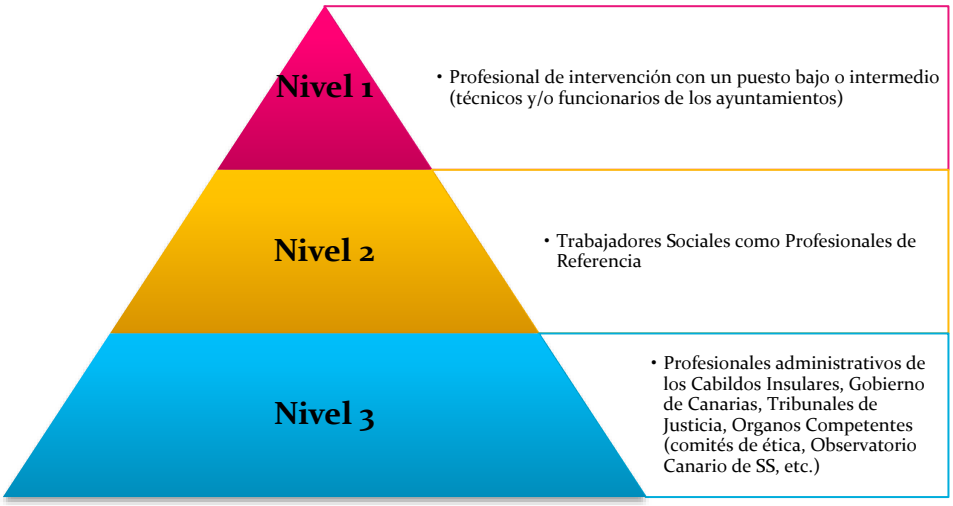


Figura: Diferentes niveles de los profesionales [Utilizar a modo de orientación]

INFORMACIÓN DE CARÁCTER PÚBLICO

Las personas que acceden a los servicios sociales y por tanto a PLASMAC, deben tener información profesional, suficiente y fácilmente comprensible, sobre sus derechos y deberes, los servicios y prestaciones disponibles, los requisitos para acceder a los mismos, y los mecanismos de presentación de quejas y reclamaciones.

Requisito:
PLASMAC debería plasmar información sobre:

- La Carta de Derechos y Obligaciones (*ver anexo I*)
- El Catálogo de Servicios y Prestaciones (*ver anexo II*)
- El Mapa de Servicios y Prestaciones
- Los mecanismos para la presentación de quejas y reclamaciones

Recomendación:
PLASMAC debería poder habilitar este contenido para que fuese "descargable" e imprimible, en caso de que así lo solicite alguna persona.
Se recomienda que PLASMAC vuelque la información recogida del Registro Único de Entidades, Centros y Servicios, filtrando solo cuatro variables:

- Tipo: Servicio, prestación tecnológica, prestación económica y otros.
- Requisitos necesarios de los usuarios para beneficiarse de un tipo de ayuda
- Disponibilidad de los mismos (que dependerá de la vigencia de la "Autorización Administrativa Definitiva de Funcionamiento")
- Ubicación de los servicios y prestaciones, o de las entidades y centros que ofrecen estos servicios sociales y que estén registradas en el "Registro Único de Entidades, Centros y Servicios".

Requisito:

El **Mapa de Servicios Sociales de PLASMAC** establecerá el despliegue del Sistema Público de Servicios Sociales, definiendo al efecto los criterios poblacionales más idóneos para la implantación de los diferentes servicios incluidos en el Catálogo, atendiendo a la naturaleza de los mismos, al número de personas potencialmente demandantes y a la necesidad de garantizar, en todo lo posible, su mayor proximidad con vistas a facilitar la integración de las personas usuarias en el entorno social habitual.

En el **Mapa de Servicios Sociales**, se establecerán las ratios y la cobertura para cado uno de los servicios y prestaciones en función de los sectores poblacionales y territoriales establecidos y las necesidades de atención detectadas.

Recomendación:

Se recomienda incluir una herramienta estadística que vuelque los datos de las personas de un municipio que estén recibiendo algún servicio social en un determinado centro.

Se recomienda que esta información solo pueda tener acceso un determinado perfil, anonimizando los datos de las personas que están implicadas, o permitiendo filtrar estos datos por alguna variable de estudio.

Las entidades de iniciativa privada social o mercantil, deberán figurar inscritas en el "Registro Único de entidades, centros y servicios", y además, disponer de la "Autorización administrativa" (previa y finalmente, la definitiva de funcionamiento) para poder acceder a la "Concertación Social".

El procedimiento por el cual una entidad de iniciativa privada debe recorrer para poder ofrecer un determinado servicio social de forma integral o parcial, puede resultar abrumador (ver anexo III).

Entre estos pasos, cabe destacar que requiere de que estas entidades se registren previamente en el Registro Único de Centros de PLASMAC, y posteriormente consigan las autorizaciones administrativas determinadas (después de la comprobación de una serie de condiciones y especificaciones).

Solo hasta que consigan la Autorización Administrativa Definitiva de Funcionamiento, conseguirán poder entrar en el Catálogo de Servicios y Prestaciones de PLASMAC. Esta situación se explica mejor en el siguiente gráfico:

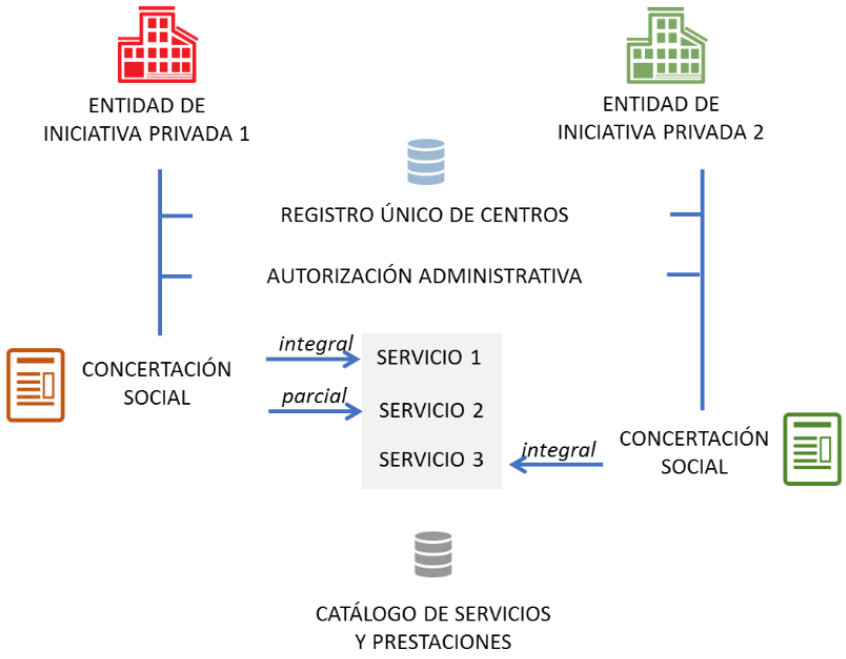


Figura: Relación entre el Registro Único de Centros y el Catálogo de Servicios y Prestaciones.

La información que se debe recopilar, por tanto, en el Registro Único de Centros y el Catálogo de Servicios y Prestaciones, deberá tener el mismo contenido único y genérico que permita después su valoración, para la obtención de las correspondientes Autorizaciones Administrativas.

Requisito:

1. El Registro único de entidades, centros y servicios autorizados y, en su caso, acreditados, del Sistema Público de servicios sociales se crea como instrumento básico para el conocimiento, constatación, publicidad y control de los servicios y las entidades que los prestan

2. El Registro único tiene naturaleza pública, y depende orgánicamente de la Consejería competente en materia de Servicios Sociales.

3. Los datos que debe contener el registro y el procedimiento de inscripción, modificación y cancelación de estos se establecerán reglamentariamente por el Gobierno de Canarias, indicando los que tienen carácter público.

4. El Registro se organizará en las secciones que establezca el Gobierno de Canarias reglamentariamente.

5. Se constituirán secciones insulares del Registro en cada una de las islas, las cuales dependerán de cada cabildo Insular.

6. Los datos de este Registro servirán de base para la elaboración del Mapa de Servicios Sociales que permitirá conocer su distribución por el territorio.

Sugerencias:

El Registro único de entidades, centros y servicios autorizados y, en su caso, acreditados, del Sistema Público de servicios sociales (que abreviaremos como "el Registro") debe contener información "pública" pero también "privada" que atañe a datos sensibles de estos centros.

Se recomienda que, antes de incluir un centro en el catálogo de PLASMAC, se compruebe que este centro dispone de la "Autorización Administrativa" (*ver procedimiento de acción concertada en el anexo III*).

Los datos que debe contener el Registro y el procedimiento de inscripción, modificación y cancelación sean los mismos para centros, entidades privadas, públicas del Tercer Sector...

Se sugiere clasificar internamente el Registro de PLASMAC por secciones, que posteriormente puedan activarse a nivel insular.

El procedimiento de inscripción en el Registro, se describe en detalle en el anexo III y corresponde a la descrita en el gráfico anterior.

Requisito: El Catálogo de Servicios y Prestaciones, según la ley deben ser:

Para los servicios:

- Información
- Valoración:
  - Valoración inicial
  - Valoración Especializada
  - Valoración de seguimiento
- Diagnóstico social
- Orientación y seguimiento
- Acompañamiento social
- Prevención de la situación de dependencia y promoción de la autonomía personal:
- Cuidados en el entorno familiar:
  - Servicio de apoyo a las personas cuidadoras.
  - Ayuda a domicilio.
  - Centro de día o noche.
  - Centros ocupacionales.
- Intervención:
  - Intervención y apoyo familiar.
  - Intervención socio-familiar.
  - Prevención e intervención socio-comunitaria e inclusión social.
  - Intervención socioeducativa y psicosocial.
  - Intervención socio-sanitaria.
  - Intervención socio-laboral de colectivos en riesgo o exclusión social.
- Atención residencial.
- Servicio de Atención Temprana.
- Protección jurídica y ejercicio de la tutela de las personas mayores de edad con capacidad de obrar modificada y en situación de desamparo.
- Alojamiento para personas sin hogar.
- Atención a mujeres víctimas de violencia de género, doméstica o de actos contra la libertad sexual.
- Servicio de Atención a la Infancia y Adolescencia.
- Servicio de apoyo a la emancipación.

Para las prestaciones económicas:

- La vinculada a cubrir necesidades básicas:
  - Alojamiento de urgencia
  - Atención alimenticia
  - Vestido
  - Higiene y aseo personal
  - Medicamentos
  - Suministros básicos de la vivienda (agua, luz, gas, etc.)
  - Alquiler de la vivienda
- La vinculada a cuidados en el entorno familiar y apoyo a personas cuidadoras no profesionales
- La vinculada a la asistencia personal
- La vinculada al servicio
- La vinculada al pago único a mujeres víctimas de violencia de género
- La vinculada a la realización de adaptaciones en la vivienda habitual y en los vehículos particulares
- Prestación económica individual para la adquisición de ayudas técnicas y productos de apoyo
- Prestación económica para el acogimiento familiar
- Prestación económica de apoyo a la emancipación dirigida a jóvenes extutelados.
- Prestación económica de percepción periódica vinculada a la inclusión social.
- Prestación económica, de percepción periódica vinculada a la inclusión social.

Para las prestaciones tecnológicas:

- La asistencia tecnológica o técnica
- La teleasistencia
- La asistencia para la accesibilidad universal

Otros servicios y prestaciones

Se debe dejar un apartado del listado en "otros" en caso de que en el futuro se añadan como causa de las actualizaciones del catálogo.

Sugerencia:

Se sugiere que PLASMAC permita la gestión de reclamaciones y quejas a través de un formulario web, que sea capaz de devolver la respuesta de dicho procedimiento administrativo al usuario.

Sugerencia:
Se sugiere que el lenguaje utilizado en la información expuesta en PLASMAC sea en "términos comprensibles"
PLASMAC podría tener una opción de que los usuarios puedan rechazar voluntariamente a la utilización de un servicio y/o prestación que se le haya reconocido a una persona (siempre que no venga interpuesta por Resolución Judicial).
Se podría indicar además en el catálogo, el régimen de oferta a régimen parcial o integral de cada centro, por ejemplo, según lo especificado en el "Acuerdo de acción concertada".

OBLIGACIONES DE LAS PERSONAS USUARIAS

Entre las obligaciones de las personas usuarias, se destacan además los siguientes requisitos:

Requisito:
Las personas tienen el derecho de poder escoger libremente el tipo y modalidad de servicio más adecuado a su caso en función de su disponibilidad, atendiendo a la orientación de la persona profesional de referencia asignada.

Sugerencia:
Se sugiere que PLASMAC muestre el Catálogo de Servicios y Prestaciones de manera que el usuario pueda comprobar qué alternativas tiene disponible y que este pueda actualizarse, pues así podría saber la disponibilidad.

INFORMACIÓN DE CARÁCTER PRIVADO

En cuanto a la información de "carácter privado", cada persona usuaria y el equipo de personas profesionales del Sistema Público de Servicios Sociales, será muy específica y podrá tener algunos campos ocultos.

Requisito:
Las personas usuarias del sistema público de servicios sociales poder conocer la valoración, el diagnóstico técnico, a un itinerario individualizado de su situación particular, y el tipo de intervención que se le asigne.

Es por ello que se considera que, a través de PLASMAC, las personas pueden conocer esta información de forma telemática si tuvieran acceso a una determinada información de su expediente.

De cualquier modo, se espera que la información en PLASMAC siempre y en todos los casos se disponga de cada persona dos documentos importantes:

Requisito:
PLASMAC deberá presentar la información de cada persona usuaria de forma que sea compatible en un futuro con:

- Historia Social Única (tendrá un número de identificación)
- Plan de Atención Personalizada (o Plan de Intervención Social Personalizado)

Recomendación:

- Se recomienda que PLASMAC tenga la opción de generar estos dos modelos a partir de la información que introduzca el personal de Asistencia Primaria y Comunitaria de los profesionales de servicios sociales.
- Se recomienda que esta información, puedan tener acceso exclusivamente las personas profesionales de los servicios sociales y los propios interesados (habrá datos que se limitarán en función del perfil de acceso).
- Cada persona usuaria tendrá asignado un código alfanumérico que será único e intransferible. Podrá ser actualizable en caso de que exista alguna incompatibilidad con otro código de otra localidad en el futuro.

De forma adicional, y atendiendo a los derechos de las personas usuarias de los servicios sociales, PLASMAC podría implicar la gestión de los servicios y prestaciones que se les asigna a las personas, pudiendo hacer uso de su libertad de decisión:

Requisito:
Las personas que accedan a obtener servicios o prestaciones deberán firmar un acuerdo con la entidad prestadora de los mismos.

Sugerencia:
Se sugiere que PLASMAC contemple la opción de adjuntar documentación, generar acuerdos y habilitar la herramienta de firma electrónica o firma digital.

LA HISTORIA SOCIAL ÚNICA Y EL PLAN DE ATENCIÓN PERSONALIZADA.

En la nueva ley canaria de Servicios Sociales, no se ha descrito ninguna "plantilla" o "modelo" o solicitud general que deba tenerse en cuenta para la creación de esta documentación, de tal manera que todos los expedientes tengan la misma validez, en tanto que recojan los datos necesarios para evaluar cada uno de manera correcta, equitativa, igualitaria...

Estos datos deberían ser los que en PLASMAC figurase para la gestión de los expedientes de todas las personas de los servicios sociales de un ayuntamiento.

Requisito:
El contenido mínimo de cada modelo es:

Para la Historia Social Única:

a. Información relevante de la persona usuaria y los documentos que contienen los datos.
b. La valoración sobre la situación objeto de intervención.
c. El plan personalizado de atención social.
d. La identificación del personal profesional.
e. Las prestaciones.

Y para el Plan de Intervención Social:

a. El diagnóstico de la situación y la valoración de las necesidades:
    a. Valoración inicial,
    b. Valoración especializada y
    c. Valoración de seguimiento
b. Los objetivos propuestos.
c. Las prestaciones previstas.
d. La planificación de las actuaciones.
e. Los indicadores de evaluación y seguimiento.

Sugerencia:
Se recomienda incluir los campos que se desarrollaron en mayor extensión en el Anteproyecto de Ley para la Historia Social Única:

- Identificación (incluyendo el domicilio, si es residente canario o está empadronado/a)
- Núcleo de convivencia
- Relaciones familiares y sociales de la persona
- Situación laboral
- Nivel educativo
- Capacidad económica
- Todas las actuaciones realizadas por el Sistema público de SS:
    - Solicitudes
    - Valoraciones
    - Reconocimientos
    - Infracciones, clasificándolas en: "Leves", "Graves" y "Muy graves"
    - Código de identificación si dispone de Tarjeta Social (esto no debe ser considerado un campo obligatorio)
    - Contratos de servicios firmados con la entidad prestadora del servicio
- Situación de necesidad de la persona demandante (ver descripción de las personas con acceso al sistema púbico de servicios sociales, descrito anteriormente).

PERSONAS QUE PUEDEN ACCEDER A LOS SERVICIOS SOCIALES

La identificación de las personas con acceso al Sistema Público de servicios sociales es importante para delimitar a la población que puede tener acceso y beneficiarse de diferentes tipos de ayudas contempladas en la nueva ley.

La identificación y documentación aportada por los usuarios debe presentarse ante los Servicios de Atención Primario y Comunitaria de cada Ayuntamiento. Estos serán responsables de comprobar que esta información es verídica. En caso de tratarse de una situación de urgencia, lo derivarán a otros responsables, que en la ley no se describe.

Requisito:
Las personas que pueden tener acceso al Sistema Público de Servicios Sociales, y por tanto, a PLASMAC, son:
a) Las personas con nacionalidad española, sus familias y demás unidades de convivencia, así como aquellas
que sean nacionales de los Estados miembros de la Unión Europea, empadronados y con residencia en Canarias.
b) Las personas nacionales de países no incluidos en la Unión Europea, sus familias y demás unidades de convivencia, que carezcan de nacionalidad española, siempre que estuvieran empadronados y fueran residentes en Canarias.
c) Las personas emigrantes de nacionalidad española, sus cónyuges o sus descendientes de igual nacionalidad que hubieran tenido en Canarias su último domicilio y que hayan retornado al archipiélago en los términos establecidos en el Estatuto de Autonomía de Canarias.
d) Las personas menores de edad extranjeras que se encuentren en Canarias con independencia de su situación administrativa.
e) Los refugiados, asilados, solicitantes de protección internacional y apátridas tendrán asimismo derecho a los servicios sociales en los términos que las normas legales y reglamentarias y los convenios internacionales ratificados por España determinen.
f) Todas aquellas personas no contempladas en los apartados anteriores, que se encuentren en Canarias en situación de urgencia social con independencia de su situación administrativa.
Lo anterior se entiende sin perjuicio de los requisitos adicionales respecto de un periodo de empadronamiento previo o de otra naturaleza que se establezcan para el acceso a los diferentes servicios y prestaciones del Sistema Público de Servicios Sociales, en la nueva ley o en otras disposiciones que resulten de aplicación a PLASMAC.

Sugerencia:
Se sugiere que los campos que tengan que completar el personal de cada Ayuntamiento responsable de la Atención Primaria o Comunitaria, para todas las personas usuarias, se correspondan con los anteriormente descritos, y en su caso, puedan guardar documentación relacionada.

Usuarios/as	Condiciones
Personas con nacionalidad española, nacionales de los Estados miembros de la Unión Europea	Empadronadas y con residencia efectiva en cualquiera de los municipios de Canarias
Personas nacionales de países no incluidos en la Unión Europea que carezcan de nacionalidad española	En los términos que establece la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social y, en su caso, en los convenios internacionales vigentes sobre la materia que tenga suscrito el Reino de España, siempre que fueran residentes en Canarias
Personas emigrantes de nacionalidad española o sus descendientes de igual nacionalidad	Que hubieran tenido en Canarias su último domicilio y que hayan retornado al Archipiélago, en los términos establecidos en el artículo 4.2 del Estatuto de Autonomía de Canarias

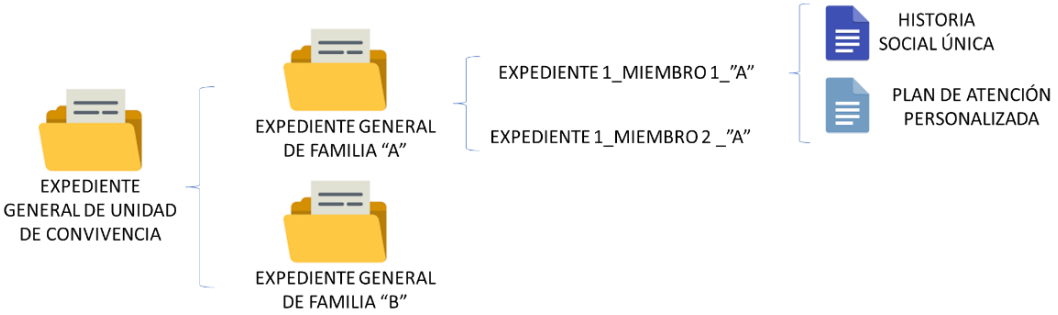
Personas menores de edad extranjeras	Que se encuentren en situación de riesgo o bajo la tutela o guarda de la Comunidad Autónoma de Canarias, aun cuando no residan legalmente en Canarias
Las personas sin hogar, en situación de emergencia social que requieran una rápida intervención de los recursos y servicios sociales.	
Las mujeres respecto a los servicios y prestaciones de intervención y asistencia ante situaciones inminentes de violencia de género o riesgo de las mismas.	Cualquiera que sea su edad, estado civil, nacionalidad o lugar de residencia, que se encuentren en territorio de la Comunidad Autónoma
Los refugiados, asilados y apátridas	En los términos que las normas legales y reglamentarias y los Convenios internacionales ratificados por España determinen

UNIDADES FAMILIARES Y DE CONVIVENCIA

Se entiende que, para cada persona, existe la posibilidad de que otras personas de su mismo entorno familiar, por ejemplo, requieran de otros servicios. Es por ello que, se estima necesario que PLASMAC reúna las siguientes sugerencias.

Sugerencia:
La estructura lógica y ordenada de PLASMAC de las bases de datos de las personas que acceden a los servicios y prestaciones, debería tener una estructura que facilite la labor de trabajo de los profesionales de los ayuntamientos.
Para ello, se sugiere que PLASMAC tenga una estructura de "Expedientes" para cada tipo de intervención que se realice a cada persona. Es decir, se recomienda que se cree un **Expediente General de Unidad de Convivencia**, y a partir de este, se generen los **Expedientes Generales de Familia**, y dentro, los diferentes expedientes individuales para cada miembro de la familia. Para cada expediente individual, se debería poder acceder a la **Historia Social Única** y al **Plan de Atención Personalizada** (*ver esquema siguiente*).

No obstante, se sugiere que estos expedientes solo puedan estar accesibles para los profesionales de los servicios sociales y en el caso de los expedientes individuales solo los propios usuarios (en caso de ser representantes legales de menores, podrán acceder los representantes legales que tengan la tutela).



Sugerencia de ordenación de los expedientes de los usuarios en PLASMAC [Elaboración propia].

Sugerencia:
Se recomienda incluir la posibilidad de "Exportar" la información recogida en cada expediente en diferentes formatos, filtrando campos o datos de los usuarios, de tal forma que los diferentes perfiles de profesionales y de administración, puedan trabajar solo con a información que precisan sin vulnerar los derechos de protección de datos.
Se recomienda que los profesionales de los servicios sociales puedan subir documentación a los expedientes.
Se recomienda incluir, para los profesionales de los servicios y prestaciones, la posibilidad de ver si un expediente tiene un caso pendiente de inspección o una sanción.
Los profesionales del sistema deben clasificarse según su formación, experiencia, área de trabajo y zona geográfica. De esta manera, a la hora de asignar un Profesional de Referencia, se haga de manera lógica y ordenada.

Recomendación:
Se recomienda crear "grupos de trabajo" para los que, el líder sea el Profesional de Referencia, necesariamente un/a Trabajador/a Social y que el resto de miembros del equipo puede ser de diferente titulación.

INSPECCIÓN Y SANCIÓN

Dado que uno de los aspectos importantes de la gestión a través de PLASMAC podría permitir agilizar o facilitar la vigilancia, control y comprobación de los Servicios Sociales, participen o no en el Sistema Público de Servicios Sociales, a fin de que su actuación se adecue a lo dispuesto en la nueva ley de servicios sociales y en las futuras normativas. PLASMAC podría contener un módulo de carácter privado y que solo pueden tener acceso el perfil de "Personal de Inspección".

Requisito:

Solo podrán tener acceso el personal inspector para el ejercicio de sus funciones. No pueden verlo las personas usuarias.

Podrán generarse desde PLASMAC **las actas de inspección** con el siguiente contenido mínimo:

a) Fecha, hora y lugar de actuaciones.

b) Identificación del personal inspector.

c) Identificación de la entidad prestadora de servicios y de la persona responsable ante cuya presencia se lleva a cabo la inspección y ante la cual se extiende el acta.

d) Hechos y circunstancias relevantes sobre los servicios que hayan sido detectados en la inspección realizada.

e) Firma del inspector y de la persona responsable de la entidad prestadora del servicio, así como, la conformidad o disconformidad de esta última, que podrá hacer constar cuantas manifestaciones considere necesarias.

Sugerencia:

Las personas físicas o jurídicas que son titulares o gestionan los centros o servicios sociales, así como el personal de gestión y directivo de estos, que tengan acceso al Registro Único de Entidades de PLASMAC de su correspondiente entidad, podrán recibir notificaciones al respecto a través de los resultados de las correspondientes Actas de Inspección emitida a través de PLASMAC.

El sistema de imposición de sanciones viene regulado en la nueva ley de Servicios Sociales desde tres niveles: leves, graves, y muy graves. Los criterios de cada graduación se describen en detalle en el anexo IV.

Capítulo 2. Protección de datos. Requisitos técnicos para el cumplimiento del Reglamento General de Protección de Datos en el marco del proyecto PLASMAC

El segundo bloque del estudio se centra en el análisis de los requisitos técnicos para el cumplimiento del Reglamento General de Protección de Datos en el marco del proyecto PLASMAC.

TERMINOLOGÍA

AAPP: Administraciones Públicas.

AEPD: Agencia Española de Protección de Datos.

Autoridad de control: la autoridad pública independiente establecida por un Estado miembro.

Consentimiento del interesado: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

Datos personales: Los datos personales cualquier tipo de información que se pueda usar para identificar directa o indirectamente a una persona.

Destinatario: Interesado.

Elaboración de perfiles: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física.

Encargado del tratamiento (encargado): la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Fichero: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

Interesado: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero.

Limitación del tratamiento: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.

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

Normas corporativas vinculantes: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos

personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta.

Nube: Espacio virtual al que se accede a través de internet en el que se guardan datos para que otros usuarios conectados a la misma red puedan acceder a ellos y usarlos.

Responsable del tratamiento (responsable): la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

RGPD: Reglamento General de Protección de Datos.

Seudonimización: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional.

Tercero: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Violación de la seguridad de los datos personales: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

INTRODUCCIÓN

En la era moderna, los datos (personales) se han convertido en un bien preciado y, gracias a la **transformación digital**, en vías de convertirse en el bien más preciado de personas, empresas u organizaciones.

Hasta este momento, en las sociedades modernas e industriales, los ciudadanos eran consumidores pasivos de los medios de información de masas (prensa, radio y televisión), en cambio, hoy producimos una **gran cantidad de información**. La inmensa mayoría de ella la producimos de forma en gran parte inconsciente en nuestra actividad cotidiana en Internet. La búsqueda en la red, el uso de las redes sociales o la compra online son actividades cada vez más extendidas.

Toda esta información se acumula a lo largo del tiempo sin efectos aparentes. Pero los datos son el petróleo de la sociedad de la información, un **recurso clave** para que los actores tomen decisiones en contextos de incertidumbre creciente. Por eso, la información no permanece aislada. **El conocimiento surge cuando los datos son agregados, analizados y reutilizados**. Los efectos agregados de mayor información y mayor poder de computación dan lugar a una nueva versión de la estadística: el *Big Data*. Con él, es posible extraer tendencias sociales y predecir comportamientos. Por ello, es un recurso tan valioso.

Su valor es paralelo al riesgo que comportan. Y es que los distintos actores -fundamentalmente empresas y administraciones- pueden utilizarlos tanto para **fines legítimos como ilegítimos**. Las empresas pueden usarlos para **personalizar su oferta** y desarrollar productos y servicios adaptados a la demanda, con mayor calidad y a precios decrecientes, haciendo que los **ciudadanos estén mejor informados** en su comportamiento como consumidores. Las administraciones pueden usarlos para **mejorar la transparencia** y para diseñar y evaluar sus políticas públicas según las evidencias disponibles, siendo más eficaces y eficientes, y ofreciendo a los ciudadanos una vía de control adicional de las actuaciones de los poderes públicos. Pero, también caben **usos ilegítimos**.

Estas **nuevas formas de criminalidad** destacan por su bajo coste, la capacidad de afectar a una gran cantidad de dispositivos o a infraestructuras críticas, la posibilidad de hacerlo desde cualquier lugar con conexión a internet y la consecuente dificultad de seguimiento. **Un ataque lanzado por personal cualificado tiene grandes posibilidades de éxito** frente a la dificultad de custodia ante cualquier amenaza de un ingente volumen de datos a lo largo de un tiempo indefinido.

PLASMAC es una plataforma en la nube que permite a las administraciones regionales mejorar los procesos de valoración, atención y prestación de servicios a los ciudadanos. Factores como envejecimiento, el aumento de enfermedades crónicas o cambios en la estructura y organización de las familias o de la organización social del cuidado impulsan al avance de las políticas públicas, con el fin de que éstas puedan responder de manera proactiva e innovadora a estos desafíos sociales.

Con este objetivo, en el presente informe se analiza cómo PLASMAC debe actuar para salvaguardar la seguridad y privacidad de los datos que se recogen, gestionan y almacenan para hacer frente a los servicios socio-asistenciales de la población.

MARCO LEGAL DE PLASMAC

El avance de la tecnología es tan rápido que muchas veces supera a las leyes, y es que la última ley europea al respecto databa de 1995. A nivel nacional, la ley vigente hasta el año 2018 era la Ley Orgánica 15/1999, de Protección de Datos de carácter personal. En ambos casos, la legislación quedó obsoleta. Es por ello, que el 25 de mayo de 2018 entró en vigor el **Reglamento General de Protección de Datos** (RGPD), aprobado como normativa de Control (UE) 2016/679. El RGPD pretende elevar la protección de datos en todos los países de la Unión Europea mediante la devolución de los datos a los

ciudadanos y a su derecho a controlar su información personal. Para ello, se **realiza un marco regulador común para todos los países de la Unión** y actuar contra las multinacionales con respecto al intercambio de datos fuera de Europa.

Por otro lado, el 5 de diciembre de 2018 se aprueba la **Ley de Protección de Datos y Garantía de los Derechos Digitales** (LOPDGDD) cuya finalidad es la introducción en el ordenamiento jurídico interno del RGPD. Si bien la LOPDGDD es la trasposición nacional del reglamento europeo, **supone algunas pequeñas diferencias con respecto al reglamento comunitario** (y que éste da cabida a la modificación por parte de los Estados Miembros).

Los principales aspectos introducidos por la LOPDGDD, con respecto al texto original del RGPD, pueden resumirse en diez puntos:

1. Legitimación de las AAPP para utilizar y ceder datos personales

El art. 8 de la LOPDGDD aclara cuándo el tratamiento de datos personales podrá considerarse fundado en el cumplimiento de una obligación legal exigible a la AAPP. El RGPD establece dos bases legales para la utilización y cesión de los datos por una AAPP.

2. Utilización de datos para perfilación partidos políticos

La LOPDGDD establece la utilización de medios tecnológicos y datos personales en las actividades electorales por los partidos políticos.

3. Delegado de Protección de Datos (DPD)

La LOPDGDD otorga el papel de intermediario al DPD en caso de reclamación ante las autoridades de protección de datos.

4. Redes sociales y protección de datos

La LOPDGDD incorpora el derecho al olvido en servicios de redes sociales y servicios equivalentes. Además, incorpora el derecho de portabilidad en servicios de redes sociales y servicios equivalentes.

5. Nuevas obligaciones de transparencia

La LOPDGDD modifica la Ley 19/2013 de Transparencia, Acceso a la Información Pública y Buen Gobierno (LTBG) a través de la Disposición adicional segunda relativa a la protección de datos y transparencia y acceso a la información pública.

6. Protección de Datos de las personas fallecidas

Las personas vinculadas al fallecido por razones familiares o, de hecho, así como sus herederos, podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella para su rectificación o supresión.

7. Intermediación de datos en el Procedimiento Administrativo Común (LPAC)

La Disposición adicional octava, relativa a la potestad de verificación de las APP, otorga legitimidad al señalar cuando se formulen solicitudes en las que el interesado declare datos personales que obren en poder de las AAPP, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la exactitud de los datos.

8. Novedades en el régimen jurídico de los empleados

La LOPDGDD, en su art. 91, relativo a los derechos digitales en la negociación colectiva ofrece garantías adicionales, que modifican las dos normas básicas que regulan las relaciones laborales.

9. Modificación de normas importantes

Además, de en la LOREG, LPAC y LTBG, se modifican la Ley Orgánica del Poder Judicial, la Ley General de Sanidad, la Ley reguladora de la Jurisdicción Contencioso-administrativa, la Ley de Enjuiciamiento Civil, la Ley Orgánica de Universidad, la Ley básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica y la Ley Orgánica de Educación.

10. Introducción de los derechos digitales

La LOPDGDD, en el Título X relativo a la garantía de los derechos digitales, recoge los derechos que introducen en el ordenamiento jurídico, aspectos necesarios para adaptar la norma a la sociedad actual.

De este modo, el presente informe analiza de qué forma y en qué medida PLASMAC debe actuar para satisfacer los requerimientos legales tanto del RPGD y la LOPDGDD como referentes máximos legales en torno a la seguridad y privacidad de los datos de carácter personal.

INFORME DE REQUISITOS Y REQUERIMIENTOS TÉCNICOS DE PLASMAC

Con el fin de extraer un listado de requisitos y requerimientos técnicos que PLASMAC debe cumplir para satisfacer la legislación vigente, se ha realizado un estudio y análisis de las dos normas de aplicación para la protección de los datos de carácter personal que son de aplicación: (1) el Reglamento General de Protección de Datos – de aplicación en todos los Estados Miembros de la Unión Europea y (2) la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales – de aplicación en todo el territorio nacional. Es necesario destacar que:

> Este informe **no supone un resumen general de la norma,** sino un estudio específico para el ámbito y finalidad con la que PLASMAC tratará los datos.

Como resultado, se debe tener en cuenta dos aspectos relevantes: 1. Hay artículos y normas que no son de aplicación a PLASMAC debido a la tipología, funcionalidad, carácter o finalidad del tratamiento de los datos, por lo que, con el objetivo de hacer efectivo el informe se han obviado todas las partes que no son de aplicación a PLASMAC. 2. Como todo reglamento y/o ley, el articulado de los mismos estima una gran variedad de casos. En este informe, se ha realizado una serie de hipótesis con el fin de aligerar y mejor el entendimiento del contenido del documento. A continuación, se resumen las hipótesis seguidas:

6. *No hay transferencias internacionales de datos (fuera del espacio UE)*
7. *Se tratarán datos de menos de 14 años*
8. *Se estima que PLASMAC, como responsable de los datos, es una Administración Pública*
9. *PLASMAC no hará pública ninguna información obtenida directamente del interesado o a partir del tratamiento de datos de éstos.*
10. *Se estima que PLASMAC realizará tratamientos a gran escala de datos sensibles.*

A continuación, se detalla el resultado obtenido tras el estudio comparativo de la norma y el análisis de cómo la legislación vigente afecta el funcionamiento de PLASMAC como plataforma de gestión de datos en la nube. Para una organización eficiente de los resultados obtenidos, los requisitos y recomendaciones técnicas se han dividido en seis grandes bloques:

1. *Principios de PLASMAC para el tratamiento de los datos* – La base en la que se debe apoyar PLASMAC para realizar el tratamiento de datos de carácter personal y sobre la claridad en la que se informa a las personas de las condiciones del tratamiento.
2. *Cómo PLASMAC garantiza los derechos de las personas* – Los derechos que tienen las personas sobre sus datos de carácter personal. Además, establece cómo PLASMAC debe atender estos derechos.
3. *Relación entre PLASMAC y los profesionales del servicio* – Las obligaciones de PLASMAC, como responsable del tratamiento, y las garantías técnicas que debe cumplir un encargado del tratamiento y qué actividades debe desarrollar.
4. *Medidas de PLASMAC para una responsabilidad activa* – Las medidas que debe tomar PLASMAC para garantizar que dicho tratamiento se realiza conforme a la legislación vigente.
5. *PLASMAC y los menores de edad* – Las medidas que debe tomar PLASMAC para obtener el consentimiento explícito de menores para el tratamiento de sus datos.

6. *Listado de verificación* – La AEPD ha puesto a disposición pública una guía-listado de verificación, con el fin de comprobar la situación en que se encuentra con respecto a la aplicación de la legislación vigente.

PRINCIPIOS DE PLASMAC PARA EL TRATAMIENTO DE LOS DATOS

Con la nueva legislación (RGPD y LOPDGDD), se mantiene el principio recogido en la Directiva 95/46, de que todo trata**miento de datos necesita apoyarse en una base que lo legitime**. El RGPD ofrece seis bases legales para la recopilación y el procesamiento de datos en Europa:

- Interés vital del individuo
- Interés público
- Necesidad contractual
- Cumplimiento de obligaciones legales
- Consentimiento inequívoco del individuo
- Interés legítimo del responsable del tratamiento de datos

Aspectos en los que el RGPD y la LOPDGDD hacen especial hincapié:

1. Documentar e identificar claramente la base legal sobre la que se desarrollan los tratamientos

La **identificación de la base legal** es indispensable para estar en condiciones de demostrar que se cumple con las previsiones del RGPD.

La identificación y documentación debe **adaptarse al tipo de tratamiento y a las características de las organizaciones**.

Requisito:

La base legal del tratamiento debe estar incluida dentro del texto de petición de consentimiento para el tratamiento de los datos.

Recomendación:

Estructurar la petición de consentimiento de manera que se identifique claramente cuál es la base legal del tratamiento.

1. El consentimiento debe ser inequívoco

El consentimiento inequívoco es aquel que se ha prestado mediante una **manifestación del interesado o mediante una clara acción afirmativa**. No se admiten formas de consentimiento tácito o por omisión.

Requisito:

El consentimiento debe ser inequívoco y para un fin concreto.

- ✓ Ejemplo en Anexo II – 2. Comunicaciones y 5. Web.

3. Transparencia e información a los interesados

Toda comunicación que se realice a los interesados, ya sea con respecto a las condiciones del tratamiento de los datos como en respuesta al ejercicio de los derechos que poseen los interesados, se realizará de forma **concisa**, **transparente**, **inteligible** y de **fácil acceso**, con un **lenguaje claro y sencillo**. Asimismo, es obligatorio enviar toda información a los interesados **por escrito**.

Además, toda petición de tratamiento de información que se realice debe aclarar los siguientes puntos:

1. Base jurídica del tratamiento
2. Datos del Delegado de Protección de Datos
3. Elaboración de perfiles

Por otro lado, es recomendable evitar fórmulas especialmente farragosas (especialmente textos legales), y si es necesario proporcionar cláusulas informativas, se debe explicar el contenido al que se refiere de forma clara y sencilla.

Requisito:

Las condiciones del tratamiento se exponen de forma concisa y transparente. Debe incluirse en la petición de consentimiento: 1. La base jurídica del tratamiento, 2. Los datos del delegado de Protección de Datos y 3. La elaboración de perfiles.

Recomendación:

Expresar las condiciones del tratamiento en lenguaje claro y sencillo, evitando cualquier tipo de jerga legal, e incluyendo los contenidos mínimos requeridos por ley.

- ✓ Ejemplo en Anexo II – 2. Comunicaciones y 5. Web.

CÓMO PLASMAC GARANTIZA LOS DERECHOS DE LAS PERSONAS

PLASMAC tiene en cuenta, además los tradicionales **derechos ARCO** (Acceso, Rectificación, Cancelación y Oposición), tres nuevos derechos de los interesados: el **derecho al olvido, derecho a la limitación del tratamiento** y el **derecho a la portabilidad**.

PLASMAC facilitará a los interesados el ejercicio de estos derechos de una for**ma sencilla, fácil y gratuita**.

El responsable debe responder en un plazo inferior a un mes, la petición del interesado para el ejercicio de sus derechos, incluso para comunicar que no se atenderá dicha solicitud, detallando la razón de su negativa.

El responsable debe verificar la identidad de quién solicite el acceso y ejerzan los restantes derechos ARCO.

Recomendación:

Se recomienda la utilización de cuentas usuario para el acceso a los datos de los interesados.

Se recomienda la utilización de métodos de validación y verificación (¿a través de cuentas de correo electrónico?) para la verificación de la identidad del interesado.

- ✓ Ejemplo en Anexo II – 1. Derechos ARCO.

1. **Derecho de acceso**

Requisito: Además de facilitar todos los datos de base del afectado, el interesado tiene derecho a una copia de los datos personales que son objeto de tratamiento.

Recomendación: Facilitar el acceso a un sistema remoto que ofrezca al interesado ejercitar, además de derecho de acceso, su derecho de rectificación, cancelación y oposición.

2. **Derecho al olvido**

En sí mismo no consiste en un derecho nuevo, sino el resultado de los derechos de cancelación y oposición en el entorno online.

3. **Derecho a la limitación del tratamiento**

Este derecho otorga al interesado el poder de limitar los datos a ser utilizados en cualquier tratamiento de datos. El interesado puede ejercer este derecho de forma parcial o total (ejerciendo el derecho de rectificación y/u oposición).

Requisito: Mientras dure la limitación, sólo se podrá tratar los datos afectados, más allá de su conservación, con el consentimiento del interesado.

Recomendación: Recopilar el consentimiento del interesado a través de la plataforma.

- ✓ Ejemplo en Anexo II – 1. Derechos ARCO.

4. **Derecho a la portabilidad**

Este derecho supone una evolución del derecho de acceso, ya que supone que la copia de los datos proporcionados al interesado debe darse en un **formato estructurado**, de **uso común** y **lectura mecánica**. Esto quiere decir, que la copia de los datos debe darse en una forma (contenido y formato) fácilmente reutilizable.

Además, el derecho a la portabilidad permite que los datos personales del interesado se transmitan de un responsable a otro, **sin necesidad de que el interesado haga de intermediario**.

Requisito: Se proporcionará una copia de los datos proporcionados al interesado debe darse en un **formato estructurado**, de **uso común** y **lectura mecánica**.

Recomendación: Se recomienda desarrollar un formulario tipo en el que, automáticamente, se clasifique la información que se posea del interesado para su envío.

- ✓ Ejemplo en Anexo II – 1. Derechos ARCO.

RELACIÓN ENTRE PLASMAC Y LOS PROFESIONALES DEL SERVICIO

La relación entre PLASMAC y los profesionales del tratamiento de los datos puede resumirse en tres puntos: 1. Obligaciones específicas de los encargados, 2. Elección del encargado del tratamiento y 3. Contenido del contrato de encargo.

1. Obligaciones específicas para los profesionales

Mientras que la antiguas, y derogadas, Directiva 95/46 y la LOPD 15/1999 se centraban en la actividad de los responsables del tratamiento (responsabilidades que debe asumir PLASMAC), el nuevo reglamento y ley nacional (RGPD y LOPDGDD) establecen obligaciones expresamente dirigidas a los profesionales del servicio (encargados del tratamiento).

Si bien, cabe destacar, que **la responsabilidad última sobre el tratamiento de los datos se atribuye al responsable, es decir, a PLASMAC.**

Requisitos:

Los profesionales encargados del tratamiento, están obligados a: 1. Mantener un registro de actividades de tratamiento, 2. Determinar las medidas de seguridad aplicables a los tratamientos que se realicen y 3. Designar a un Delegado de Protección de Datos (DPD).

La LOPDGDD, a través de la AEPD, establece unos códigos de conducta que todo profesional encargado de un tratamiento de datos debe acreditar.

Recomendación:

Establecer claramente en el contrato que vincula PLASMAC con el profesional del servicio, las tareas que le corresponden al profesional y las que corresponden a PLASMAC, como responsable del tratamiento.

- ✓ Ejemplo en Anexo II – 6. Contrato PLASMAC – profesional encargado del tratamiento de los datos

2. **Elección del encargado del tratamiento**

A través de la elección del profesional encargado del tratamiento, PLASMAC garantiza y demuestra que el tratamiento se realiza conforme a las leyes vigentes (RGPD y LOPDGDD). De esta forma, PLASMAC cumple con el principio de responsabilidad activa establecido en la reglamentación.

Requisitos:

Recomendación:

PLASMAC debe exigir la presentación/demostración al profesional de estar adherido al código de conducta propuesto en la LOPDGDD y gestionado por la AEPD.

- ✓ Ejemplo en Anexo II – 6. Contrato PLASMAC – profesional encargado del tratamiento de los datos

3. **Contenido del contrato de encargo**

PLASMAC formaliza su relación con el profesional encargado del tratamiento con un contrato vinculante.

Requisitos:

El contrato que vincula a los responsables con los encargados del tratamiento está regulado con contenidos mínimos.

Recomendación:

PLASMAC debe incluir en el contrato, los contenidos mínimos establecidos por el RGPD.

- ✓ Ejemplo en Anexo II – 6. Contrato PLASMAC – profesional encargado del tratamiento de los datos

MEDIDAS DE PLASMAC PARA UNA RESPONSABILIDAD ACTIVA

Tanto el RGPD como la LOPDGDD, establecen un catálogo de medidas que se deben aplicar para garantizar la conformidad de los tratamientos con la legislación vigente y estar en condiciones de demostrarlo. Al conjunto de estas medidas se le llama medidas de responsabilidad activa. PLASMAC implementa las siguientes medidas:

1. **Análisis de riesgo**

La adopción de las medidas está condicionada al riesgo que los tratamientos puedan suponer para los derechos y libertades de los interesados. Es decir, dependiendo del **nivel de riesgo que suponga un tratamiento**, se aplicará una, otra o ninguna medida.

Requisitos:

PLASMAC realizará una valoración del riesgo de los tratamientos que se vayan a realizar. De esta forma, se establecerán las medidas a aplicar y cómo aplicarlas.

Recomendación:

PLASMAC debe llevar a cabo un análisis previo del riesgo de los tratamientos que plantea realizar de los datos.

- ✓ Ejemplo en Anexo II – 3. Tratamiento de datos.

2. Registro de actividades de tratamiento

Desde la entrada en aplicación del RGPD y su trasposición a ley española (LOPDGDD), es obligatorio mantener un registro de operaciones de tratamiento con los contenidos mínimos establecidos en dicha legislación.

Requisitos:

PLASMAC mantendrá un registro de operaciones de tratamiento, cuyo contenido mínimo será el establecido por el RGPD.

Recomendación:

Se sugiere la organización del registro de actividades en torno a operaciones de tratamiento concretas vinculadas a una finalidad básica.

- ✓ Ejemplo en Anexo II – 3. Tratamiento de datos.

3. Protección de Datos desde el Diseño y por Defecto

Este tipo de medidas trata de pensar en términos de protección de datos desde el mismo momento en que se diseña un tratamiento, un producto o servicio que implica el tratamiento de datos personales.

Para ello, es especialmente importante, que **PLASMAC tome medidas organizativas y técnicas antes y durante el desarrollo del tratamiento de los datos**, con el fin de aplicar de forma efectiva el principio de responsabilidad proactiva.

Requisitos:

PLASMAC aplicará, desde el inicio del tratamiento, medidas organizativas y técnicas para integrar en los tratamientos, garantías que permitan proteger los datos desde el diseño.

Recomendación:

La aplicación de medidas durante el diseño del tratamiento de los datos, para que, por defecto, los tratamientos realizados cumplan con la legislación vigente y el principio de responsabilidad activa.

4. Medidas de seguridad

En la legislación anterior, las medidas de seguridad a aplicar estaban determinadas en detalle, por el contrario, la nueva legislación dice que serán los **responsables y encargados los que establezcan las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad** adecuado en función de los riesgos detectados en el análisis previo. También, **se toman en consideración más variables** para la elección de medidas de seguridad con respecto a la legislación anterior.

Requisitos:

PLASMAC debe establecer las medidas técnicas y organizativas apropiadas para garantizar un nivel adecuado en función de los riesgos detectados en el análisis previo de riesgos.

Recomendación:

Las medidas técnicas y organizativas se deben establecer teniendo en cuenta el coste de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento y los riesgos para los derechos y libertades.

5. Notificación de "violaciones de seguridad de los datos"

La legislación actual define las violaciones de seguridad de los datos como *"**todo incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos**"*.

Es de obligatorio, cuando se produzca una violación, que **PLASMAC notifique a la AEPD**, a menos que sea improbable que esa violación suponga un riesgo. Esta notificación debe producirse como máximo 72 horas después de la quiebra.

En los casos en los que la violación **suponga un alto riesgo para los interesados**[2], se ha de notificar además de a la AEPD, a los interesados afectados.

Es de obligación que PLASMAC, como responsable del tratamiento, **documente todas las violaciones de seguridad**.

Requisitos:

Se debe notificar siempre a la AEPD cuando se produzca una violación de seguridad de los datos, a menos que sea improbable que esa violación suponga un riesgo.

Se debe documentar todas las violaciones de seguridad.

Si la violación de seguridad supone un alto riesgo, se ha de notificar a los interesados. Además, dicha notificación debe contener recomendaciones sobre las medidas a tomar por los interesados.

Recomendación:

Producir notificaciones para notificar tanto a la AEPD como a los interesados afectados cuando se produzcan violaciones de seguridad.

Generar un registro de violaciones de seguridad.

- ✓ Ejemplo en Anexo II – 4. Brechas de seguridad.

6. Evaluación de Impacto sobre la Protección de Datos

PLASMAC debe realizar una Evaluación de Impacto sobre la Protección de Datos (EIPD) **antes de la puesta en marcha de los tratamientos** que conlleven un alto riesgo para los interesados. Por ejemplo, el tratamiento a gran escala de datos sensibles (algo que llevará a cabo PLASMAC) es un tratamiento de alto riesgo para los interesados.

La legislación establece los contenidos mínimos de las EIPD, aunque no se establece una metodología específica para su realización.

Es obligatorio que, en caso de no poder mitigar ese alto riesgo, PLASMAC se ponga en contacto con la AEPD.

Recomendable de cara a la realización de la evaluación de impacto sobre la protección de datos, que se revise la guía de ayuda y sus listas sobre tratamientos que (no) conllevan una EIPD.

Requisitos:

[2] El criterio de alto riesgo debe entenderse en el sentido de que sea probable que la violación
de seguridad ocasione daños de entidad a los interesados.

Recomendación:

La AEPD publicó una guía de ayuda sobre las Evaluaciones de Impacto sobre la Protección de los Datos, incluyendo listas sobre qué tratamiento conllevan (o no) una EIPD.

- ✓ Lectura recomendable I – Guía práctica para las EIPD sujetas al RGPD.

7. Delegado de Protección de Datos

Una de las principales medidas impulsadas con la nueva legislación es la creación de un Delegado de Protección de Datos (DPD). Y no es más que la persona encargada en el tratamiento de las obligaciones legales en la materia de protección de datos de la organización.

Por tanto, dados los tratamientos de datos y alcance de los mismos, **PLASMAC está obligado a contar con un DPD entre su personal**.

Requisitos:

PLASMAC nombrará un DPD atendiendo a sus cualificaciones profesionales y, en particular, a su conocimiento de la legislación y la práctica de la protección de datos.

Una vez nombrado el DPD, PLASMAC comunicará a la AEPD la designación del DPD y sus datos de contacto.

Recomendación:

Se recomienda que un DPD tenga conocimientos jurídicos sobre la protección de datos personales, conocimientos sobre tecnología aplicada al tratamiento de datos y en relación con el ámbito de actividad de PLASMAC.

La inscripción del DPD y sus datos de contacto se pueden registrar en la sede electrónica de la AEPD.

PLASMAC Y LOS MENORES DE EDAD

Dado el ámbito de aplicación de PLASMAC, el tratamiento de datos personales de menores de edad es un factor muy relevante a analizar.

Se da por hecho que, la edad de los menores que se verán afectados por el tratamiento de datos realizado por PLASMAC irá desde 0 a 18 años.

Requisitos:

La LOPDGDD establece la edad de 14 años como límite por el cuál un niño puede dar su consentimiento para el tratamiento de sus datos. Para niños menores de 14 años, es obligatorio obtener el consentimiento de la persona con la patria potestad o tutela del menor.

Recomendación:

En caso de menores de 14 años, la legislación vigente no obliga a obtener el consentimiento de padres o tutores del menos, sino a emplear los medios tecnológicos que dispone PLASMAC para establecer la intervención real de los padres o tutores.

- ✓ Ejemplo en Anexo II – 7. Menores.

LISTA DE VERIFICACIÓN:

La AEPD pone a disposición pública en su web un listado de verificación actualizado, con el fin de comprobar su situación con respecto a la aplicación de la legislación vigente.

- ✓ Lectura recomendable II – Guía cumplimiento normativo.

Capítulo 3. Ciberseguridad en PLASMAC

Este capítulo enmarca el concepto de Ciberseguridad para la plataforma en la nube de PLASMAC.

CONCEPTOS FUNDAMENTALES

El carácter cuasi exponencial al que ha avanzado tanto la computación como las redes computacionales desde el inicio de siglo ha difuminado la línea entre lo que consideramos "futurista" y lo que somos capaces de hacer a día de hoy. A medida que progresamos hacia un mundo digital centrado en internet las medidas de seguridad tradicionales van quedando en gran medida obsoletas.

Al igual que la mecánica de Newton es inútil a la hora de debatir sobre física cuántica o la relatividad especial, la humanidad ha tenido que desarrollar un nuevo tipo de seguridad. La ciberseguridad ha nacido para contrarrestar el conjunto de amenazas y acciones criminales que actúan exclusivamente en el espacio cibernético.

La ciberseguridad, seamos o no conscientes, es un elemento esencial de nuestra vida cotidiana. A nivel personal nos protege mientras navegamos por internet, utilizamos la banca online o desperdiciamos innumerables horas en las redes sociales. A nivel empresarial la ciberseguridad engloba todas las medidas que mantienen nuestra red segura de intrusiones y protegida frente a amenazas como el malware. Sin estas medidas de seguridad nuestra empresa sería un "libro abierto" a la vista del público en general, de los competidores o incluso algo peor.

Por otra parte los cibercriminales crecen a un ritmo vertiginoso y tecnologías básicas como "sandboxing" o detección de malware basado en firma autenticada han devenido irrelevantes. Este escenario convierte en urgente estar preparados para la ciberseguridad corporativa.

Respecto al futuro de la ciberseguridad es importante tener en cuenta los efectos de la globalización en el ámbito sociopolítico y socioeconómico de los países desarrollados y en vías de desarrollo en todo el mundo. La facilidad y rapidez de las comunicaciones internacionales y los viajes han hecho del mundo un lugar más pequeño. Efecto que se ve agravado con internet y las tecnologías en la nube.

Una consecuencia de todo esto es que los cibercriminales no se ven constreñidos por limitaciones geográficas ni deben prestar atención a la soberanía de las fronteras políticas.

En 2014, Microsoft llevó a cabo un profundo estudio predictivo sobre cómo sería el ciberespacio y la ciberseguridad en 2025. El informe centró su pronóstico en la macro-economía, los aspectos sociodemográficos y las condiciones tecnológicas y destacó el papel que jugará la política gubernamental en la conformación de futuro del ciberespacio y la ciberseguridad. J. Paul Nicholas, Director Senior de Estrategia de Seguridad Global y Diplomacia de Microsoft, ofreció en el informe esta perspicaz visión sobre el futuro de la ciberseguridad:

“La respuesta de la sociedad a los desafíos de la inmigración, a las necesidades educativas y laborales, al libre mercado así como la cooperación internacional para resolver ciber conflictos conformará el futuro del ciberespacio a lo largo de todas las economías desarrolladas y emergentes. La política, si quiere tener éxito en este campo, debe contemplar una solución equilibrada que favorezca tanto la innovación como el avance de la ciberseguridad”

A tenor de las tendencias de desarrollo en el mundo, la dependencia de internet será una realidad para la mayoría de la humanidad en la próxima década. Por esta razón, así como por las vulnerabilidades derivadas de estar online, el Foro Económico Mundial ha proclamado la ciberseguridad como uno de los mayores problemas que confronta el mundo en la actualidad.

En los últimos años la computación en la nube, un claro ejemplo de esta dependencia de internet, ha impulsado la transformación tecnológica como ninguna otra disrupción tecnológica lo había hecho antes.

Un estudio de la consultora Forrester de 2018 afirma que más del 50% de las empresas globales basarán el impulso de su transformación digital en una plataforma en la nube pública.

Las plataformas en la nube han cambiado por completo la forma en que se consumen tecnologías y se adoptan todo tipo de sistemas. El modelo de distribución de licencias está dando paso a un enfoque más orientado a los servicios.

Esta nueva realidad supone un gran desafío en materia de seguridad. De ahí que el cloud computing y la ciberseguridad encabecen la lista de prioridades de las organizaciones con un alto componente tecnológico.

McAfee en su informe “Construyendo confianza en un cielo nublado” concluye:

- Más del 90% de las organizaciones utilizan servicios en la nube alrededor del mundo.

- La falta de personal especializado en ciberseguridad no ha ralentizado la adopción de servicios en la nube (49% encuestados)

- Los profesionales que confían en nubes públicas superan en proporción de 2 a 1 a aquellos que desconfían.

- 52% de los encuestados aseguran haber rastreado un malware o infección en una aplicación SaaS

El recurso a plataformas en la nube por parte de las organizaciones conlleva un cambio en la forma de entender la seguridad informática. Deja de estar bajo el control de la compañía para estar parcial o totalmente delegada en los proveedores.

La empresa proveedora de cualquier servicio cloud se hará cargo de una parte importante de la seguridad. Garantiza la seguridad física en sus centros de proceso de datos y mantiene los equipos actualizados tanto a nivel de hardware como software para poder hacer frente a las amenazas existentes en internet.

Los principales proveedores de servicios en la nube como Amazon Web Services o Google Cloud, sobre los cuales operan gran parte de los servicios en la nube ofrecidos en el mercado, han abordado de manera proactiva sus controles de seguridad, privacidad y cumplimiento.

La garantía de la integridad de los datos comienza con la certificación del cumplimiento de las normas ISO 27017, 27001 y 27018.

ISO 27001

La norma se orienta a que las organizaciones conozcan los riesgos asociados al manejo de información, asumiéndolos, minimizándolos y gestionándolos por medio de un proceso documentado, sistemático, estructurado, eficiente, repetible y adaptable a los eventuales cambios derivados del entorno, la tecnología y los riesgos.

ISO 27017

La norma pretende ser un estándar de seguridad que proporciona controles tanto para clientes como para proveedores de servicios en la nube. Establece con precisión las relaciones entre clientes y proveedores de servicios en la nube, determinando qué se puede exigir al cliente y qué información debe proporcionarle el proveedor.

Fortalece la ciberseguridad y la gestión del servicio en relación a la arquitectura, medidas de seguridad, funcionalidades disponibles, tecnología de cifrado y localización geográfica de los datos.

ISO 27018

Compendio de buenas prácticas de relacionadas con controles de protección de datos para servicios cloud.

Su objetivo es limitar las normas, procedimientos y controles que los proveedores, en su calidad de “procesadores de datos”, deben aplicar. Así como garantizar el cumplimiento de la normativa legal en cuanto al manejo de datos personales.

PRINCIPALES AMENAZAS Y RIESGOS

La información que recibe, genera o conserva la organización requiere un tratamiento específico durante todo su ciclo de vida. Deben preservarse sus propiedades de autenticidad, fiabilidad y usabilidad y en algunos casos confidencialidad independientemente del dispositivo del que se acceda.

Los proveedores de servicios en la nube se apoyan en la ciberseguridad para garantizar que dicha información permanezca protegida y disponible en cualquier momento.

Las amenazas dependerán del tipo de servicio contratado, forma de contratación y despliegue.

Las principales amenazas son:

- Accesos no autorizados

Proveedor y cliente deben adoptar medidas conjuntas de seguridad adecuadas para evitar robo de datos, inyección de código malicioso, etc...

- Amenazas internas

Adecuado control de permisos y privilegios de acceso para empleados y exempleados.

- Interfaces inseguras

Proporcionar accesos seguros para que no sean explotados por terceros para acceder a información protegida.

- Problemas derivados de uso de las tecnologías compartidas

Controlar posibles fallos de seguridad que permitan a usuarios ajenos a la organización acceder a la información.

- Fuga de información

Cifrar las operaciones de transferencia de datos.

Sistemas de prevención y detección de ataques de ingeniería social o infección con malware para evitar que un delincuente pueda conseguir que algún usuario envíe información confidencial.

- Suplantación de identidad

Medidas de seguridad encaminadas a evitar que ciberdelincuentes por medio de la ingeniería social, fuerza bruta o simple descuido consigan las credenciales de algún usuario y le suplanten a la hora de acceder a la plataforma en la nube.

- Desconocimiento del entorno

El personal a cargo de implantar las políticas de seguridad debe conocer el entorno cloud para evitar configuraciones erróneas e ineficaces.

- Ataques de hacking

Medidas de seguridad dirigidas a evitar que un ciber criminal robe o acceda a la información que maneja alguno de los empleados de la organización o el administrador de la plataforma.

Las amenazas en las circunstancias adecuadas pueden transformarse en incidentes que provoquen daños irreparables en la reputación o perdidas económicas a una organización. Por ello se hace necesario una evaluación de los riesgos que afectan a las características de la plataforma en la nube y adoptar las medidas adecuadas para tratarlos.

- Acceso de usuarios con privilegios

Riesgo de pérdida de confidencialidad, integridad e incluso disponibilidad a causa de: accesos indebidos o acciones maliciosas por parte de un administrador, privilegios otorgados por error a usuarios no autorizados que causen daños no intencionados.

- Incumplimiento normativo

El proveedor de servicios en la nube no cumple o no permite cumplir con las obligaciones legales. Riesgo de sanciones legales.

- Desconocimiento de la localización de los datos

El proveedor aloja los datos en un Centro de Datos del que desconocemos su ubicación. Ponemos en riesgo la seguridad de los datos al desconocer la legislación de otros países.

- Falta de aislamiento de los datos

En aquellos servicios en los que la organización comparte infraestructura en la nube con otras es necesario que el proveedor asegure que los datos de las distintas organizaciones no se mezclen y que cada organización acceda a los suyos.

- Indisponibilidad del servicio en caso de desastre o incidente

Si el proveedor sufre un incidente grave o un desastre debe asegurar un plan de continuidad (por ejemplo datos y servicios replicados en otro centro de datos) para no poner en riesgo la prestación del servicio.

- Carencia de soporte investigativo

En caso de un incidente se hace necesario revisar los accesos a los datos para saber que ha ocurrido. El riesgo de no poder actuar porque el proveedor no nos garantiza el acceso a los logs o registros de actividad.

- Viabilidad a largo plazo

El riesgo de que las condiciones contratadas sufran algún tipo de modificación a causa de: un cambio de estructura del proveedor, de la alta dirección, a la entrada en situación de quiebra o a la externalización de parte de sus servicios. Es indispensable asegurarse el acceso a los datos y a su recuperación.

TECNOLOGÍAS Y TENDENCIAS EN CIBERSEGURIDAD A TENER EN CUENTA EN PLASMAC. LA TECNOLOGÍA CONFORMARÁ EL FUTURO DE LA PLATAFORMA

A la vista del estado actual de la tecnología a nivel global (tendencias y trayectorias) se prevé que serán: el Open Source, el Big Data y el Análisis de Tráfico de Red (ATR) las tecnologías que jueguen un rol vital en el futuro de la ciberseguridad.

Big Data

En las últimas décadas el "Big Data" se ha convertido en una especie de palabra de moda en el mundo de los negocios. En concreto a medida que la memoria y el procesamiento informático permitieron la acumulación de cantidades masivas de datos que superan con creces la capacidad tradicional de procesamiento.

Una de las definiciones más citadas proviene de Wikibon que describe Big Data como "conjuntos de datos cuyo tamaño, tipo y velocidad de creación hace imposible procesarlos y analizarlos con tecnología de base de datos tradicionales y herramientas relacionadas de manera eficaz en tiempo y coste"

Hay una necesaria ambigüedad que es fundamental para el papel que jugara inevitablemente el Big Data no sólo en el futuro de la ciberseguridad sino también en la manera de hacer negocios y la política en su totalidad.

El impulso por mejorar y desarrollar la tecnología ha creado un recurso totalmente nuevo y único para la humanidad: los datos. Como cualquier otro recurso, se puede conseguir tanto en "crudo" como, previa cierta inversión, "procesado" para su aplicación y consumo humano. Incluso hemos adoptado la misma terminología que utilizamos cuando hablamos de recursos naturales: "minería" de datos.

El Big Data así como la tecnología que pueda gestionarlo y procesarlo de manera eficaz es crucial para la ciberseguridad por dos razones esenciales:

La primera aborda la ciberseguridad y las fuentes de datos disponibles a una escala macro global a medida que un número creciente de personas y dispositivos se conectan. No es ningún secreto que compañías como Facebook están continuamente amasando enormes volúmenes de datos de todos sus usuarios.

Cuando el Big Data en cuestión abarca miles de millones de personas en todo el mundo, como ya lo hace, proporciona conocimiento de valor sobre ciberseguridad a escala global.

Con capacidades de procesamiento correctas, las políticas de ciberseguridad a nivel gubernamental o corporativo pueden ser mucho más proactivas y estar mejor enfocadas gracias al conocimiento extraído de los datos.

En las próximas décadas, los datos irán "in crescendo", especialmente en países en desarrollo. India, por ejemplo, prevé que incrementar en un 3000% las suscripciones a

banda ancha de internet. De 20 millones en 2012 a más de 700 millones en 2025. En un mundo cada vez más globalizado este nivel de cambio tan acelerado nos afectará a todos.

El Big Data en este sentido también puede plantear una serie de riesgos de ciberseguridad tanto en la actualidad como en el futuro.

La privacidad es lo primero que tienen en mente los consumidores cuando hay corporaciones de por medio. Si se vulneran las medidas de seguridad o se filtran bancos de datos - datos con potencial de afectar a millones de personas - pueden terminar en manos de ciberdelincuentes.

La filtración de datos de alto perfil del ataque Ashley Madison nos ha mostrado las consecuencias de este tipo de cibercrimen y no es difícil imaginar las consecuencias de una filtración de datos donde haya mucho más en juego.

Organizaciones terroristas podrían usar este tipo de datos para perpetrar ataques en el mundo real, o Estados autoritarios y antidemocráticos podría usarlo para identificar a disidentes políticos ex partidarios. Situaciones ambas con graves consecuencias en la vida real.

La segunda razón de la importancia del Big Data para la ciberseguridad reside en las medidas de seguridad en sí mismas.

La ciberseguridad eficaz, tanto para redes de empresas como gubernamentales, es aquella que necesariamente monitoriza la actividad dentro de esa red para saber cuándo y dónde actuar en el supuesto de que la red sufra un ataque.

Dependiendo del tamaño de la red y el alcance de las medidas de protección implementadas, se puede generar enormes volúmenes de datos imposibles de procesar por la mente humana que permita sacar algo en claro del Big Data.

La tecnología de procesamiento de Big Data es por tanto una parte fundamental para maximizar la eficacia de una infraestructura de ciberseguridad y para comprender el estado general de salud de esa red.

Para cumplir con esta funcionalidad de procesamiento de Big Data la plataforma de análisis en tiempo real y ciberseguridad de redborder utiliza Apache Hadoop (un gran ejemplo de solución para procesamiento distribuido de Big Data totalmente escalable). La escalabilidad es un factor crucial para cualquier solución de procesamiento de Big Data destacable en el panorama de la ciberseguridad del futuro.

Open source / Código abierto

El valor del software Opensource ha sido progresivamente reconocido desde que el término fue acuñado y ampliamente aceptado a principios del 1998 a raíz de la aprobación generalizada de Linux y el lanzamiento público del código fuente del navegador Netscape.

El hecho diferencial de las aplicaciones y el software Open Source es su inconfundible calidad.

Al abordar el desarrollo y mejora del software como una experiencia colaborativa y compartida, el producto final tiene más probabilidades de ser más testeado que cualquier otro software propio. Incrementando su estabilidad y seguridad con respecto a ciberamenazas como el malware así como un menor coste y tiempo de producción.

El hecho de que el Open Source conduzca a software y sistemas más seguros es ya un signo revelador de su papel vital en el futuro de la ciberseguridad.

Hay razones que van más allá de estar mejor preparado para lidiar con amenazas a la ciberseguridad. Tomando en consideración factores geopolíticos que jugarán un factor decisivo en la definición del mundo cibernético del mañana, la tecnología Open Source aborda necesidades específicas a nivel básico y fundamental. El Open Source prospera con el talento, la movilidad y la cooperación, todos ellos componentes esenciales de la socio-economía globalizada de hoy en día.

A nivel macro y micro una cultura de colaboración y corresponsabilidad es vital para que países desarrollados y en desarrollo prosperen. Esto se evidencia en el desigual número de graduados en Ciencias, Tecnologías, Ingeniería y Matemáticas (STEM) previstos en países en desarrollo comparado con los países desarrollados.

Esta situación es descrita en el estudio Cyber 2025 de Microsoft:

“En el 2025 las economías emergentes producirán casi 16 millones anuales de graduados en Ciencias, Tecnologías, Ingeniería y Matemáticas (STEM) lo que supondrá 5 veces más que los 3.3 millones anuales en países desarrollados”

Esto traerá consigo numerosas implicaciones. Para empezar, los países desarrollados tendrán que confiar en la inmigración y la movilidad internacional del talento para mantener un entorno tecnológico competitivo a largo plazo. Sobre todo si tenemos en cuenta el rápido envejecimiento de la población que pronto quedará fuera del mercado laboral.

Otra circunstancia que afectará al futuro de la ciberseguridad es el incremento exponencial del número de personas formadas en informática con dificultades para encontrar un trabajo adecuado en sus países de origen. Esta situación crea un entorno ideal para el cibercrimen oportunista enfocado a la riqueza de los países desarrollados especialmente si los ciberdelincuentes trabajan desde un país cuya política gubernamental no aborda de manera eficaz la problemática de la ciberseguridad.

La tecnología Open Source no es de ningún modo una cura milagrosa a este tipo de cibercrimen pero ofrece la oportunidad de que gente de todo el mundo colabore y comparta su pericia con un objetivo común. Para ser lo más eficaz posible, la ciberseguridad del futuro tendrá que operar con la misma ética y espíritu colaborativo que hay detrás de la tecnología Open Source (razón de su eficacia a escala global).

En el contexto de la ciberseguridad de una red de empresa u organización, la tecnología Open Source da acceso a conocimiento colectivo esencial para identificar amenazas, facilitar análisis anticipados y compartir conocimiento. Así mismo permite que la seguridad sea escalable y resiliente

Análisis de tráfico de red

El Análisis de Tráfico de Red (ATR) también juega un papel relevante en el futuro de la ciberseguridad pero en una escala mucho más localizada y discreta que el Big Data y el Open Source.

En cierto sentido el Análisis de Tráfico de Red usa lo mejor de las dos tecnologías previamente mencionadas para proporcionar conocimiento y un alto nivel de seguridad a la red. El Análisis de Tráfico de Red es un elemento esencial de la ciberseguridad independientemente de si se administra una red corporativa de bajo nivel o una a gran escala en un entorno gubernamental.

Conocer lo que sucede dentro de una red y las potenciales amenazas que confronta es el primer paso hacia medidas de seguridad de red proactivas y efectivas

Quizás la razón de más peso para que el Análisis de Tráfico de Red juegue un papel tan importante en el futuro de la ciberseguridad es el incremento exponencial del uso masivo de dispositivos móviles en el mundo. Esta tendencia ya ha afectado a las redes corporativas en muchos países desarrollados con la implementación de políticas BYOD ("trae tu propio dispositivo") y el aumento en el número de puntos finales con potencial para introducir malware o actuar como punto de entrada para los hackers.

El Análisis de Tráfico de Red proporciona a los administradores de red la visibilidad y el conocimiento para evaluar eficazmente el riesgo y adoptar medidas adecuadas.

En el futuro, la ciberseguridad, estará en gran medida centrada en el riesgo que plantea la afluencia masiva de posibles puntos de entrada de malware derivado del uso masivo de smartphones en los países desarrollados. Así como la tendencia global hacia la adopción del internet de las cosas (IoT) donde numerosos objetos de nuestra vida cotidiana estarán conectados a internet y se comunicarán entre ellos.

La comodidad que ofrece el IoT es innegable. También es inevitable a la vista de que la mayor parte de la población en los países desarrollados estará compuesta de frágiles ancianos. Una demografía que se beneficiará de una mayor conectividad y comodidad.

Con el aumento de la comodidad se incrementa el riesgo, y las consecuencias del cibercrimen en una sociedad saturada de tecnología IoT podrían ser terribles. Por ejemplo actualmente ya es posible hackear y apagar un jeep de manera remota mientras hay personas a bordo. No es muy difícil imaginar un futuro cercano donde haya personas haciendo lo mismo con aviones, vehículos militares o incluso equipo médico.

Al proporcionar herramientas para mantener tu red segura, el Análisis de Tráfico de Red te permite detectar cualquier cambio sospechoso e identificar malware antes de que plantee una amenaza sustancial. Además el análisis de tráfico te permite crear listas

negras, archivos “hashes” y registrar cualquier cambio en los registros de ataques. En el futuro de la ciberseguridad, la visibilidad y el control del Análisis de Tráfico de Red será crucial para garantizar la seguridad y estabilidad de redes de todos los tamaños.

Conclusión

El impulso hacia una conectividad móvil generalizada aumentará la demanda mundial de funcionalidades en la nube confiables y seguras tanto en el ámbito privado como en el público.

La tecnología que lo permite va a desempeñar un papel vital en el desarrollo futuro de la ciberseguridad y aplicaciones tecnológicas más amplias. Como decíamos hay buenas razones para creer que la tecnología Big Data y Open Source junto con el Análisis de Tráfico de Red son parte integral de esta. Concretamente el análisis estadístico de datos es la clave para la gestión segura de la nube.

Esto es aplicable a redes de todos los niveles desde una corporativa a la red de un proveedor de telefonía móvil o una red gubernamental, pasando por una plataforma como Plasmac.

CIBERSEGURIDAD EN PLASMAC

La plataforma PLASMAC, como repositorio común de datos sensibles en materia de servicios sociales, debe trasladar a su servicio en la nube la misma seguridad que exigiría a sus instalaciones en local.

Los puntos críticos desde el punto de vista de la seguridad giran en torno a la gestión y acceso a datos sensibles de ciudadanos de las Islas Canarias y a la futura Historia Social Única. Tomando en consideración esta realidad podemos identificar una serie de riesgos:

- Gestión y configuración de accesos con especial atención a los usuarios con privilegios especiales.
- Cumplimiento normativo tanto a nivel interno de la organización como por parte del proveedor de servicios en la nube.
- Ubicación de los datos del que depende el marco regulatorio aplicable al almacenamiento y procesado de datos sensibles.
- Aislamiento de datos en particular de intervenciones sociales ya finalizadas.
- Recuperación, soporte investigativo y viabilidad a largo plazo aspectos cruciales de los que depende que la plataforma y la historia social única tenga viabilidad en el largo plazo.

RIESGO	MITIGACIÓN	ACCIONES
Acceso de **usuarios** con **privilegios**	Consensuar/**Asegurar con** el **proveedor cloud** para que los **usuarios con privilegios** sean **sólo los que deben tenerlos**.	Decidir qué **privilegios de acceso** habrá **en función de la información a acceder**
Cumplimiento normativo	Realizar **auditorías externas** y **certificaciones de seguridad**	**Supervisar** que se **cumpla dentro de la organización** (RGPD) **Asegurar auditorías** realizadas **correctamente**.
Localización de los datos	**Conocer marco regulatorio aplicable** al almacenamiento y procesado de **datos sensibles**. **Proveedor cloud adaptado** al **marco legal del país suscriptor del servicio**	**Conocer** la **localización** de los **datos** para saber la **legislación aplicable**.

Aislamiento de datos	**Datos en reposo aislados** Procedimientos de **cifrado ejecutado por personal experto**	**Adoptar** las **medidas de protección necesarias** (**cifrado de datos**) para la **información más sensible**.
Recuperación	**Exigir** al proveedor **capacidad de recuperación de datos** y **tiempo estimado**.	
Soporte investigativo	**Garantía** del proveedor de que **logs y datos se gestionan de forma centralizada**.	**Replicar** los **datos en otra plataforma** (servidores o equipos propios) **Negociar** estas **condiciones** en el **acuerdo con el proveedor**
Viabilidad a largo plazo	**Asegurar** que va a poder **recuperar todos los datos** si el proveedor cambia la estructura o la dirección.	

RECOMENDACIONES DE CIBERSEGURIDAD PARA PLASMAC

A continuación, una vez identificadas cuáles son los riesgos y puntos críticos que deberían tenerse en cuenta en PLASMAC, se van a introducir algunas recomendaciones más específicas que el desarrollador de la plataforma PLASMAC debe contemplar/responder antes de abrir el uso de la plataforma a los usuarios. A modo de hipótesis de partida, suponemos que PLASMAC se localiza en un proveedor externo al que debemos exigir unos criterios de ciberseguridad.

Para la identificación y desarrollo de estas recomendaciones nos hemos basado en los estándares y modelos aplicables del Instituto Nacional de Ciberseguridad (INCIBE) y de la Agencia Europea de Ciberseguridad (ENISA – EU Agency for Cybersecurity).

Recomendación 1: Identificar los datos y las operaciones de PLASMAC que estarán definitivamente en la nube

Como está previsto que PLASMAC sea una plataforma que opere totalmente o en gran parte en la nube, antes de planear el uso de ciberseguridad para PLASMAC, se deben identificar claramente qué datos, operaciones de procesamiento o servicios estarán precisamente alojados en la nube.

Para cada tipo de procesamiento se debe establecer qué tipos de datos hay, distinguiendo entre:

- Información personal.
- Datos sensibles.
- Datos estratégicos para PLASMAC.
- Datos utilizados en otras aplicaciones.

Hay que asegurarse de que las operaciones de procesamiento transferidas a la nube no es probable que incluyan datos de otras operaciones de procesamiento que no se hayan migrado. Por otra parte, ciertos datos están sujetos a regulaciones específicas, y por lo tanto es necesario comprobar si los datos que pueden transferirse a la nube están sujetos a tales obligaciones y, en su caso, identificar las mínimas condiciones para su traslado. En este sentido en apartados específicos de este documento tratamos aspectos con la protección de datos o la seguridad entre otros.

Todos estos aspectos deberán quedar definidos en el DMP-Data Management Plan, Plan de Gestión de Datos.

Recomendación 2: Definir los requisitos específicos de seguridad técnica y jurídica de PLASMAC utilizando los requisitos y recomendaciones proporcionados en los capítulos anteriores del estudio

En los capítulos anteriores del estudio se aportan una serie de requisitos técnicos y jurídicos que PLASMAC debe tener en cuenta. En cualquier caso, para garantizar la ciberseguridad de PLASMAC se debe considerar cuales son exactamente los requisitos específicos definitivos que el desarrollador va a implementar/tener en cuenta. De esta forma, y como muchas ofertas son "estándar" para todos los clientes y no cumplen con

una especificación en particular, consideramos clave solicitar una respuesta personalizada a las especificaciones definitivas definidas en PLASMAC.

Los requisitos deben incluir todos los puntos importantes para PLASMAC, en particular:

- Restricciones legales (ubicación de los datos, garantía de seguridad y confidencialidad, regulaciones específicas para ciertos tipos de datos, etc.);
- Restricciones prácticas (disponibilidad, reversibilidad / portabilidad, etc.);
- Limitaciones técnicas (interoperabilidad con los sistemas existentes en el ayuntamiento, etc.).

Recomendación 3: Realizar un análisis de riesgos para identificar las medidas de seguridad esenciales para PLASMAC basándonos en el apartado anterior de ciberseguridad en PLASMAC

Es muy importante realizar un análisis de riesgo completo para que PLASMAC pueda definir las medidas de seguridad adecuadas que se deben exigir al proveedor del servicio o que se implementen dentro de la organización (en el caso de no externalizar el servicio en la nube). Si no se realiza un análisis completo y exhaustivo al menos deben tenerse en cuenta de forma genérica los siguientes riesgos identificados:

- Dependencia tecnológica del proveedor, es decir, la imposibilidad de cambiar de solución (para otro proveedor o una solución interna) sin pérdida de datos. O en el caso concreto de PLASMAC la posibilidad real de escalarse hacia arriba, es decir, el poder integrarse más adelante con una plataforma única gestionada por el Gobierno de Canarias que integre todas las plataformas/datos de ayuntamientos como es el caso de PLASMAC.
- Defectos en el aislamiento de los datos, es decir, el riesgo de que los datos alojados en un sistema virtualizado se modifiquen o se hagan accesibles a terceros no autorizados, por parte de un fallo del proveedor del servicio o de una mala gestión de la función supervisora.
- Defectos en la cadena de subcontratación, si el propio proveedor de servicios ha utilizado a terceros para proporcionar el servicio;
- Destrucción ineficaz o no segura de datos, o período de retención excesivo;
- Problema de la gestión de los derechos de acceso para los interesados debido a la insuficiencia de los medios establecidos por el proveedor del servicio;
- Indisponibilidad del servicio, que incluye la indisponibilidad del servicio en sí, pero también la indisponibilidad de los medios de acceso al servicio (en particular los problemas de red);
- Cierre de servicio o toma de control del proveedor de servicios por un tercero; o Incumplimiento de la normativa, en particular sobre las transferencias internacionales.

Estos son los riesgos genéricos que debemos tener en cuenta en PLASMAC. Si solo una parte de los datos y el procesamiento se transfieren a la nube, PLASMAC debe considerar el impacto de la migración parcial en el procesamiento y los datos que no se transfieren; es decir, si los datos confidenciales o estratégicos se excluyen explícitamente de la

transferencia a la nube, las operaciones de procesamiento que requieren el envío de dichos datos por correo electrónico deben adaptarse.

La mayoría de estos riesgos pueden reducirse mediante disposiciones contractuales, y medidas técnicas y organizativas para PLASMAC y el proveedor del servicio.

Recomendación 4: Identificar el tipo de servicio en la nube que se utilizará en PLASMAC

Las ofertas de servicios de computación en la nube pueden distinguirse según tres modelos de servicio:

Los modelos de servicio son los siguientes:

- SaaS: "Software como servicio", es decir, aprovisionamiento de software en línea;
- PaaS: "Plataforma como servicio", es decir, aprovisionamiento de plataforma de desarrollo de aplicaciones en línea;
- IaaS: "Infraestructura como servicio", es decir, computación en línea y aprovisionamiento de infraestructura de almacenamiento.

Como cada oferta de ciberseguridad en la nube es específica, deben compararse identificando las fortalezas y debilidades de cada una en términos del tipo de procesamiento considerado. Un análisis de este tipo permitirá seleccionar la oferta de más adecuada.

En principio, por la casuística de PLASMAC, parece que el modelo adecuado puede ser el de SaaS, a falta del análisis definitivo del desarrollador de la solución/plataforma final.

Recomendación 5: Elegir para PLASMAC un proveedor de servicios que ofrezca garantías suficientes

Es una recomendación bastante obvia pero que consideramos que se debe mencionar explícitamente. En este sentido, PLASMAC como cliente de los servicios de ciberseguridad en la nube, debe asegurarse de poder cumplir con sus obligaciones frente a los usuarios de la plataforma de Servicios Sociales (usuarios, profesionales, técnicos de la administración) y para ello, se deben elegir proveedores de servicios que garanticen la configuración de las medidas adecuadas de seguridad y confidencialidad, y que sean transparentes respecto a los medios utilizados para prestar sus servicios (transferencia de datos al extranjero, uso de subcontratistas, política de seguridad y medidas).

Recomendación 6: Revisar la política de seguridad interna del Ayuntamiento

PLASMAC no es solo la plataforma en la nube de forma independiente ya que quizás de alguna forma se integrará/interaccionará con técnicos, operaciones o servicios del propio ayuntamiento. La ciberseguridad en la nube de PLASMAC requiere una revisión completa de los procedimientos internos en línea con las conclusiones del análisis de riesgos propuesto anteriormente. De hecho, el uso de la nube introduce nuevos riesgos relacionados, en particular, con las transmisiones a través de Internet o el uso de terminales móviles. Se debe prestar especial atención a los mecanismos de autenticación

de los técnicos del ayuntamiento y el proveedor de servicios en la nube debe ofrecer un servicio compatible con estos requisitos de seguridad.

Recomendación 7: Posibilidad de evaluar y controlar los cambios de PLASMAC o que afecten a PLASMAC

En un espíritu de mejora continua de PLASMAC, y sobre todo también pensando en su escalabilidad hacia arriba, se recomienda que el servicio en la nube de PLASMAC se evalúe periódicamente en el contexto, los riesgos, las soluciones disponibles en el mercado, la legislación, etc. Particularmente, un análisis de riesgo óptimo debe actualizarse tan pronto como se produzca un cambio significativo en el servicio para adaptar las medidas o soluciones tan pronto como sea necesario.

Estos cambios pueden referirse a las funcionalidades de PLASMAC o la provisión técnica del servicio (nuevo centro de datos, cambio en la política de seguridad, cambio en el procesamiento iniciado por el ayuntamiento, integración de PLASMAC hacia arriba, etc.).

Capítulo 4. Desarrollo de la plataforma PLASMAC

Este último capítulo identifica y elabora el proceso de desarrollo que debería cumplir una plataforma en la nube como PLASMAC, y sobre todo cómo puede la entidad responsable de la plataforma controlar todo el proceso de desarrollo.

METODOLOGIA APLICADA AL DESARROLLO DEL PROYECTO

El desarrollo del proyecto se hará siguiendo un ciclo de vida iterativo, con entregas periódicas de programas y refinamiento progresivo de funcionalidades. Se tendrán en consideración las siguientes directrices:

- Se fijarán unos criterios mínimos de calidad que tiene que satisfacer el código desarrollado, basados en conceptos como cobertura de código, complejidad ciclomática, código duplicado y estándares de codificación.
- El código desarrollado se mantendrá versionado y deberá incluir los test (unitarios, de integración y de pantallas). Después de cada entrega periódica debería ser posible integrar el código desarrollado en el repositorio y estar disponible en un entorno de preproducción.
- Los despliegues de código se harán respetando la política que se aplica a los diferentes entornos de preproducción y producción.
- El despliegue de los componentes de la nueva plataforma se hará de manera que se garantice que las posteriores actualizaciones puedan ser instaladas por el personal TI sin necesidad de nuevos desarrollos, con la mayor simplicidad posible y siguiendo la documentación proporcionada.

El proceso de desarrollo se divide en tres hitos, que se realizaran en cada iteración, como son:

1. **Especificación del producto**

   El proveedor entregará un documento de especificación del producto que cumpla con los requisitos definidos. En este documento se definirá su propuesta para la solución. Contendrá la definición de los diferentes módulos que integrara la plataforma para dar solución a los requisitos que el cliente pidió. También se definirá el diseño de la plataforma, desde el lenguaje de programación o las plantillas de diseño, hasta accesibilidad (en que dispositivos estará y como, con una app o desde el navegador) o seguridad (se puede acceder desde cualquier país, qué medidas se imponen en el acceso).

   El cliente revisará este documento y concluirá si se deben o no incluir otros módulos para completar la solución y dar cabida a todo lo que se le va a pedir a la plataforma y también que cumple con todos los requerimientos.
   Este punto concluye con un documento acordado entre cliente y proveedor en el que se define la solución y los módulos que esta contendrá.

2. **Diseño de la solución**

En base a lo acordado, el cliente habrá diseñado un código y se entregará junto con la documentación de este. En este punto también se entregará el diseño de las pruebas unitarias y el documento funcional.

La documentación del código debe ser completa y clara, como para que otro desarrollador pueda usarla en el futuro.

Las pruebas unitarias deberán cubrir todo el código y las especificaciones acordadas y deben entregarse con un documento de verificación que demuestre que todas las pruebas han sido pasadas con resultado positivo. En caso de que alguna prueba no esté pasada o tenga un resultado negativo, esto deberá estar justificado.

El documento funcional incluirá la definición de todos los módulos que componen la plataforma y como estos deben funcionar.

3. **Implementación de la solución**

Según lo acordado en puntos anteriores, en este hito el proveedor entregará el producto final, que deberá cumplir con lo especificado. Es decir, el código desarrollado y probado estará desplegado en la plataforma de pruebas y accesible.

El producto se entregará junto con el manual de usuario, que contendrá una descripción completa del producto final y en el que se especificará como acceder y realizar todas las acciones que el producto ofrece. Este manual debe ser completo y manejable para un usuario final.

En este punto se habrán realizado tanto las pruebas funcionales como las de carga, y se entregara el diseño de estas y el documento de validación en el que se demuestre que todas las pruebas han sido pasadas con resultado positivo. En caso de que alguna prueba no esté pasada o tenga un resultado negativo, esto deberá estar justificado.

En el caso de las pruebas funcionales, estas tendrán que cubrir todas las funcionalidades del producto.

En el caso de las pruebas de carga, estas tendrán que cubrir los SLA acordados.

En cada hito, por tanto, se han definido las siguientes entregas por parte del proveedor, junto con los términos que el cliente deberá revisar en cada caso para conseguir los objetivos fijados:

Hito	Entregas proveedor	Acciones cliente
1	Documento de especificación del producto	Las especificaciones cumplen con los requerimientos del cliente
2	Código, documentado	El código cubre las especificaciones y está bien documentado
	Diseño y resultado de pruebas unitarias	Cubren todas las especificaciones y están bien documentadas
	Documento funcional	Contiene el diseño de la plataforma y sus módulos
3	Producto final (Plataforma web, App...): Código desplegado	El producto cumple con lo especificado
	Manual de usuario	Contiene una descripción completa del producto final, con explicaciones sobre cómo acceder y realizar todas las acciones que este ofrece. Debe ser completo y manejable.
	Diseño y resultados de pruebas funcionales	Cubren todas las funcionalidades y están bien documentadas
	Diseño y resultados de pruebas de carga	Cubren los SLA y momentos pico concretos

ESPECIFICACIÓN DEL PRODUCTO

En una primera aproximación, se considera que la solución deberá cumplir con al menos los requisitos que se exponen a continuación:

Requisitos comunes para los diferentes componentes de la plataforma	
COM-1	Todo componente de la plataforma debe ofrecer un conjunto normalizado de entidades de negocio (objetos de datos, data transfer objects).
COM-2	Todo componente de la plataforma debe ofrecer una interfaz de servicios normalizados (casos de uso, API). Su especificación sólo podrá utilizar entidades de negocio normalizadas.
COM-3	Todo componente de la plataforma debe ofrecer una implementación de los servicios normalizados que se comuniquen con el producto concreto propuesto por el licitador.
COM-4	Todo componente de la plataforma debe comunicarse a través de la capa de integración. Así se podrá tener el control sobre las interacciones que se

	dan entre los componentes y se podrán monitorizar las comunicaciones entre ellos.
COM-5	Todo componente de la plataforma debe ofrecer un cliente que implemente la misma interfaz de servicios normalizados pero limitándose a hacer la comunicación con la capa de integración (ESB, Enterprise Service Bus) para desencadenar la ejecución del servicio. Este cliente permitirá facilitar las integraciones entre componentes. Deben ser fácilmente configurables (timeout de conexión, comportamiento de redirects, etc.).
COM-6	Todo componente de la plataforma debe contar con un sistema que permita establecer la trazabilidad de los errores o incidencias detectadas. Es necesario registrar, de manera centralizada, información de las acciones que llevan a cabo los usuarios para poder hacer el seguimiento y detectar problemas de seguridad o de funcionamiento. Debe ser granular y configurable.
COM-7	Todo componente de la plataforma establecerá los permisos de acceso a la información que gestiona y a las funcionalidades que ofrece, en función de los perfiles y roles del usuario conectado. Como mínimo se diferenciará entre consulta, edición y administración.
Requisitos de las interfaces de acceso de los productos concretos	
INT-1	Todo producto concreto incorporado en la plataforma ofrecerá acceso directo a través de aplicación web. No será la vía de acceso habitual, pero en caso de ser necesario (emergencia, problema de disponibilidad de la plataforma, etc.) los usuarios tienen que poder acceder directamente a los servicios del componente.
INT-2	Todo producto concreto incorporado en la plataforma ofrecerá acceso directo mediante servicios web (SOAP o preferiblemente REST). No será la vía de integración por defecto, ya que se quiere prescindir de integraciones directas punto a punto entre componentes si no que éstas se hagan mediante la capa de integración, pero se dispondrá de esta opción.
INT-3	Todo producto concreto incorporado en la plataforma ofrecerá acceso a los servicios normalizados a través del paso de mensajes. La capa de integración hará uso de esta vía de acceso.
INT-4	Todo producto concreto incorporado en la plataforma ofrecerá un cliente con la implementación de los servicios normalizados que deposite mensajes en una cola concreta de la capa de integración, utilizando únicamente entidades de negocio normalizadas. Este cliente se utilizará por el resto de componentes para interactuar.

DISEÑO DE LA SOLUCIÓN

Se establecen unos principios generales de diseño para la concepción de la nueva plataforma, de cara a su mantenibilidad y evolución futura. A continuación se indican las directrices que condicionarán las acciones a realizar en el desarrollo y la implantación de la nueva plataforma de tramitación y que se tendrán en cuenta por parte de la empresa desarrolladora del piloto (adjudicataria si fuera una fase posterior de desarrollo completo):

1. Interoperabilidad e integración con los diferentes sistemas y aplicaciones del ayuntamiento en principio o de terceros que este utiliza, y más adelante con las soluciones que proponga el Gobierno de Canarias (quizás una plataforma única gestionada por el Gobierno de Canarias que integre todas las plataformas/datos de ayuntamientos como es el caso de PLASMAC).
2. Modularidad y reutilización, tratando los componentes y desarrollos como elementos reusables y autónomos de forma que se facilite su posterior mantenimiento y evolución y, si fuese necesario, que unos componentes puedan ser reemplazados por otros con el mínimo impacto y sin afectar al funcionamiento de la plataforma. El objetivo de esta arquitectura es minimizar los recursos necesarios para crear y mantener el sistema requerido.
3. Diseño de la plataforma que garantice la alta disponibilidad del servicio.
4. Auditoría y trazabilidad, registrando a este efecto las acciones realizadas por los usuarios de la plataforma (usuarios finales, técnicos en informática y las acciones procedentes de la integración con otras aplicaciones). De esta manera y en caso necesario, se tendrá que poder seguir estas acciones y operaciones, permitiendo conocer la situación y traza de cualquier operación o tramitación, así como los estados por los que ha pasado. Para cada acceso se registrará como mínimo:
    a. Identificación unívoca del usuario que accede.
    b. Fecha y hora exacta en la que se ha realizado el acceso.
    c. Tipo de acceso.
    d. Acceso autorizado o denegado.
    e. Datos o información que identifique los registros accedidos por el usuario.
    f. Información de contexto que permita correlacionar con operaciones anteriores o posteriores.

Las interfaces de usuario de los componentes de la plataforma deben satisfacer los requisitos siguientes:

Requisitos de las interfaces de usuario	
GUI-1	El producto final resultante se tendrá que poder ejecutar en las versiones más recientes de los navegadores más habituales. (Safari, Firefox, Chrome, Edge y Explorer).
GUI-2	La solución final tiene que ser totalmente adaptable, responsive, o al menos serlo en los principales módulos de cara al usuario final y en este sentido, funcionar correctamente en los dispositivos móviles (tabletas y smartphones, Android e iOS). Para ello, el producto deberá disponer de los mecanismos para presentar los formularios en dispositivos móviles sin que ello suponga trabajo adicional de desarrollo.
GUI-3	Todo componente de la plataforma debe seguir los estándares marcados por el W3C. En concreto:

	- HTML5 y XHTML válidos. Se realizarán comprobaciones contra un estándar formal como los publicados por la W3C (http://validator.w3.org). - CSS3 válidas. Las hojas de estilos seguirán los estándares marcados por el W3C. Se realizarán comprobaciones contra un estándar formal, como los publicados por el W3C (http://jigsaw.w3.org/css-validator/). - Accesibilidad. Se comprobará que las interfaces web cumplan las directrices de accesibilidad con un nivel mínimo AA según las WCAG 2.1.

IMPLEMENTACIÓN DE LA SOLUCIÓN

Control de calidad del producto

Se tiene que respetar la calidad del software requerido en cuanto a la seguridad de aplicaciones (desarrollo de código seguro). Los componentes de la plataforma tienen que seguir las recomendaciones de desarrollo seguro como son OWASP o ISSAF, para los lenguajes de programación y tecnologías utilizadas, asegurando como mínimo los siguientes requisitos de seguridad:

- Validación de parámetros de entrada y salida.
- Gestión correcta de errores y excepciones.
- Cifrado de información sensible y de comunicaciones utilizadas con otros componentes.
- Gestión correcta de sesiones.
- Métodos de autenticación y autorización robustos que impidan el escalado de privilegios, tanto en horizontal como en vertical.
- Evitar el abuso de funcionalidades o evasión de los procesos establecidos por la lógica original de la aplicación.

También se tienen que aplicar, para cada componente de la plataforma, los mecanismos adecuados que contribuyan a documentar el código y simplificar el diseño. Son ejemplos de esto los test unitarios sobre una implementación mock de los servicios normalizados o contra un producto concreto.

Habrá que definir quién será el encargado de supervisar el trabajo de la empresa desarrolladora y que tendrá potestad para determinar si se satisfacen los requisitos, teniendo como referencia las indicaciones de este documento, los acuerdos adoptados durante el desarrollo del proyecto y el propio criterio técnico del departamento.

El desarrollador/adjudicatario (dependiendo de que sea fase piloto o desarrollo completo) se compromete a aplicar las mejores prácticas para la entrega de todas y cada una de las fases del producto: validación funcional y técnica del producto, gestión del cambio y aplicación de pruebas de carga y estrés. Todos los procedimientos y trabajos incluidos en el alcance del proyecto deberán estar suficientemente revisados en los

términos anteriores por la empresa desarrolladora, hasta asegurar su correcto funcionamiento antes de la entrega.

Los controles de calidad se aplicarán sobre:

- Documentación: Revisiones de estructura, formato y contenido
- Software
    - Evaluaciones de funcionalidad. Incluye los componentes de la plataforma y la implementación de procedimientos.
    - Evaluaciones de eficiencia y de rendimiento.
    - Evaluaciones de uniformidad y usabilidad sobre las interfaces gráficas.
    - Evaluaciones de calidad del código fuente: diseño, mantenibilidad y legibilidad entre otros.
    - Evaluaciones de seguridad.
    - Evaluaciones de documentación del código fuente y software de terceros utilizado.

Rendimiento del producto

Se establece como rendimiento aceptable aquel que permite el acceso y uso simultáneo de la aplicación a los usuarios, con unos tiempos de respuesta considerados aceptables en aplicaciones similares y en entornos de explotación homólogos, suponiendo el cumplimiento de los requisitos técnicos de explotación mínimos establecidos.

Se acordarán unos parámetros para medir el rendimiento, que serán válidos en el momento de la instalación inicial del nuevo sistema y serán verificados en sucesivas actualizaciones.

Se deberá informar de los mecanismos de supervisión y métricas que utilizaran para garantizar el rendimiento y la escalabilidad de la nueva plataforma.

Los siguientes requisitos se aplicarán a cada componente de la plataforma y a la plataforma en general como ente común:

Requisitos de rendimiento	
REN-1	Todo componente de la plataforma tiene que garantizar un tiempo de carga adecuado. Por defecto, la páginas garantizaran un tiempo de carga nunca superior a 3 segundos. Para los casos debidamente justificados por las numerosas interacciones internas entre componentes, el tiempo de carga nunca superará los 10 segundos.
REN-2	Desde el punto de vista de concurrencia, se garantizará un tiempo de respuesta correcto para la plataforma, considerando un contexto en el que las peticiones de servicio simultáneas activas oscilan desde una media de 10 hasta un máximo puntual aproximado de 25.

REN-3	El sistema contemplará las medidas necesarias para garantizar el correcto funcionamiento sobre una configuración en alta disponibilidad.

Transferencia de conocimiento

Todos los componentes desarrollados, mejorados o modificados durante la ejecución del contrato deberán estar a disposición del ayuntamiento (receptor de la solución), quien los podrá modificar o evolucionar en el futuro. Se pondrá también a su disposición el entorno de librerías necesario para permitir la ampliación y actualización de éstas por el personal TI.

En este sentido, durante toda la vigencia del contrato y según la planificación establecida en la oferta, la empresa desarrolladora deberá, de manera continua, transferir el conocimiento al personal TI del ayuntamiento/receptor de la solución para que adquiera la cualificación necesaria para explotar, mantener y evolucionar la plataforma.

Anexo I. Carta de derechos y obligaciones

En el presente anexo se describen los derechos y deberes de las personas usuarias de los servicios sociales, según viene recogido en la nueva ley de Servicios Sociales de Canarias. En dicha ley se solicitaba la máxima difusión de su contenido en todo el ámbito del sistema de servicios sociales de responsabilidad pública y privada. Por estos motivos, se recomienda su inclusión en PLASMAC, pues además, constituye uno de los derechos de por sí: en recibir información sobre sus derechos y deberes.

En este anexo se describen los derechos y obligaciones de las personas usuarias en general, de las personas usuarias de los centros y servicios de atención diurna / nocturna y estancia residencial, y de los profesionales de referencia que trabajan en el Sistema Público y, por ende con PLASMAC.

Derechos de las personas usuarias del sistema público de servicios sociales.

Las personas usuarias del Sistema Público de Servicios Sociales, tendrán garantizado el ejercicio de los siguientes derechos:

a) A acceder a los servicios sociales en condiciones de igualdad, dignidad y privacidad.

b) Al acceso y seguimiento, vía telemática, de su expediente.

c) A recibir información profesional, suficiente, veraz y fácilmente comprensible, y si lo requiere por escrito, sobre:

- Los servicios y prestaciones disponibles y los requisitos necesarios para acceder a los mismos.
- Los derechos y deberes de las personas usuarias.
- Los mecanismos de presentación de quejas y reclamaciones.

d) A disponer de un plan de intervención social personalizado elaborado con su participación y autorización, o de las personas responsables de su entorno familiar o social que les representen, que sea revisable en función de las circunstancias y resultados.

e) A conocer la valoración y diagnóstico técnico y a un itinerario individualizado de su situación y del tipo de intervención que se le asigne y a, dentro de los plazos que reglamentariamente se determinen, disponer de la misma en un lenguaje claro y comprensible.

f) A tener asignada una persona titulada en trabajo social como profesional de referencia, preferentemente integrada en un equipo interdisciplinar de profesionales de los servicios sociales, que procure la coherencia, el carácter integral y la continuidad del proceso de intervención.

g) A la libre elección del profesional de referencia y a un segundo diagnóstico de su situación Dentro de los condicionantes y límites establecidos reglamentariamente.

h) A escoger libremente el tipo y modalidad de servicio más adecuado a su caso en función de su disponibilidad, atendiendo a la orientación y a la prescripción técnica de la persona profesional de referencia asignada.

i) A participar en el proceso de toma de decisiones sobre su situación personal y familiar, así como a dar o denegar su consentimiento en relación con una determinada intervención. Este consentimiento deberá ser otorgado siempre por escrito cuando la intervención implique el ingreso en un servicio de alojamiento o en un centro residencial. En el caso de personas con capacidad de obrar modificada judicialmente o personas menores de edad, se estará a lo que resulte de la correspondiente resolución judicial o administrativa.

j) A disponer de equipamientos y atención en las debidas condiciones de higiene y salubridad, intimidad y privacidad en sus comunicaciones.

k) A formular quejas y reclamaciones sobre la atención y servicio recibidos y a obtener respuestas a las mismas.

l) A renunciar voluntariamente a la utilización y disfrute de los servicios y prestaciones que tengan reconocidas,

salvo cuando su ejecución venga impuesta por resolución judicial o se deriven efectos perjudiciales para personas menores de edad o personas con capacidad de obrar modificada.

m) A la confidencialidad, entendiéndose por ello el derecho a que los datos de carácter personal que obren en su expediente o en cualquier documento que les concierna sean tratados con pleno respeto a lo previsto en la legislación vigente en materia de protección de datos de carácter personal. No será preciso el consentimiento de la persona interesada para comunicar dicha información a terceras personas cuando se trate de personal inspector en el ejercicio de una acción inspectora o de cualquier otro de los supuestos previstos en esta ley y en la legislación del procedimiento administrativo común.

n) A recibir atención en el propio domicilio familiar cuando las personas tengan dificultad grave de movilidad física.

ñ) A decidir, cuando no tenga modificada judicialmente la capacidad de obrar, sobre la tutela de su persona y bienes, para el caso de pérdida de su capacidad de autogobierno, así como a decidir libremente sobre el ingreso en centro residencial y al ejercicio pleno de sus derechos jurisdiccionales en el caso de internamientos no voluntarios o involuntarios en centros, garantizándose un proceso contradictorio en todo caso.

o) A recabar y recibir ayuda en los casos en que sea necesario por una institución u organización de apoyo, protección o tutela, si a la persona le ha sido modificada judicialmente su capacidad judicialmente.

p) A dar instrucciones previas para situaciones futuras de limitación de su capacidad de obrar en casos de pérdida de su capacidad de autogobierno.

q) Cualesquiera otros derechos que les reconozca la legislación vigente, esta ley y las disposiciones reglamentarias.

Derechos específicos de las personas usuarias de centros y servicios de atención diurna / nocturna y estancia residencial.

Las personas usuarias de centros y servicios de atención diurna/nocturna y estancia residencial tienen, además de los derechos reconocidos en el artículo anterior, los siguientes:

a) Al ejercicio de la libertad individual para el ingreso, la permanencia y la salida del centro o servicio, con las limitaciones establecidas en la legislación vigente para las personas menores de edad, tanto las que tengan la capacidad de obrar modificada como las incursas en medidas judiciales de internamiento.

b) A participar individual o colectivamente en la toma de decisiones del centro o servicio que les afecte, en los términos establecidos en la normativa y reglamento de régimen interno.

c) A conocer el reglamento interno del centro o servicio, redactado de manera comprensible, y a disponer de una copia.

d) A que se recoja en una historia personal, información de todos los aspectos relacionados con su salud, bienestar y gestión de su caso, así como a acceder a la misma con las garantías que prevé la legislación vigente en materia de protección de datos de carácter personal.

e) A recibir una atención personalizada de acuerdo con sus necesidades específicas.

f) A recibir atención sanitaria por el Servicio Canario de Salud en igualdad de condiciones que el resto de la ciudadanía, a tener asignado al personal de atención primaria en el centro de salud de la zona básica en que se encuentre el centro residencial y a recibir una atención integral resultado de una adecuada coordinación entre los sistemas de protección social y sanitario.

g) A la privacidad de sus comunicaciones, tanto dentro como fuera del centro, excepto disposición contraria por resolución judicial, así como derecho a la intimidad en vida cotidiana.

h) A considerar como domicilio el centro residencial donde viven, con garantía de todos los servicios y derechos, y a mantener su relación con el entorno familiar y social, así como a personalizar su espacio con objetos propios, siempre respetando los derechos del resto de personas usuarias.

i) A mantener una relación de afectividad en el establecimiento residencial, facilitándosele compartir el mismo alojamiento.

j) A no ser sometida a ningún tipo de inmovilización mecánica, restrictiva o sujeción física o tratamiento farmacológico sin prescripción específica facultativa o del equipo

multidisciplinar competente, salvo que exista peligro inminente para la seguridad física de la persona usuaria o de terceras personas y durante el tiempo imprescindible en el que se prolongue esa situación.

k) A la práctica religiosa que no altere el funcionamiento normal del centro, siempre que se ejerza desde el respeto a la libertad de otras personas.

l) A conocer el coste de los servicios que se reciben y la participación que, en su caso, deben realizar en su condición de persona usuaria.

m) A recibir atención complementaria de carácter socioeducativo, cultual y en general todas aquellas que favorezcan la promoción y la autonomía personal.

n) A ser informadas sobre sus derechos y deberes de forma adecuada a su nivel de comprensión en el caso de personas con discapacidad intelectual.

ñ) A obtener facilidades para hacer la declaración de voluntades anticipadas, de acuerdo con la legislación vigente.

o) Cualesquiera otros derechos reconocidos por la normativa vigente.

Obligaciones de las personas usuarias del sistema público de servicios sociales.

Las personas usuarias del Sistema Público de Servicios Sociales de Canarias, tendrán las siguientes obligaciones:

a) Respetar la dignidad de las autoridades y personal que gestionan los recursos y prestan los servicios del Sistema Público de Servicios Sociales, así como el plan de atención personalizada acordado y las orientaciones establecidas en el mismo.

b) Observar una conducta basada en el respeto, la no discriminación y la colaboración para facilitar la convivencia en el centro o servicio en el que se preste la atención, sí como la resolución de los problemas.

c) Cooperar positivamente con los profesionales de servicios sociales, participando activamente en el plan de atención social acordado.

d) Conocer y cumplir las normas, requisitos y procedimientos establecidos para el acceso a los recursos y servicios del Sistema Público de Servicios Sociales y los compromisos asumidos en el desarrollo de la intervención de la que sea objeto, haciendo un uso responsable de los bienes muebles, instalaciones y equipamientos en los que se preste la atención.

e) Facilitar a la administración pública información veraz de los datos personales, convivenciales, económicos y familiares, siempre que su conocimiento sea necesario para valorar y atender su situación. Asimismo, y con idéntica finalidad, presentar los documentos que sean imprescindibles salvo que estos obren en poder de la Administración pública requirente, o autorizar su obtención cuando exista convenio entre Administraciones.

f) Acudir y atender a las entrevistas a las que sean citadas por el personal profesional de los servicios sociales, a los efectos de poder valorar su situación y posibles cambios en la misma.

g) Comunicar las situaciones que se produzcan en su situación personal y unidad convivencial que puedan afectar al proceso de inserción social o a los servicios y prestaciones solicitadas o recibidas.

h) Firmar el acuerdo del servicio o la prestación pertinente con la entidad prestadora de los mismos.

i) Destinar las prestaciones económicas que perciban al fin previsto, y contribuir a la financiación del coste de los servicios recibidos cuando así lo establezca la normativa aplicable, en atención a la capacidad económica de las personas usuarias y, en su caso, de la unidad de convivencia.

j) Reintegrar total o parcialmente las prestaciones económicas y tecnológicas recibidas y no aplicadas al objeto de las mismas, cuando sea requerido para ello.

k) Cumplir cualquier otra obligación que establezca la legislación vigente.

Derechos de las personas profesionales del Sistema Público de Servicios Sociales.

Las personas profesionales de los servicios sociales, además de los derechos que se deriven de la legislación aplicable en función de su profesión, tendrán los siguientes derechos:

a) Derecho al desempeño de su actividad profesional en los servicios sociales en condiciones de igualdad y dignidad.

b) Derecho a recibir la información necesaria para el desarrollo de las funciones encomendadas por parte de las personas responsables de los servicios.

c) Derecho a recibir un trato respetuoso y correcto por parte de los responsables de los servicios, del resto de los profesionales y de las personas usuarias de los servicios sociales.

d) Derecho a que por parte de los empleadores se adopten medidas destinadas a proteger su identidad, si es preciso para prestar correctamente el servicio o garantizar su seguridad en el desempeño de las funciones encomendadas.

e) Derecho a que por parte de los empleadores se adopten medidas de prevención y atención ante situaciones provocadas por factores psicosociales que afecten a su estado emocional, cognitivo, fisiológico y de comportamiento.

f) Derecho a beneficiarse de una formación profesional continuada durante toda su vida activa con vistas a garantizar la adecuación de la atención prestada a las pautas de buena práctica profesional.

g) Derecho a participar, individual o colectivamente, en las decisiones que les afecten y en la organización de los servicios, y a acceder a los cauces de información, sugerencias y quejas que permitan el ejercicio efectivo y la defensa de sus derechos. Asimismo, a presentar sugerencias y participar en los procesos de evaluación de los servicios.

h) Derecho a disponer de los medios necesarios para garantizar la prestación de un servicio en condiciones que respondan a los criterios de calidad exigidos por la normativa correspondiente.

i) Otros derechos que se les reconozcan en la presente ley y sus normas de desarrollo.

Obligaciones de las personas profesionales del Sistema Público de Servicios Sociales.

Las personas profesionales de los servicios sociales, además de los derechos que se deriven de la legislación aplicable en función de su profesión, tendrán las siguientes obligaciones:

a) Promover la dignidad, la autonomía, la inclusión y el bienestar de las personas a las que atienden y respetar todos los derechos reconocidos en la presente ley a las personas usuarias y profesionales.

b) Conocer y cumplir la normativa vigente en el ámbito de los servicios sociales, y en particular las normas reguladoras de la organización y del funcionamiento de los servicios en los que ejercen su actividad y de los programas que gestionan.

c) Informar a la persona responsable del servicio, del departamento, o de la unidad competente, de aquellas cuestiones que puedan mejorar el funcionamiento, la organización o las instalaciones donde se efectúa la prestación de servicios sociales.

d) Mantener, en sus relaciones con otras personas profesionales y usuarias, un comportamiento no discriminatorio.

e) Respetar las opiniones, criterios y sugerencias que las personas usuarias tomen por sí mismas o a través de su representante legal.

f) Respetar la intimidad de los usuarios, garantizando la confidencialidad de los datos de carácter personal de los mismos.

g) Guardar las normas de convivencia y respeto mutuo en los servicios en los que prestan servicios sociales y en cualquier otro lugar relacionado con sus actividades.

h) En caso de que sea necesaria la derivación de la persona usuaria a otro u otros servicios, hacerlo de la manera más favorable para aquella, procurando la continuidad de la intervención.

i) Respetar y utilizar correctamente los bienes muebles y las instalaciones de los servicios en los que desarrollan sus funciones y de cualquier otro lugar relacionado con sus actividades.

j) Respetar los plazos que se establezcan para las distintas intervenciones, ajustándose, en todo caso, a los plazos máximos previstos en la normativa vigente.

k) Poner en conocimiento de la autoridad competente cualquier situación que en su opinión, y basándose en los elementos de valoración de los que disponen, pudiera conllevar una vulneración de derechos.

l) Otras obligaciones que se les impongan en la presente ley y sus normas de desarrollo.

Anexo II. Catálogo de servicios y prestaciones

En el presente anexo se ha incluido una descripción más detallada de los diferentes tipos de servicios y prestaciones mencionadas en el informe de Servicios Sociales de PLASMAC. En este sentido, se pretende que este anexo sirva de apoyo a la elaboración de los diferentes tipos de ayudas que puede gestionar PLASMAC. Por estos motivos, se ha incluido para cada tipo de servicio y prestación su definición, tal y como figura la nueva ley de Servicios Sociales.

Destacar la importancia de dejar en PLASMAC algunos campos como "inhabilitado" u "oculto". De tal manera que, en el futuro, en caso de que el Ayuntamiento prevea la incorporación de un nuevo servicio o prestación, el catálogo que disponga PLASMAC permita su habilitación o visibilidad.

Servicios del sistema público de servicios sociales.

1. Son servicios el conjunto de las actuaciones realizadas por profesionales, ya sea directamente o a través de medios tecnológicos, dirigidas a la prevención, diagnóstico, seguimiento, valoración, intervención, protección, promoción de la autonomía personal, acompañamiento social, mediación, e inclusión social, mediante actuaciones de atención a las personas, unidades de convivencia, grupos y comunidades.

2. Todos los servicios del Sistema público quedarán recogidos en el catálogo contenido en esta ley y en su posterior desarrollo reglamentario para su atención personalizada y/o comunitaria.

3. Los servicios del Sistema Público de servicios sociales de Canarias serán, al menos, las siguientes, en los términos que se recojan en el catálogo de servicios y de prestaciones:

a) Información: Servicio que posibilita a las personas, familias y grupos acceder en tiempo y forma a un conocimiento adecuado y suficiente sobre los derechos, servicios y prestaciones que pueden favorecer su inclusión social, autonomía y bienestar social, garantizando una información veraz, accesible y facilitada en términos comprensibles.

b) Valoración, que incluirá:

- **Valoración inicial:** Consiste en la identificación básica, desde una perspectiva integral, de las necesidades y capacidades de las personas, las familias y su entorno al objeto de constatar si procede una intervención del Sistema Público de Servicios Sociales y, en su caso, remitir a las personas usuarias a una valoración especializada.
- **Valoración Especializada:** Es una valoración que incluye la baremación de las situaciones de dependencia, discapacidad, exclusión y desprotección. La misma podrá ser: social, psicosocial, sociosanitaria o socioeducativa.
- **Valoración de seguimiento:** Servicio que conlleva la realización de evaluaciones periódicas del plan de atención personalizada.

c) Diagnóstico social: Consiste en la descripción y valoración profesional de las necesidades sociales y capacidades que presentan las personas, familias y grupos que

solicitan la atención del Sistema Público de Servicios Sociales, al objeto de determinar la intervención adecuada en el marco de un Plan de Atención Personalizada.

d) Orientación y seguimiento: Conjunto de acciones profesionales orientadas a dar a conocer derechos y recursos sociales que permitan a la persona la toma de decisiones y su participación en la elaboración del Plan de Atención Personalizada.

f) Acompañamiento social: Prestación en virtud de la cual la persona participa, en interacción con un profesional cualificado, en una relación de ayuda que contribuye a mejorar su desenvolvimiento autónomo e integración social. Se incluye dentro de este servicio la acción tutorial, la supervisión y el apoyo social, entre otros.

g) Prevención de la situación de dependencia y promoción de la autonomía personal: Conjunto de actuaciones dirigidas a la prevención de la aparición o agravamiento de enfermedades o discapacidades y de sus secuelas, así como el apoyo de la vida independiente y/o autónoma, a través de la promoción de condiciones de vida saludables, programas específicos de carácter preventivo y/o rehabilitador y de integración y mejora de las capacidades personales. Se incluye dentro de estos servicios todos aquellos establecidos en la Ley 39/2006, de 14 de diciembre, de Promoción de la Autonomía Personal y Atención a las personas en situación de dependencia.

h) Cuidados en el entorno familiar: Comprende el conjunto de actuaciones llevadas a cabo tanto en el domicilio de la persona como fuera de él, con el fin de atender las condiciones básicas de accesibilidad, necesidades y actividades de la vida diaria y prevenir la pérdida de autonomía, mejorando su calidad de vida. Este servicio comprende el apoyo a los desplazamientos que garantizan el acceso a los servicios sociales, además de:

- **Servicio de apoyo a las personas cuidadoras:** Conjunto de actuaciones de formación, apoyo y sustitución a aquellas personas que se dedican, con carácter habitual con o sin retribución, al cuidado de personas con limitaciones en su autonomía personal, familiar y social.
- **Ayuda a domicilio:** Conjunto de atenciones y cuidados de carácter personal y doméstico que pueden tener un carácter preventivo, asistencial o rehabilitador, destinadas a personas, familias o grupos para evitar o, en su caso, retrasar el ingreso en centro o para intervenir en situaciones de conflicto psico-familiar.
- **Centro de día o noche:** Este servicio ofrece, con carácter temporal o permanente, una atención individualizada e integral, durante el periodo diurno o nocturno a los menores en situación de riesgo o desprotección, a las personas en situación de dependencia, discapacidad o con enfermedad mental crónica.
- **Centros ocupacionales:** Aquellos donde se desarrollan actividades de terapia ocupacional, de rehabilitación y de inserción personal y socio-laboral para personas con discapacidad o aquellas que encuentran barreras para integrarse en el mercado laboral.

i) Intervención, que comprenderá:

- **Intervención y apoyo familiar:** Conjunto de actuaciones profesionales dirigidas a facilitar la convivencia y la inclusión social de las familias abordando situaciones de crisis, riesgo o vulnerabilidad familiar. Se incluye dentro de este servicio, entre otros, asesoramiento, intermediación arrendaticia, bancaria, inmobiliaria y tramitación de prestaciones económicas.
- **Intervención socio-familiar:** Conjunto de actuaciones profesionales de ayuda psico-educativa y social para el tratamiento y resolución de las necesidades sociales, educativas y familiares de las personas, las familias o grupos de población y su entorno.
- **Prevención e intervención socio-comunitaria e inclusión social:** Conjunto de actuaciones profesionales orientadas a la prevención de las situaciones de exclusión social, la dinamización comunitaria y la búsqueda de respuestas colectivas a las necesidades sociales, así como la transformación social de estas zonas desde unos objetivos comunes entre todas las partes implicadas para el logro de la cohesión social.
- **Intervención socioeducativa y psicosocial:** Conjunto de actuaciones profesionales que implican el establecimiento de un proceso, a través del cual las personas usuarias adquieren conocimientos, actitudes, hábitos o capacidades útiles para su desenvolvimiento autónomo e integración social. Se incluyen dentro de estos servicios la intervención social, estimulativa o rehabilitadora, psicológica, ocupacional, educativa, psicosocial, la mediación familiar y la intermediación y mediación social.
- **Intervención socio-sanitaria:** Conjunto de actuaciones profesionales orientadas a dar respuesta a situaciones de necesidad compleja que requieren de intervención de naturaleza mixta, social y sanitaria, de forma simultánea, o también secuencial, en todo caso complementaria y estrechamente articulada.
- **Intervención socio-laboral de colectivos en riesgo o exclusión social:** Conjunto de actuaciones profesionales orientadas a promover el acceso a la inclusión de estos colectivos, mediante la incorporación al mercado laboral, fomentando su autonomía.

n) Atención residencial: Servicio destinado a proporcionar alojamiento, temporal o permanente según los casos, a las personas o unidades de convivencia que carecen de este recurso básico, o que por necesidades especiales se considere adecuado una alternativa habitacional que ofrezca una atención personalizada y continuada.

ñ) Servicio de Atención Temprana: Conjunto de intervenciones dirigidas a la población infantil de 0 a 6 años, a la familia y al entorno, que tienen por objeto dar respuesta lo antes posible a las necesidades transitorias o permanentes que presenten los niños y niñas con trastornos en su desarrollo o en riesgo de padecerlo.

o) Protección jurídica y ejercicio de la tutela de las personas mayores de edad con capacidad de obrar modificada y en situación de desamparo: Es un servicio de apoyo a las personas mayores de edad con capacidad de obrar modificada y en situación de desamparo con el objeto de proteger sus derechos, así como promover y facilitar su ejercicio efectivo, velando especialmente por el cuidado de la persona y la administración de sus bienes, promoviendo su pleno desarrollo personal, su máxima

inclusión social y la mejora de la calidad de vida. Este servicio abarcará, además de la atención jurídica, la tutela judicial, la guarda y curatela.

p) Alojamiento para personas sin hogar: Alojamiento no permanente, organizado en distintos niveles de exigencia (alojamiento de baja exigencia, centros de acogida, viviendas tuteladas y pisos supervisados), destinado a acoger personas en situación de sin hogar. Así mismo, este servicio incluirá la atención inmediata de personas sin hogar que rechazan servicios de alojamiento.

q) Atención a mujeres víctimas de violencia de género, doméstica o de actos contra la libertad sexual: Es el conjunto de actuaciones profesionales destinadas a ofrecer información, orientación, acompañamiento, asesoramiento, protección socio-jurídica y apoyo psicológico. Asimismo, contempla todas las actuaciones que garanticen la prevención y reparación del daño.

r) Servicio de Atención a la Infancia y Adolescencia: Es el conjunto de actuaciones profesionales encaminadas a la promoción del bienestar personal y social de los niños y las niñas y la adolescencia y de las actuaciones de prevención, atención, protección, reparación y participación dirigidas a estas personas con el fin de garantizar el ejercicio de sus derechos, la asunción de sus responsabilidades y la consecución de su desarrollo integral.

Este servicio abarcará, entre otros, los de familia numerosa, servicio de apoyo técnico a menores con conductas violentas en la familia, servicio de mediación para el encuentro entre personas adoptadas y sus familiares de origen, servicio de intervención-terapéutica para niños y niñas en acogimiento, servicio de acogida residencial y familiar, servicio de adopción y post-adopción y servicio de justicia juvenil.

s) Servicio de apoyo a la emancipación: Está compuesto por el conjunto de actuaciones de apoyo y seguimiento personalizado de los adolescentes mayores de 16 años con alguna medida de protección o mayores de 18 años sobre lo que se ha ejercido alguna medida protectora.

Prestaciones económicas del sistema público de servicios sociales.

1. Son prestaciones económicas las aportaciones dinerarias o en especie, periódicas o en un solo pago, integrantes del sistema público de servicios sociales o de cualquier otro sistema de protección, destinadas a lograr los objetivos previstos en esta ley.

2. Las prestaciones económicas responderán a alguna de las siguientes situaciones:

a) Aquellas dirigidas al sostenimiento de las necesidades básicas y a la inclusión social de personas, familias o colectivos.

b) Las destinadas a apoyar y compensar a las personas que asuman las-tereas de cuidado en el entorno familiar esenciales para el desenvolvimiento autónomo y la inclusión social de alguno de sus integrantes.

c) Las ayudas de rehabilitación de vivienda y mejora de la accesibilidad en orden a la mejora y la inclusión social.

d) Aquellas vinculadas a servicios a que tengan derecho las personas usuarias del sistema público de servicios sociales pero cuyo acceso no pueda garantizarse temporalmente por déficit de servicio en la red canaria de servicios sociales en los términos definidos reglamentariamente.

e) Aquellas dirigidas a las víctimas de violencia de género.

f) Cualquier otra que pueda establecerse de acuerdo con los fines establecidos en esta ley y sus disposiciones reglamentarias.

3.-Las prestaciones económicas del sistema público de servicios sociales de Canarias serán, al menos, las siguientes, en los términos que se recojan en el catálogo de servicios y de prestaciones:

a) La vinculada a cubrir necesidades básicas: Conjunto de prestaciones destinadas a dar cobertura a las necesidades básicas con carácter temporal ante una situación excepcional o extraordinaria y puntual que requiere de una atención inmediata, sin la cual podría producirse un grave deterioro o agravamiento del estado de vulnerabilidad y de desprotección en una persona o unidad de convivencia.

Esta prestación incluirá, al menos, las siguientes necesidades básicas: el alojamiento de urgencia, la atención alimenticia adecuada, incluidas las personas afectadas por celiaquía y diabetes, vestido, higiene y aseo personal, medicamentos, suministros básicos de la vivienda (agua, luz, gas, etc.), y alquiler de la vivienda.

b) La vinculada a cuidados en el entorno familiar y apoyo a personas cuidadoras no profesionales: Esta prestación se reconoce, con carácter excepcional, con el fin de contribuir a la cobertura de los gastos derivados de la atención prestada, cuando una persona en situación de dependencia está siendo atendida por alguna persona de su entorno familiar o afectivo y lleva haciéndolo de forma continuada en el tiempo.

c) La vinculada a la asistencia personal: Esta prestación tiene la finalidad de promocionar una vida más autónoma en el entorno habitual que facilite la atención de manera personalizada e integradora en atención a las circunstancias y necesidades de la persona en situación de dependencia, ayudándola en su plena integración social. Está destinada a contribuir a la cobertura de los gastos derivados de la contratación de una persona con funciones de asistencia personal.

d) La vinculada al servicio: Está destinada a aquellos casos en los que existe imposibilidad de acceder al servicio público o concertado adecuado a la persona en situación de dependencia. Su objetivo es contribuir a la financiación del coste

de dicho servicio proporcionado por entidades privadas y debidamente acreditadas.

e) La vinculada al pago único a mujeres víctimas de violencia de género: Se destina a mujeres víctimas de violencia de género y su finalidad es contribuir a paliar temporalmente la ausencia de ingresos, por lo que debe quedar acreditada la insuficiencia de recursos económicos.

f) La vinculada a la realización de adaptaciones en la vivienda habitual y en los vehículos particulares: Aquellas destinadas a facilitar a las personas con limitaciones en su autonomía personal la realización de adaptaciones en su vivienda habitual y/o en su vehículo particular con el fin de mejorar su accesibilidad, favorecer al máximo sus posibilidades de desenvolverse autónomamente y facilitar el apoyo que les prestan otras personas para realizar las actividades básicas de la vida diaria.

g) Prestación económica individual para la adquisición de ayudas técnicas y productos de apoyo: Aquellas destinadas a facilitar la compra de ayudas técnicas y productos de apoyo a personas con limitaciones en su autonomía personal, con el fin de favorecer al máximo sus posibilidades de desenvolverse autónomamente y/o facilitar el apoyo que les prestan otras personas para realizar las actividades básicas de la vida diaria.

h) Prestación económica para el acogimiento familiar: Aquellas de carácter periódico destinadas a remunerar el acogimiento familiar, tanto en familia ajena como familia extensa, por el tiempo que dure la medida de protección y cuando concurran las circunstancias que reglamentariamente se determinen.

i) Prestación económica de apoyo a la emancipación dirigida a jóvenes extutelados.

j) Prestación económica de percepción periódica vinculada a la inclusión social. Está dirigida a las personas o unidades de convivencia sin ingresos o con los umbrales de renta que se determinen reglamentariamente y que se encuentren en situación de vulnerabilidad social, sea cual sea la causa, actuando como última red de protección social.

k) Prestación económica, de percepción periódica vinculada a la inclusión social. Está dirigida a los Hogares sin ingresos y en situación de necesidad social sea cual sea la causa, actuando como última red de protección social para atender a las personas que queden desamparadas.

Prestaciones tecnológicas del sistema público de servicios sociales.

1. Son prestaciones tecnológicas del sistema público de servicios sociales, las que, por medio de una ayuda técnica o producto de apoyo, atienden a las necesidades sociales de la persona, pudiéndose asociar con otras prestaciones.

2. Las prestaciones tecnológicas del sistema público de servicios sociales de Canarias serán, al menos, las siguientes, en los términos que se recojan en el catálogo de Servicios y de Prestaciones.

a) La asistencia tecnológica o técnica: dispositivo de alarma para mujeres víctimas de violencia de género, atención telefónica continuada durante las 24 horas para la infancia, atención telefónica continuada durante las 24 horas personas mayores de 65 años e intérprete de lengua de signos en el servicio de información de la Consejería competente, entre otras.

b) La teleasistencia: prestación que tiene por objeto garantizar la permanencia en el domicilio a las personas que se hallen en situación de necesidad social, ofreciendo una respuesta inmediata ante situaciones de urgencia, inseguridad, soledad y aislamiento a las personas usuarias, mediante el uso de tecnologías de la comunicación y de la información, con apoyo de los medios personales necesarios.

c) La asistencia para la accesibilidad universal: transporte adaptado para personas en situación de dependencia, entre otras.

Otros servicios y prestaciones del sistema público de servicios sociales.

Otros servicios y prestaciones adicionales a los previstos en la presente ley que puedan establecerse a través de la revisión del catálogo de Servicios y prestaciones, así como los que están o pudieran estar previstos en el futuro en la legislación sectorial.

Anexo III. Registro de entidades de iniciativa social

En el presente anexo se describe el procedimiento que una entidad de iniciativa privada debe recorrer para poder ofrecer un determinado servicio social de forma integral o parcial. Entre estos pasos, cabe destacar que requiere de que se registren previamente en el Registro Único de Centros de PLASMAC, y posteriormente consigan las autorizaciones administrativas determinadas (después de la comprobación de una serie de condiciones y especificaciones).

Solo hasta que consigan la **Autorización Administrativa Definitiva de Funcionamiento**, conseguirán poder participar en el **Catálogo de Servicios y Prestaciones de PLASMAC.** Y a continuación, se adjunta la descripción que aparece en la nueva ley de Servicios Sociales.

Régimen de concertación en el Sistema Público de los Servicios Sociales con entidades de iniciativa social.

1. Las administraciones públicas canarias, incluidos los cabildos y los ayuntamientos competentes en materia de servicios sociales podrán encomendar a entidades privadas de iniciativa social la provisión de servicios y prestaciones previstas en el Catálogo de Servicios y Prestaciones, mediante acuerdos de acción concertada.

2. Las entidades de iniciativa social que opten a un concierto para la gestión de servicios y prestaciones deberán contar con la acreditación o autorización administrativa, según proceda, de los centros y servicios de los que sean titulares, así como figurar inscrita en el registro de entidades, centros y servicios, según lo previsto en esta ley.

3. El Gobierno de Canarias, en el marco de lo dispuesto en esta ley, establecerá el régimen jurídico y las condiciones de actuación de los centros privados concertados que participen en el Sistema Público de Servicios Sociales, determinando los requisitos de acceso, la duración máxima y las causas de extinción del concierto, así como las obligaciones de las partes.

4. La concertación puede implicar la gestión integral o parcial de los servicios y prestaciones contenidas en el Catálogo de Servicios y Prestaciones.

5. El acceso a las plazas concertadas con entidades privadas de iniciativa social será siempre a través de la administración concertante.

Objeto de los conciertos.

1. Podrán ser objeto de concierto:

> a) La reserva y ocupación de plazas para su uso exclusivo por las personas usuarias del sistema público de servicios sociales, cuyo acceso será autorizado por las administraciones públicas competentes mediante los criterios previstos para ello en la presente ley y normativa que la desarrolla.

b) La gestión integral de servicios, prestaciones o centros que se determine reglamentariamente.

2. Cuando la prestación del servicio conlleve procesos que requieran de diversos tipos de intervenciones en distintos servicios o centros, la Administración Pública competente podrá adoptar un solo acuerdo de acción concertada con dos o más entidades, imponiendo en dicho acuerdo mecanismos de coordinación y colaboración de obligado cumplimiento.

Requisitos de las entidades.

1 Podrán suscribir conciertos con las administracionespúblicas competentes en materia de servicios sociales de la Comunidad Autónoma de Canarias, todas las personas físicas o jurídicas de carácter privado, sin ánimo de lucro.

2. Para poder suscribir los conciertos, las personas y entidades solicitantes deberán reunir necesariamente los requisitos que se establezcan en esta ley y en su normativa de desarrollo, y en especial:

a) Haber obtenido la oportuna autorización o acreditación, para la prestación del servicio objeto de concierto.

b) Estar inscritas en el Registro Único de Entidades, Centros y Servicios, según lo establecido en la presente ley y en su normativa de desarrollo.

c) Acreditar la solvencia técnica para prestar el servicio objeto del concierto.

d) Acreditar la disposición de los medios y recursos suficientes para garantizar el cumplimiento de las condiciones previstas en el acuerdo de formalización del concierto.

e) Aquellas entidades con las que se suscriban conciertos de ocupación o reserva de plazas deberán acreditar la titularidad del centro o tener su disponibilidad por cualquier título jurídico válido por un periodo no inferior al de vigencia del concierto y acreditar que el mismo cuenta con las condiciones adecuadas para prestar el servicio.

3. No obstante, el Gobierno de Canarias mediante Decreto podrá establecer un procedimiento de concertación diferenciado vinculado a aquellos servicios que, en función de su naturaleza y alta especialización, recoja las características específicas de los mismos, tales como la concurrencia de las entidades o el ámbito de vigencia del concierto, entre otras.

Méritos preferentes para suscribir los conciertos.

Para la elección de la entidad que prestará el servicio, se valorarán los méritos y capacidades de las mismas, tales como:

a) Los años de experiencia acreditada en la prestación del servicio.

b) Que acredite buena valoración de las personas usuarias, si ya ha prestado el servicio anteriormente.

c) Que haya obtenido certificaciones de calidad.

d) Que la entidad aporte informes de buenas prácticas en el ámbito laboral de las empresas.

e) Que la entidad cuente con más del 40% de mujeres en los órganos de dirección.

f) Que aplique medidas orientadas a la conciliación personal, familiar y laboral de quienes trabajan en la entidad.

g) Que la entidad aplique medidas para la efectiva integración laboral de las personas con discapacidad más allá de las exigencias legales.

h) Otros que se determinen reglamentariamente.

Formalización de los conciertos.

1. La formalización de los conciertos se efectuará a través de un documento administrativo que, además de aquellos aspectos que se determinen reglamentariamente, contemple los siguientes:

a) La identificación de las partes del concierto y obligaciones que adquieran las mismas.

b) La determinación del objeto del concierto, con especificación de los objetivos a alcanzar.

c) La fecha de inicio de la prestación del servicio concertado y plazo de vigencia, causas de extinción y procedimientos para su modificación.

d) El régimen de aportación económica por parte de la Administración concertante, de acuerdo con los módulos económicos correspondientes y sistema de actualización de dicha aportación.

e) La periodicidad y procedimiento de realización de los pagos y anticipos, así como la justificación de los gastos.

f) El régimen de acceso de las personas usuarias a los servicios y prestaciones.

g) Los mecanismos de seguimiento, control y auditoría por parte de la Administración.

2. Los conciertos podrán incorporar la modalidad de anticipo, pudiéndose establecer hasta el 75% anual.

3. Se podrá suscribir un único concierto para la reserva y ocupación de plazas en varios centros o para la gestión integral de una pluralidad de prestaciones o servicios cuando

todos ellos dependan de una misma entidad. Esta suscripción se efectuará en las condiciones que se determinen reglamentariamente.

Efectos de los conciertos.

1. La formalización por escrito del correspondiente concierto a que se refiere la presente ley perfecciona el acuerdo entre las partes, obligando al titular de la entidad concertada a la prestación del servicio o provisión de plazas en los términos estipulados, y de acuerdo a lo previsto en el pliego técnico que deberá contener, al menos, las condiciones técnicas y económicas referidas al objeto del concierto.

2. El concierto obliga al titular de la entidad privada de iniciativa social a proveer las prestaciones y servicios en las condiciones previstas en el Catálogo de Servicios y Prestaciones.

3. En relación con las prestaciones no gratuitas del Sistema Público de Servicios Sociales, las entidades no podrán cobrar a las personas usuarias cantidad distinta a las determinadas por la Administración que hubiera establecido el concierto.

4. El cobro a las personas usuarias de cualquier cantidad por servicios complementarios, al margen de las tarifas o los precios públicos estipulados deberá ser autorizado por la Administración que hubiera establecido el concierto.

Duración, renovación, modificación y extinción de los conciertos.

1. La duración inicial de los conciertos será de un máximo de cinco años, pudiendo renovarse por acuerdo expreso de las partes, adoptado 6 meses antes de su vencimiento, por un nuevo período máximo de dos años.

2. Los conciertos podrán ser objeto de revisión y, en su caso, de modificación en los términos que se establezca en el correspondiente acuerdo de concierto.

3. Sin perjuicio de lo dispuesto en esta ley en relación al régimen sancionador, son causas de extinción de los conciertos:

a) El acuerdo mutuo de las partes, manifestado con la antelación que se determine en el concierto para garantizar la continuidad de los servicios y prestaciones.

b) El incumplimiento grave de las obligaciones derivadas del concierto por parte de la Administración pública o del titular del servicio, previo requerimiento para exigir el cumplimiento de las obligaciones derivadas del mismo.

c) El vencimiento del plazo de duración del concierto, salvo que se acuerde su prórroga o renovación.

d) La extinción de la persona jurídica a la que corresponda la titularidad.

e) La revocación de la acreditación o autorización administrativa de la entidad concertada.

f) El cese voluntario, debidamente autorizado, de la entidad concertada en la prestación del servicio.

g) La inviabilidad económica del titular del concierto, constatada por los informes de auditoría que se soliciten.

h) La negativa a atender a las personas usuarias derivadas por la Administración pública.

i) La solicitud de abono a las personas usuarias de servicios o prestaciones complementarias cuando no hayan sido autorizadas por la Administración pública.

j) La cesión de la prestación de los servicios concertados por otras entidades sin la autorización expresa y previa de la Administración que firmó el concierto.

k) El resto de causas que establezca esta ley y su normativa de desarrollo.

4. Concluida la vigencia del concierto, las administraciones públicas deberán garantizar que los derechos de las personas usuarias de los servicios y prestaciones concertadas no se vean perjudicadas por la finalización del mismo.

Autorización de centros y servicios.

1. Las entidades que desarrollen sus actividades en el ámbito de la Comunidad Autónoma de Canarias requerirán de autorización administrativa de la Consejería competente en materia de servicios sociales para su instalación y funcionamiento, así como para las modificaciones que respecto de su estructura física o funcional puedan establecerse.

2. La Consejería competente en materia de servicios sociales determinará reglamentariamente las condiciones de la autorización administrativa de los centros y servicios, que deberán contener, al menos:

a) Las condiciones de edificación, emplazamiento y acondicionamiento exigibles a las infraestructuras donde se deben prestarán los servicios.

b) Las condiciones materiales, de seguridad y de equipamiento exigibles a los servicios en función de su naturaleza.

c) Los requisitos de titulación del personal, y las ratios de profesionales, según el número de personas a las que se deba atender y el grado de ocupación.

d) Una memoria en la que se especifique la organización y funcionamiento del centro o servicio, así como el plan de actuación.

3. Los centros requerirán de las siguientes autorizaciones:

a) Autorización previa, por la que declara que un proyecto de creación, reforma o traslado de una centro o servicio de titularidad privada, reúne los requisitos y

condiciones necesarios para garantizar a las personas usuarias la calidad de la atención, que se concederá una vez se haya constatado dicho cumplimiento, en el plazo máximo de 3 meses desde la presentación de la misma.

b) Autorización definitiva de funcionamiento, que tendrá la finalidad de habilitar al centro para realizar las actividades que constituyen su objeto, una vez que se haya constatado su adecuación al proyecto autorizado con anterioridad.

4. Las entidades prestadoras de servicios, requerirán de una autorización de funcionamiento en los términos que reglamentariamente se determinen, con la finalidad de constatar su competencia para realizar las actividades que constituyen su objeto.

5. Las condiciones a que se refiere este artículo se entienden exigibles sin perjuicio del cumplimiento por los centros y los servicios de las disposiciones estatales, autonómicas y locales que les sean de aplicación.

Acreditación administrativa.

1. Las entidades que pretendan concertar plazas o servicios con las administraciones públicas deberán contar con la correspondiente acreditación administrativa, en los términos que reglamentariamente se determinen.

2. El otorgamiento de la acreditación administrativa corresponde a la Consejería competente en materia de servicios sociales, y tiene como finalidad asegurar el cumplimiento de los requisitos de calidad de los centros y servicios objeto de concierto.

3. Las condiciones para la acreditación administrativa deberán comprender las especificaciones concretas, parámetros y estándares de calidad de referencia de las infraestructuras físicas y rotacionales, recursos humanos y demás aspectos de carácter organizativo y de funcionamiento de los servicios y centros.

Resolución, vigencia, revocación, suspensión y extinción de la autorización y acreditación administrativa.

El Gobierno de Canarias regulará mediante Decreto los supuestos y efectos de la resolución, vigencia, revocación, suspensión y extinción, tanto de la acreditación como de la autorización administrativa a que se refieren los artículos anteriores.

Anexo IV. Sanciones del sistema público de Servicios Sociales

Dado que uno de los aspectos importantes de la gestión a través de PLASMAC podría permitir agilizar o facilitar la vigilancia, control y comprobación de los Servicios Sociales, participen o no en el Sistema Público de Servicios Sociales, a fin de que su actuación se adecue a lo dispuesto en la nueva ley de servicios sociales y en las futuras normativas. PLASMAC podría contener un módulo de carácter privado y que solo pueden tener acceso el perfil de "Personal de Inspección".

La elaboración de las Actas de Inspección en PLASMAC, tiene como resultado la imposición de sanciones, las cuales vienen reguladas en la nueva ley de Servicios Sociales **desde tres niveles: leves, graves, y muy graves.**

En el presente anexo, se describen qué se considera una infracción, como se tipifica de acuerdo con las acciones cometidas tanto por las personas beneficiarias como por los profesionales y entidades de acción social, así como los criterios de graduación de la importancia de las infracciones cometidas.

Infracciones en materia de servicios sociales.

1. Constituyen infracciones administrativas en materia de servicios sociales las acciones u omisiones de las personas físicas o jurídicas tipificadas en la presente ley, sin perjuicio de lo previsto en la normativa estatal básica y en las disposiciones específicas de los distintos sectores de servicios sociales.

Las infracciones se clasificarán en leves, graves y muy graves, de acuerdo con la naturaleza de la obligación infringida y la entidad del derecho afectado.

2. Las infracciones y sanciones tipificadas en la Ley 39/2006, de 14 de diciembre, de promoción de la autonomía personal y atención a las personas en situación de dependencia, se calificarán y sancionarán de acuerdo con lo que establece la mencionada ley. En aquello no regulado en la normativa específica de dependencia, se aplicará lo que se dispone en este título.

3. Las infracciones en materia de servicios sociales darán lugar a las sanciones administrativas correspondientes, previa instrucción del oportuno procedimiento y sin perjuicio de las responsabilidades de otro orden que pudiesen concurrir.

4. Sin perjuicio de las especialidades establecidas en los procedimientos de carácter sancionador en la legislación del procedimiento administrativo común, reglamentariamente el Gobierno de Canarias desarrollará las previsiones de esta ley para adaptar el procedimiento sancionador a la estructura de las administraciones integrantes del Sistema público de Servicios Sociales de Canarias, determinar los órganos competentes, plazos, formas de iniciación y terminación, publicación e informes a recabar, sin que, en ningún caso, puedan incluirse trámites adicionales o distintos a los contemplados en dicha legislación estatal.

Prescripciones de las infracciones y sanciones.

1. Las infracciones y sanciones en materia de servicios sociales tipificadas en esta ley prescriben, respectivamente:

- Al año, si son leves.
- A los tres años, si son graves.
- A los cuatro años, las muy graves.

2. Dicho plazo comenzará a contar desde la fecha en que la infracción haya sido cometida o la sanción acordada.

En el caso de las infracciones continuadas o permanentes, el plazo comenzará a contar desde que finalizó la conducta infractora.

Infracciones y sanciones de centros y servicios sociales

a. Infracciones leves.

Constituyen infracciones leves las siguientes:

a) Vulnerar los derechos relativos a la disposición, al conocimiento y cumplimiento del reglamento interno de los equipamientos y centros de servicios sociales, a la existencia de un sistema de recepción y resolución de quejas y sugerencias, a la comunicación a la persona usuaria del precio de la prestación y la contraprestación que ha de satisfacer, y a la tenencia de objetos personales significativos para la persona usuaria, siempre y cuando dichas conductas no deriven perjuicio directo y concreto sobre las personas usuarias de los servicios sociales.

b) No tener adaptados a la normativa vigente el reglamento de régimen interno o el documento contractual suscrito con la persona usuaria, por parte de los responsables de los centros y servicios.

c) Incumplir las normas, requisitos, procedimientos y condiciones establecidos para el disfrute de las prestaciones, siempre y cuando de dichas conductas no derive un perjuicio directo y concreto sobre las personas usuarias de los servicios sociales.

d) Incumplir o no ejecutar correctamente cualquiera de las acciones asignadas en el expediente individual de atención, siempre y cuando dichas de conductas no un derive perjuicio directo y concreto sobre las personas usuarias de los servicios sociales.

e) Incumplir la normativa reguladora de las condiciones materiales y funcionales mínimas que tienen que cumplir los centros y servicios, si el incumplimiento no pone en peligro para la seguridad de las personas usuarias o los profesionales.

f) Realizar en los centros o en el desarrollo de los servicios actividades distintas de las autorizadas o inscritas, cuando ello no suponga una infracción grave o muy grave.

g) No mantener actualizados o correctamente cumplimentados los libros de registro y control de las personas usuarias que exija la normativa, sus expedientes personales, la documentación relativa al grado de dependencia de las personas usuarias, o cualquier otra documentación que exija la normativa vigente, siempre y cuando ello no constituya una infracción grave.

h) No presentar la declaración responsable o la comunicación, o la falsedad en cualquier dato, siempre que cumpla todos los requisitos necesarios que establece la normativa, y no derive en un perjuicio directo y concreto sobre las personas usuarias de los servicios sociales

i) Incumplir la obligación sobre supervisión y formación continuada del personal adscrito a los centros o servicios cuando la normativa lo exija.

b. Infracciones graves.

Constituyen infracciones graves las siguientes:

a) Todas las tipificadas como leves en el artículo anterior, cuando hubieran producido consecuencias graves para la salud o la integridad de las personas usuarias o los profesionales de los centros o servicios sociales, o para el patrimonio de las mismas.

b) Incumplir el deber de sigilo y confidencialidad con respecto a los datos de las personas usuarias de los servicios sociales.

c) No salvaguardar el derecho a la intimidad de las personas usuarias.

d) Incumplir la legislación específica para cada tipo de centro o servicio social, cuando de la infracción pudiera derivarse daño o perjuicio para las personas usuarias.

e) No presentar la declaración responsable, incumpliendo los requisitos necesarios establecidos en la normativa.

f) No suministrar a la Administración los datos o documentos a que obligue la normativa.

g) No realizar con claridad y transparencia la administración, custodia y manejo de fondos y bienes de las personas usuarias de los centros o servicios sociales por parte de los directores, administradores o personas responsables, cuando, debido a la situación física o psíquica de aquéllos, estos últimos sean guardadores de hecho y actúen como tales conforme al artículo 303 del Código Civil y sin perjuicio de las responsabilidades de otro orden en que hubieren incurrido.

h) Realizar ofertas, promociones o publicidad de centros y servicios que no se correspondan con los prestados efectivamente.

i) Ocultar o falsear documentación relevante para tramitar la autorización, acreditación o registro de centros o servicios, así como para la celebración de conciertos, contratos o convenios con la administración.

j) Incumplir las condiciones contenidas en el concierto, convenio o contrato de plazas con la Administración.

k) Obstruir o dificultar, de cualquier modo, la acción del personal inspector en el desempeño de su cargo, así como no prestar la colaboración y auxilio requeridos para el ejercicio de sus funciones.

l) Vulnerar los derechos de las personas profesionales en los centros o servicios sociales y dañar de forma premeditada equipamientos e instalaciones.

ll) Impedir el ejercicio de la libertad individual en el ingreso, permanencia y salida de un centro residencial, salvo lo establecido al efecto por la legislación vigente para menores y personas con la capacidad de obrar modificada.

m) La realización de actuaciones destinadas a menoscabar o restringir los derechos derivados del respeto a las personas.

n) La realización de actos que alteren o perturben el normal funcionamiento del centro o servicio o sus condiciones de habitabilidad cuando afecten a la asistencia que prestan.

ñ) La resistencia, falta de respeto, la toma de represalias o cualquier otra forma de presión ejercida contra las personas profesionales de los centros y servicios sociales, las personas usuarias o sus acompañantes, siempre que no sean constitutivas de ilícito penal.

o) Efectuar el cambio de titularidad de un centro o servicio social sin presentar nueva solicitud de autorización, declaración responsable o acreditación administrativa.

p) Carecer de lista actualizada de precios o cobrar a las personas usuarias de centros o servicios cantidades superiores a las que corresponda.

q) Reincidir en la comisión de infracciones leves. A los efectos de la presente ley, se entenderá que existe reincidencia en los casos de comisión de la segunda infracción de la misma naturaleza en el término de un año, cuando así haya sido declarado por resolución administrativa firme.

c. Infracciones muy graves.

Constituyen infracciones muy graves las siguientes:

a) Todas las tipificadas como leves o graves cuando hubieran producido consecuencias muy graves para la salud o la integridad de las personas usuarias.

b) El trato degradante hacia las personas usuarias de las entidades y centros de servicios sociales, que afecte a su dignidad o a su integridad física o psíquica, así como el encubrimiento y el silenciamiento de dicha conducta.

c) Incumplir la normativa reguladora del registro de centros y servicios sociales, así como la normativa reguladora de la acreditación de los mismos.

d) Impedir la acción del personal inspector en el desempeño de su cargo.

e) La agresión física a las personas usuarias o a sus acompañantes, siempre que no sea constitutiva de ilícito penal.

f) Reincidir en la comisión de infracciones graves. A los efectos de la presente ley, se entenderá que existe reincidencia en los casos de comisión de la segunda infracción de la misma naturaleza en el término de un año, cuando así haya sido declarado mediante resolución administrativa firme.

Sanciones.

1. Las infracciones tipificadas en el presente capítulo se sancionarán como sigue:

- Las infracciones leves, con apercibimiento o multa de 300 euros a 3.000 euros, o con ambos.
- Las infracciones graves, con multa de 3.001 euros a 30.000 euros.
- Las infracciones muy graves, con multa de 30.001 euros a 300.000 euros.

2. La sanción por la comisión de infracciones muy graves en centros y servicios podrá llevar aparejada la imposibilidad de obtener subvenciones públicas, de conformidad con la legislación general de subvenciones, el cierre temporal, total o parcial de los mismos, o la pérdida de la autorización o acreditación del centro o servicio, en los casos que proceda, así como la rescisión de los conciertos, convenios o contratos que pudieran existir con la entidad titular o gestora.

3. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario, se estará a lo que dispone el artículo 85 de la Ley del Procedimiento Administrativo Común de las administraciones públicas.

4. En todos aquellos casos en los que de la infracción se derive un enriquecimiento indebido, la persona o la entidad infractora deberá abonar, además de la sanción correspondiente en función de la gravedad de la infracción, el importe equivalente al enriquecimiento producido.

5. Por el Gobierno de Canarias se procederá reglamentariamente a la actualización de las cuantías de las sanciones previstas en el presente artículo.

Infracciones y sanciones de las personas usuarias de servicios sociales

a. Infracciones leves.

Son infracciones leves de las personas usuarias o beneficiarias de los servicios y prestaciones las siguientes:

a) No facilitar a la entidad o al órgano de la Administración correspondiente, los datos que les requieran y que sean legalmente exigibles.

b) No comparecer de manera injustificada en la fecha fijada ante el órgano gestor de la prestación cuando éste se lo requiera motivadamente.

c) Mostrar falta de consideración y de respeto hacia el personal del centro o servicio, o a las otras personas usuarias o a las visitantes.

d) Incumplir los preceptos del reglamento de funcionamiento del centro cuando no esté tipificado como falta grave o muy grave.

b. Infracciones graves.

Son infracciones graves de las personas usuarias o beneficiarias de los servicios y prestaciones las siguientes:

a) Falsear datos a la Administración si la falsedad no ha sido determinante para acceder a la prestación.

b) No comunicar a la Administración los cambios o las alteraciones de las circunstancias o de los requisitos que determinaron la concesión de la prestación.

c) Producir daños a las instalaciones del centro o servicio.

d) Alterar gravemente la convivencia del centro o servicio.

e) Cometer agresión física al personal de los centros y servicios y a las demás personas usuarias y sus acompañantes, siempre que no sea constitutiva de ilícito penal.

c. Infracciones muy graves.

Son infracciones muy graves de las personas usuarias o beneficiarias de los servicios y prestaciones las siguientes:

a) Reincidir en la comisión de infracciones graves. A los efectos de la presente ley, se entenderá que existe reincidencia en los casos de comisión de la segunda infracción de la misma naturaleza en el término de un año, cuando así haya sido declarado por resolución administrativa firme.

b) Falsear datos a la Administración, si la falsedad ha sido determinante para acceder a la prestación.

c) Tener un comportamiento incívico o agresivo, de una manera continuada, que suponga un riesgo para el resto de las personas usuarias y para el personal y que haga inviable la convivencia en el centro.

d) Incumplir las obligaciones previstas en los pactos del contrato de servicios.

e) No destinar la prestación a la finalidad para la que se ha concedido.

Sanciones.

1. Las infracciones tipificadas en el presente capítulo se sancionarán como sigue:

a) Las infracciones leves, con una amonestación o una multa por un importe mínimo de 100 euros y máximo de hasta la mitad del indicador público de renta de efectos múltiples (Iprem) mensual.

b) Las infracciones graves, con la suspensión de la condición de persona usuaria o beneficiaria de la prestación, o con el traslado a otro centro, por un periodo máximo de doce meses.

c) Las infracciones muy graves, con la extinción de la prestación económica o su reintegro, en los casos que proceda, del servicio o el traslado definitivo a otro centro.

2. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario, se estará a lo que dispone el artículo 85 de la Ley del Procedimiento Administrativo Común de las administraciones públicas.

Anexo V. Articulado RGPD correspondiente a PLASMAC

En el presente anexo se describe la base legal en la que se basa el análisis normativo sobre el funcionamiento de PLASMAC con respecto a la protección y tratamiento de datos personales. A continuación, no se encuentra el articulado del Reglamento, sino un análisis del articulado aplicable a PLASMAC, con el fin de ampliar las conclusiones expuestas en el "Capítulo 2. Protección de datos. Requisitos técnicos para el cumplimiento del Reglamento General de Protección de Datos en el marco del proyecto PLASMAC".

En los capítulos II, III, IV, el impacto de la normativa al funcionamiento y gestión de PLASMAC es muy alto. En ellos se definen los principios del tratamiento, los derechos de los usuarios y la relación entre PLASMAC y la entidad encargada del tratamiento de los datos.

En el capítulo V, el impacto de la normativa al funcionamiento y gestión de PLASMAC es medio. En él, se definen los mecanismos y esquemas para las transferencias de datos personales a terceros países u organizaciones internacionales. Dado que PLASMAC no realizará transferencias a terceros países ni organizaciones internacionales, se realiza un análisis desde un punto de vista informativo sobre las implicaciones que puede llegar a tener sobre PLASMAC.

En los últimos capítulos del reglamento (VI, VII, VIII, IX y X), el impacto de la normativa al funcionamiento y gestión de PLASMAC es bajo. En estos capítulos se tratan aspectos referentes a las autoridades de control, cooperación y coherencia entre autoridades, recursos, responsabilidad y sanciones que establece el reglamento, situaciones específicas del tratamiento de datos, la delegación de poderes y las disposiciones finales del Reglamento.

Capítulo II - Principios

Art. 5. Principios relativos al tratamiento

Los datos serán:

1- tratados de manera lícita, leal y transparente en relación con el interesado
2- recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines
3- adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»)
4- exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan
5- mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; salvo los que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos

6- tratados de tal manera que se garantice una seguridad adecuada de los datos personales: protección contra tratamiento no autorizado o ilícito, pérdida, destrucción o daño

Art. 6. Licitud del tratamiento

El tratamiento deberá cumplir al menos una de las siguientes condiciones:

1- el interesado dio su consentimiento para el tratamiento de sus datos personales
2- el tratamiento es necesario para:
    a. la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales o;
    b. el cumplimiento de una obligación legal aplicable al responsable del tratamiento o;
    c. proteger intereses vitales del interesado o de otra persona física o;
    d. el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento o;
    e. la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero

Art. 7. Condiciones para el consentimiento

1. El responsable deberá ser capaz de demostrar que el interesado consintió el tratamiento de sus datos personales
2. La solicitud de consentimiento se presentará de forma clara, inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo.
3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. Será tan fácil retirar el consentimiento como darlo.
4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta si se supedita la ejecución de un contrato al consentimiento al tratamiento de datos que no son necesarios para la ejecución de dicho contrato.

Art. 8. Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información

1- El tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años
2- Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó
3- El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño

Art. 9. Tratamiento de categorías especiales de datos personales

1- Está prohibido cualquier tratamiento de datos personales que revele:
    a. Origen étnico o racial

   b. Opinión política
   c. Convicción religiosa o filosófica
   d. Afiliación sindical
2- Además, está prohibido el tratamiento de:
   a. Datos genéticos
   b. Datos biométricos dirigidos a identificar de manera unívoca a una persona física
   c. Datos relativos a la salud o relativos a la vida sexual u orientación sexual de una persona física
3- Estas prohibiciones no serán de aplicación cuando:
   a. El interesado da su consentimiento de manera explícita para el tratamiento de dichos datos personales
   b. El tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social
   c. El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento
   d. El tratamiento es efectuado por cualquier organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados
   e. El tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos
   f. El tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial
   g. El tratamiento es necesario por razones de un interés público esencial
   h. el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social
   i. el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios
   j. el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos

Art. 10. Tratamiento de datos personales relativos a condenas e infracciones penales

1- El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados.
2- Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

Art. 11. Tratamiento que no requiere identificación

1- El responsable no está obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado, si el fin por el que trata los datos personales no requiere la identificación del interesado
2- Cuando el responsable sea capaz de demostrar que no está en condiciones de identificar al interesado, le informará en consecuencia, de ser posible

Capítulo III – Derechos del interesado

Sección 1. Transparencia y modalidades

Art. 12. Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado

1- El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño.
2- El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22 relativos al derecho de acceso, de rectificación, de supresión, a la limitación del tratamiento, obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento, derecho a la portabilidad de los datos, de oposición y decisiones individuales automatizadas).
3- El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes
4- Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará como máximo transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales
5- La información facilitada en la obtención de los datos personales, obteniéndose o no del interesado, así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. En caso de que las solicitudes sean infundadas o excesivas, el responsable del tratamiento podrá:
    a. cobrar un canon razonable en función de los costes administrativos
    b. negarse a actuar respecto de la solicitud

6- La información facilitada a los interesados en virtud de los artículos 13 y 14 (obtención de los datos personales, obtenidos o no del interesado) podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto.

Sección 2. Información y acceso a los datos personales

Art. 13. Información que deberá facilitarse cuando los datos personales se obtengan del interesado

Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento le facilitará toda la información relativa a:

1- la identidad y los datos de contacto del responsable (o representante)
2- los datos de contacto del delegado de protección de datos
3- los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento
4- cuando el tratamiento se base en el artículo 6, apartado 1, letra f) del RGPD, los intereses legítimos del responsable o de un tercero
5- los destinatarios o las categorías de destinatarios de los datos personales
6- Si procede, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión

Además, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información:

1- plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo
2- la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos
3- cuando el tratamiento esté basado en el consentimiento, explícito o no, para el tratamiento de sus datos personales, la existencia del derecho a retirar el consentimiento en cualquier momento
4- el derecho a presentar una reclamación ante una autoridad de control
5- si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos
6- la existencia de decisiones automatizas, incluida la elaboración de perfiles, y, al menos en tales casos, información significativa sobre la lógica aplicada e importancia y consecuencias previstas de dicho tratamiento

Por otro lado, Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará

al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente.

Art. 14. Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado

Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará la siguiente información:

1- la identidad y los datos de contacto del responsable y, en su caso, de su representante
2- los datos de contacto del delegado de protección de datos, en su caso
3- los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento
4- las categorías de datos personales de que se trate
5- los destinatarios o las categorías de destinatarios de los datos personales, en su caso
6- en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias mediante garantías adecuadas, normas corporativas vinculantes o cuando la transferencia sea necesaria para la ejecución de un contrato.

Además, para garantizar un tratamiento de datos leal y transparente, se facilitará:

1- el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo
2- cuando el tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, los intereses legítimos del responsable del tratamiento o de un tercero
3- la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos
4- cuando el tratamiento esté basado en el consentimiento general del interesado o explícito para uno o más fines específicos, la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada
5- el derecho a presentar una reclamación ante una autoridad de control
6- la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público
7- la existencia de decisiones automatizadas, incluida la elaboración de perfiles, además de información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado

Esta información será facilitada:

1- dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes
2- si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado
3- si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez

Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente

Todas estas acciones no serán aplicables cuando y en la medida en que:

1- el interesado ya disponga de la información
2- la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para tratamiento con fines de:
    a. archivo en interés publico
    b. investigación científica o histórica
    c. estadísticos
3- la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o
4- cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros

Art. 15. Derecho de acceso del interesado

El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

1- fines del tratamiento
2- categorías de datos personales de que se trate
3- destinatarios o categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales
4- el plazo previsto de conservación de los datos personales o los criterios utilizados para determinar este plazo
5- la existencia del derecho a la rectificación o supresión de datos personales o la limitación u oposición del tratamiento de datos personales relativos al interesado
6- el derecho a presentar una reclamación ante una autoridad de control
7- cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen

8- la existencia de decisiones automatizadas, incluida la elaboración de perfiles, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado

Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas relativas a la transferencia

El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento, sin afectar negativamente a los derechos y libertades de otros.

Sección 3. Rectificación y supresión

Art. 16. Derecho de rectificación

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan.

Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Art. 17. Derecho de supresión

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de sus datos personales.

El responsable del tratamiento estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

1- los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo
2- el interesado retire el consentimiento en que se basa el tratamiento, y este no se base en otro fundamento jurídico
3- el interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento
4- los datos personales hayan sido tratados ilícitamente
5- los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida
6- los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información a niños mayores de 16 años o menores de 16 años con autorización del titular de su patria potestad o tutela.

Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos

El derecho de supresión no será aplicable en los siguientes casos:

1- para ejercer el derecho a la libertad de expresión e información
2- para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros, el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable
3- por razones de interés público en el ámbito de la salud pública
4- con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, en la medida en que el derecho de supresión pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o para la formulación, el ejercicio o la defensa de reclamaciones

Art. 18. Derecho a la limitación del tratamiento

El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

1. el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos
2. el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso
3. el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones
4. el interesado se haya opuesto al tratamiento, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado

Una vez limitado el tratamiento de datos, éstos solo podrán ser objeto de tratamiento en los siguientes casos:

a. Para su conservación
b. Con el consentimiento del interesado
c. Para la formulación, ejercicio o la defensa de reclamaciones
d. Con miras a la protección de los derechos de otra persona física o jurídica
e. Por razones de interés público importante de la Unión o de un determinado Estado miembro

Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación

Art. 19. Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento

El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado.

El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

Art. 20. Derecho a la portabilidad de los datos

El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

1- el tratamiento esté basado en el consentimiento general o para fines explícitos del interesado, o en un contrato en el que el interesado es parte o la aplicación de medidas precontractuales
2- el tratamiento se efectúe por medios automatizados

El interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

El derecho a la portabilidad de los datos se entenderá sin perjuicio del derecho a supresión.

El derecho a la portabilidad de los datos se entenderá sin perjuicio del derecho a supresión. La portabilidad no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

El derecho a la portabilidad de los datos no afectará negativamente a los derechos y libertades de otros.

Sección 4. Derecho de oposición y decisiones individuales automatizadas

Art. 21. Derecho de oposición

El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento, incluida la elaboración de perfiles sobre la base de dichas disposiciones.

El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines

El derecho de oposición será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.

En el contexto de la utilización de servicios de la sociedad de la información, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas

Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos, el interesado tendrá derecho a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público

Art. 22. Decisiones individuales automatizadas, incluida la elaboración de perfiles

Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. Salvo si:

a. es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento
b. está autorizada por el Derecho de la Unión o de los Estados miembros
c. se basa en el consentimiento explícito del interesado

En a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

Sección 5. Limitaciones

Art. 23. Limitaciones

El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:

a. la seguridad del estado
b. defensa
c. seguridad pública

d. prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención
e. otros objetivos importantes de interés público general de la Unión o de un Estado miembro
f. protección de la independencia judicial y de los procedimientos judiciales
g. prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas
h. función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g)
i. protección del interesado o de los derechos y libertades de otros
j. ejecución de demandas civiles

Cualquier medida legislativa indicada en el apartado 1 contendrá como mínimo, en su caso, disposiciones específicas relativas a:

a. finalidad del tratamiento o de las categorías de tratamiento
b. categorías de datos personales de que se trate
c. alcance de las limitaciones establecidas
d. garantías para evitar accesos o transferencias ilícitos o abusivos
e. determinación del responsable o de categorías de responsables
f. plazos de conservación y las garantías aplicables habida cuenta de la naturaleza alcance y objetivos del tratamiento o las categorías de tratamiento
g. riesgos para los derechos y libertades de los interesados
h. derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta

Capítulo IV – Responsable del tratamiento y encargado del tratamiento

Sección 1. Obligaciones generales

Art. 24. Responsabilidad del responsable del tratamiento

Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento.

Dichas medidas se revisarán y actualizarán cuando sea necesario.

Además, cuando las medidas sean proporcionadas en relación con las actividades de tratamiento se incluirá, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

La adhesión a códigos de conducta aprobados o a un mecanismo de certificación podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

Art. 25. Protección de datos desde el diseño y por defecto

Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, las medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad.

Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

Art. 26. Corresponsables del tratamiento

Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el RGPD, en particular cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información.

Dicho acuerdo podrá designar un punto de contacto para los interesados.

El acuerdo reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.

Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables.

Art. 27. Representantes de responsables o encargados del tratamiento no establecidos en la Unión

Cuando un responsable o encargado no esté establecido en la Unión, el responsable o el encargado del tratamiento designará por escrito un representante en la Unión. Esto no será aplicable en los siguientes casos:

a. al tratamiento que sea ocasional
b. al tratamiento que no incluya el manejo a gran escala de categorías especiales de datos
c. al tratamiento de datos personales relativos a condenas e infracciones penales
d. al tratamiento que sea probable que entrañe un riesgo para los derechos y libertades de las personas físicas, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento
e. a las autoridades u organismos públicos

El representante estará establecido en uno de los Estados miembros en que estén los interesados cuyos datos personales se traten en el contexto de una oferta de bienes o servicios, o cuyo comportamiento esté siendo controlado.

El responsable o el encargado del tratamiento encomendará al representante que atienda, junto al responsable o al encargado, o en su lugar, a las consultas, en particular, de las autoridades de control y de los interesados, sobre todos los asuntos relativos al tratamiento, a fin de garantizar el cumplimiento de lo dispuesto en el RGPD.

La designación de un representante por el responsable o el encargado del tratamiento se entenderá sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable o encargado.

Art. 28. Encargado del tratamiento

Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del RGPD y garantice la protección de los derechos del interesado.

El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En el caso de ocurrir cualquier cambio previsto en la incorporación o sustitución de otros encargados, el encargado informará al responsable dando así al responsable la oportunidad de oponerse a dichos cambios.

El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Este contrato estipulará que le encargado:

a. tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado. En tal caso, el encargado

informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público

b. garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria
c. tomará todas las medidas necesarias respecto a la seguridad del tratamiento
d. respetara las condiciones establecidas por el RGPD a la hora de recurrir a otro encargado del tratamiento
e. asistirá al responsable, a través de medidas técnicas y organizativas apropiadas, con el fin de que este pueda cumplir con su obligación de responder a las solicitudes de los interesados
f. ayudará al responsable a garantizar el cumplimiento de las obligaciones de seguridad de los datos personales
g. a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros
h. pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones del encargado del tratamiento, así como para permitir y contribuir a la realización de auditorías por parte del responsable o de otro auditor autorizado por dicho responsable.

   El encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el RGPD u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento.

Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado

La adhesión del encargado del tratamiento a un código de conducta o a un mecanismo de certificación podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes.

Art. 29. Tratamiento bajo la autoridad del responsable o del encargado del tratamiento

El encargado del tratamiento y cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo podrán tratar dichos datos siguiendo instrucciones del responsable, a no ser que estén obligados a ello en virtud del Derecho de la Unión o de los Estados miembros.

Art. 30. Registro de las actividades de tratamiento

Cada responsable y representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

a. el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos
b. los fines del tratamiento
c. una descripción de las categorías de interesados y de las categorías de datos personales
d. las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales
e. las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en su caso, la documentación de garantías adecuadas
f. cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos
g. cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad

Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

a. el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos
b. las categorías de tratamientos efectuados por cuenta de cada responsable
c. en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en su caso, la documentación de garantías adecuadas
d. cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad

Estos registros constarán por escrito, inclusive en formato electrónico.

El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.

Dichas medidas no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales.

Art. 31. Cooperación con la autoridad de control

El responsable y el encargado del tratamiento y, en su caso, sus representantes cooperarán con la autoridad de control que lo solicite en el desempeño de sus funciones.

Sección 2. Seguridad de los datos personales

Art. 32. Seguridad del tratamiento

Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a. la seudonimización y el cifrado de datos personales
b. la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento
c. la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico
d. un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presenten los siguientes tratamientos de datos:

1- Destrucción
2- pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma
3- la comunicación o acceso no autorizados a dichos datos

La adhesión a un código de conducta o a un mecanismo de certificación podrá servir de elemento para demostrar el cumplimiento de los requisitos.

El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

Art. 33. Notificación de una violación de la seguridad de los datos personales a la autoridad de control

En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

La notificación de violación deberá:

a. describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados
b. comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información
c. describir las posibles consecuencias de la violación de la seguridad de los datos personales
d. describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas.

Art. 34. Comunicación de una violación de la seguridad de los datos personales al interesado

Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

Esta notificación se describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo:

a. comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información
b. describir las posibles consecuencias de la violación de la seguridad de los datos personales

c. describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Dicha comunicación al interesado no será necesaria si se cumple alguna de las condiciones siguientes:

a. el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado
b. el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado
c. suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

Sección 3. Evaluación de impacto relativa a la protección de datos y consulta previa

Art. 35. Evaluación de impacto relativa a la protección de datos

Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.

La evaluación de impacto relativa a la protección de los datos, se requerirá en particular en caso de:

a. evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar
b. tratamiento a gran escala de las categorías especiales de datos, o de los datos personales relativos a condenas e infracciones penales
c. observación sistemática a gran escala de una zona de acceso público.

La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos.

La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos.

La evaluación deberá incluir como mínimo:

a. una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento
b. una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad
c. una evaluación de los riesgos para los derechos y libertades de los interesados, y
d. las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el RGPD, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.

Art. 36. Consulta previa

El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.

Cuando la autoridad de control considere que el tratamiento previsto podría infringir el RGPD, en particular cuando el responsable no haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes.

Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto.

Cuando consulte a la autoridad de control, el responsable del tratamiento le facilitará la información siguiente:

a. en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial
b. los fines y medios del tratamiento previsto
c. las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el presente Reglamento
d. en su caso, los datos de contacto del delegado de protección de datos
e. la evaluación de impacto relativa a la protección de datos, y
f. cualquier otra información que solicite la autoridad de control.

Sección 4. Delegado de protección de datos

Art. 37. Designación del delegado de protección de datos

El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

a. el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial
b. las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o
c. las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales.

Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

El responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados miembros.

El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

Art. 38. Posición del delegado de protección de datos

El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.

El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del RGPD.

El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones.

El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

Art. 39. Funciones del delegado de protección de datos

El delegado de protección de datos tendrá como mínimo las siguientes funciones:

a. informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión o de los Estados miembros
b. supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes
c. ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación
d. cooperar con la autoridad de control
e. actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa, y realizar consultas, en su caso, sobre cualquier otro asunto.

El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Sección 5. Códigos de conducta y certificación

Art. 40. Códigos de conducta

Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del RGPD, como en lo que respecta a:

a. el tratamiento leal y transparente
b. los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos
c. la recogida de datos personales
d. la seudonimización de datos personales
e. la información proporcionada al público y a los interesados
f. el ejercicio de los derechos de los interesados

g. la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño
h. las medidas y procedimientos que atañen a la responsabilidad del responsable del tratamiento y a la protección de datos desde el diseño y por defecto y, las medidas para garantizar la seguridad del tratamiento
i. la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados
j. la transferencia de datos personales a terceros países u organizaciones internacionales, o
k. los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento

Los responsables o encargados a los que no se aplica el RGPD podrán adherirse también a códigos de conducta aprobados y que tengan validez general, a fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales.

El código de conducta contendrá mecanismos que permitan al organismo de supervisión, efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados de tratamiento que se comprometan a aplicarlo, sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes.

Art. 42. Certificación

Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados.

La certificación será voluntaria y estará disponible a través de un proceso transparente.

Capítulo V – Transferencias de datos personales a terceros países u organizaciones internacionales

Art. 45. Transferencias basadas en una decisión de adecuación

Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado.

Dicha transferencia no requerirá ninguna autorización específica.

Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:

a. el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos
b. la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y
c. los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

La Comisión publicará en el Diario Oficial de la Unión Europea y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado.

Art. 46. Transferencias mediante garantías adecuadas

A falta de decisión sobre la adecuación del nivel de protección, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

Estas garantías podrán ser aportadas por:

a. un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos
b. normas corporativas vinculantes
c. cláusulas tipo de protección de datos adoptadas por la Comisión de acuerdo al procedimiento del comité
d. cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión de acuerdo al procedimiento del comité

e. un código de conducta junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o
f. un mecanismo de certificación aprobado

Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas podrán igualmente ser aportadas, en particular, mediante:

a. cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o
b. disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

Art. 47. Normas corporativas vinculantes

La autoridad de control competente aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia, siempre que estas:

a. sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados
b. confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y
c. Se cumplan los siguientes elementos:
    1. la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros
    2. las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión
    3. su carácter jurídicamente vinculante, tanto a nivel interno como externo
    4. la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes
    5. los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros, y el derecho a obtener

una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes

6. la aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión
7. la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes
8. las funciones de todo delegado de protección de datos designado, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones
9. los procedimientos de reclamación
10. los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado.
11. los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control
12. los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control
13. el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta
14. los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes, y
15. la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

Art. 48. Transferencias o comunicaciones no autorizadas por el Derecho de la Unión

Cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional, como un tratado

de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro.

Art. 49. Excepciones para situaciones específicas

En ausencia de una decisión de adecuación, o de garantías adecuadas, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes:

a. el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas
b. la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado
c. la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica
d. la transferencia sea necesaria por razones importantes de interés público
e. la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones
f. la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento
g. la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

Cuando una transferencia no pueda basarse en una decisión de adecuación o mediante garantías adecuadas, incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo si:

1- no es repetitiva
2- afecta solo a un número limitado de interesados
3- es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado
4- y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales.

El responsable del tratamiento informará a la autoridad de control de la transferencia.

El responsable o el encargado del tratamiento documentarán en los registros de las actividades de tratamiento, la evaluación y las garantías apropiadas.

Capítulo VI – Autoridades de control independientes

Sección 1. Independencia

Art. 51. Autoridad de control

Se establecen las responsabilidades de la autoridad de control con el fin de supervisar la aplicación del RGPD.

Art. 52. Independencia

Se establece la independencia de la autoridad de control frente a cualquier otro ente o entidad y se fija el marco de actuación de una autoridad de control.

Art. 53. Condiciones generales aplicables a los miembros de la autoridad de control

Se establece el método de elección de los miembros de una autoridad de control

Art. 54. Normas relativas al establecimiento de la autoridad de control

Obligaciones de los Estados miembros respecto al establecimiento de la autoridad de control

Sección 2. Competencia, funciones y poderes

Art. 55. Competencia

Se establecen las competencias de las autoridades de control

Art. 56. Competencia de la autoridad de control principal

Se establecen las competencias de la autoridad de control principal

Art. 57. Funciones

Se establecen las funciones de las autoridades de control:

a. controlar la aplicación del RGPD y hacerlo aplicar
b. promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento. Las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención
c. asesorar al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento
d. promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del RGPD

e. previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud del RGPD y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados miembros
f. tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación, investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control
g. cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua con el fin de garantizar la coherencia en la aplicación y ejecución del RGPD
h. llevar a cabo investigaciones sobre la aplicación del RGPD, en particular basándose en información recibida de otra autoridad de control u otra autoridad pública
i. hacer un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales
j. adoptar las cláusulas contractuales tipo para un contrato u otro acto jurídico y de protección de datos
k. elaborar y mantener una lista relativa al requisito de la evaluación de impacto relativa a la protección de datos
l. ofrecer asesoramiento sobre las operaciones de tratamiento cuando una evaluación de impacto relativa a la protección de los datos muestre que el tratamiento entrañaría un alto riesgo
m. alentar la elaboración de códigos de conducta, y dictaminar y aprobar los códigos de conducta que den suficientes garantías
n. fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos, y aprobar los criterios de certificación
o. llevar a cabo, si procede, una revisión periódica de las certificaciones expedidas
p. elaborar y publicar los criterios para la acreditación de organismos de supervisión de los códigos de conducta y de organismos de certificación
q. efectuar la acreditación de organismos de supervisión de los códigos de conducta y de organismos de certificación
r. autorizar las cláusulas contractuales y disposiciones sobre garantías adecuadas
s. aprobar normas corporativas vinculantes de conformidad
t. contribuir a las actividades del Comité
u. llevar registros internos de las infracciones del RGPD y de las medidas adoptadas
v. desempeñar cualquier otra función relacionada con la protección de los datos personales.

Cada autoridad de control facilitará la presentación de las reclamaciones mediante medidas como un formulario de presentación de reclamaciones que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación.

El desempeño de las funciones de cada autoridad de control será gratuito para el interesado y, en su caso, para el delegado de protección de datos.

Art. 58. Poderes

Se establecen los poderes de investigación, correctivos y de autorización y consultivos de las autoridades de control:

Poderes de investigación:

a. ordenar al responsable y al encargado del tratamiento y, en su caso, al representante del responsable o del encargado, que faciliten cualquier información que requiera para el desempeño de sus funciones
b. llevar a cabo investigaciones en forma de auditorías de protección de datos
c. llevar a cabo una revisión de las certificaciones expedidas
d. notificar al responsable o al encargado del tratamiento las presuntas infracciones del RGPD
e. obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones
f. obtener el acceso a todos los locales del responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de conformidad con el Derecho procesal de la Unión o de los Estados miembros.

Poderes correctivos:

a. sancionar a todo responsable o encargado del tratamiento con una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el RGPD
b. sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el RGPD
c. ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del RGPD
d. ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del RGPD, cuando proceda, de una determinada manera y dentro de un plazo especificado
e. ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales
f. imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición
g. ordenar la rectificación o supresión de datos personales o la limitación de tratamiento y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales
h. retirar una certificación u ordenar al organismo de certificación que retire una certificación emitida u ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación

i. imponer una multa administrativa, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular
j. ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

Poderes de autorización y consultivos

a. asesorar al responsable del tratamiento conforme al procedimiento de consulta previa
b. emitir, por iniciativa propia o previa solicitud, dictámenes destinados al Parlamento nacional, al Gobierno del Estado miembro o, con arreglo al Derecho de los Estados miembros, a otras instituciones y organismos, así como al público, sobre cualquier asunto relacionado con la protección de los datos personales
c. autorizar el tratamiento en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública, si el Derecho del Estado miembro requiere tal autorización previa
d. emitir un dictamen y aprobar proyectos de códigos de conducta
e. acreditar los organismos de certificación
f. expedir certificaciones y aprobar criterios de certificación
g. adoptar las cláusulas tipo de protección de datos para demostrar el cumplimiento de las obligaciones establecidas al encargado o responsable del tratamiento y con arreglo al procedimiento de examen del comité
h. autorizar las cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional
i. autorizar los acuerdos administrativos contemplados entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.
j. aprobar normas corporativas vinculantes de conformidad

Capítulo VII – Cooperación y coherencia

Sección 1. Cooperación y coherencia

Art. 60. Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas

Se establecen las medidas de actuación para la cooperación entre la autoridad de control y las demás autoridades de control

Art. 61. Asistencia mutua

Se establece el marco para la asistencia entre autoridades de control y las medidas a tomar en respuesta de una petición de otra autoridad de control.

Art. 62. Operaciones conjuntas de las autoridades de control

Se establece el marco para las operaciones conjuntas entre autoridades de control, incluidas investigaciones conjuntas y medidas de ejecución conjuntas.

Sección 2. Coherencia

Art. 64. Dictamen del Comité

Se distribuyen las competencias entre el Comité y las autoridades de control, así como las medidas de comunicación entre los mismos a la hora de adoptar medidas.

Art. 65. Resolución de conflictos por el Comité

Se establece al Comité como órgano para resolver conflictos entre las autoridades de control principales y autoridades de control.

Art. 66. Procedimiento de urgencia

Se establece el marco de acción para la adopción de medidas provisionales para proteger los derechos y las libertades de interesados.

Sección 3 – Comité europeo de protección de datos

En esta sección se establecen las bases para la creación del Comité Europeo de Protección de Datos, su independencia frente a otros entes y administraciones, funciones, competencias, procedimiento, presidencia y funciones del presidente, secretaría y la confidencialidad de sus debates.

Capítulo VIII – Recursos, responsabilidad y sanciones

Art. 77. Derecho a presentar una reclamación ante una autoridad de control

Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si considera que el tratamiento de datos personales que le conciernen infringe el RGPD.

Art. 78. Derecho a la tutela judicial efectiva contra una autoridad de control

Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, toda persona física o jurídica tendrá derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna, no dé curso a una reclamación o no informe al interesado en el plazo de tres meses sobre el curso o el resultado de la reclamación presentada.

Las acciones contra una autoridad de control deberán ejercitarse ante los tribunales del Estado miembro en que esté establecida la autoridad de control.

Art. 79. Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento

Sin perjuicio de los recursos administrativos o extrajudiciales disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control, todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del RGPD han sido vulnerados como consecuencia de un tratamiento de sus datos personales.

Las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento.

Art. 80. Representación de los interesados

El interesado tendrá derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida con arreglo al Derecho de un Estado miembro, cuyos objetivos estatutarios sean de interés público y que actúe en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, para que presente en su nombre la reclamación, y ejerza en su nombre los derechos a presentar una reclamación ante una autoridad de control, a la tutela judicial efectiva contra una autoridad de control y a la tutela judicial efectiva contra un responsable o encargado del tratamiento.

Art. 81. Suspensión de los procedimientos

Se establece el procedimiento y casuística para la suspensión de procedimientos de cualquier índole.

Art. 82. Derecho a indemnización y responsabilidad

Se establecen las condiciones y requisitos para la petición de indemnización como consecuencia de una infracción del RGPD y se establecen las responsabilidades sobre y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el RGPD.

Art. 83. Condiciones generales para la imposición de multas administrativas

Se establecen las condiciones generales para la imposición de multas administrativas y las cuantías máximas para las infracciones del RGPD.

Capítulo IX – Disposiciones relativas a situaciones específicas de tratamiento

Se establecen condiciones generales para el tratamiento de datos específicos sobre los siguientes aspectos: libertad de expresión y de información, acceso del público a documentos oficiales, número nacional de identificación, ámbito laboral, garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, obligaciones de secreto y protección de datos de las iglesias y asociaciones religiosas.

Capítulo X – Actos delegados y actos de ejecución

Se establece el ejercicio de la delegación de poderes y procedimiento del comité de asistencia a la Comisión en la aplicación del RGPD.

Capítulo XI – Disposiciones finales

Se enmarca la posición del RGPD con respecto a la Directiva 95/46/CE, Directiva 2002/58/CE y acuerdos celebrados anteriormente. Se establece el plazo para la entrega de los informes de la Comisión, la revisión de otros actos jurídicos de la Unión en materia de protección de datos y la entrada en vigor y aplicación del RGPD.

Anexo VI. Plantillas para obtener consentimiento

En el presente anexo se recomiendan unas plantillas base desde los cuáles PLASMAC puede desarrollar las peticiones de consentimiento, ofrecer a los usuarios el ejercicio de sus derechos o plantillas básicas con el que desarrollar documentos relevantes como el aviso legal, la política de cookies, la política de privacidad o el contrato que relaciona PLASMAC con el profesional encargado con el tratamiento de los datos.

Por tanto, para un mejor entendimiento y funcionalidad del documento, hemos clasificado la información en 6 puntos:

1. *Derechos ARCO*
2. *Comunicaciones*
3. *Tratamiento de datos*
4. *Brechas de seguridad*
5. *Web*
6. *Contrato PLASMAC – profesional encargado del tratamiento de los datos*
7. *Menores*

1. Derechos ARCO

1.1. Derechos de acceso

1.1.1. Ejercicio del derecho de acceso

DATOS DEL RESPONSABLE DEL FICHERO

Nombre / razón social: _____, C.I.F./D.N.I. _____. Dirección de la Oficina / Servicio ante el que se ejercita el derecho de acceso: C/Plaza _____, nº____, C.P._____, Localidad _____, Provincia_____, Comunidad Autónoma _____.

DATOS DEL INTERESADO O REPRESENTANTE LEGAL

D./ Dª. _____, mayor de edad, con domicilio en la C/Plaza _____, nº_____, Localidad _____, Provincia _____, C.P._____, con D.N.I_____, del que acompaña copia, por medio del presente escrito ejerce el derecho de acceso, de conformidad con lo previsto en el artículo 15 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y en consecuencia,

SOLICITA,

Que se le facilite gratuitamente el derecho de acceso a sus ficheros en el plazo máximo de un mes a contar desde la recepción de esta solicitud, y que se remita por correo la información a la dirección arriba indicada en el plazo de diez días a contar desde la resolución estimatoria de la solicitud de acceso.

Asimismo, se solicita que dicha información comprenda, de modo legible e inteligible, los datos de base que sobre mi persona están incluidos en sus ficheros, los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los mismos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

En _____ a _____ de _____ de 20____

Firmado

1) Se trata de la petición de información sobre los datos personales incluidos en un tratamiento. Este derecho se ejerce ante el responsable del tratamiento (Organismo Público o entidad privada) que es quien dispone de los datos.
2) También podrá ejercerse a través de representación legal, en cuyo caso, además del DNI del interesado, habrá de aportarse DNI y documento acreditativo auténtico de la representación del tercero.

1.1.2. Respuesta a la solicitud de acceso a datos

Muy Sr./a. nuestro/a:

Recibida su solicitud de acceso a los datos personales que sobre su persona obran incorporados en ficheros automatizados de los que es responsable esta empresa, le informamos de lo siguiente:

Datos sobre su persona (Indicar los datos obrantes en el fichero):

Origen de los datos (Indicar si son datos obtenidos directamente del interesado o por comunicación de un tercero):

Comunicaciones realizadas (Indicar, en su caso, a qué terceros se han comunicado los datos):

Sin otro particular,

En _____ , a ___ de _____ de 20___

_____ (Firma y sello)

1.2. Derecho de rectificación

1.2.1. Ejercicio del derecho

DATOS DEL RESPONSABLE DEL FICHERO

Nombre / razón social: _____, C.I.F./D.N.I. _____. Dirección de la Oficina / Servicio ante el que se ejercita el derecho de acceso: C/Plaza _____, nº____, C.P._____, Localidad _____, Provincia_____, Comunidad Autónoma _____.

DATOS DEL INTERESADO O REPRESENTANTE LEGAL

D./ Dª. _____, mayor de edad, con domicilio en la C/Plaza _____, nº_____, Localidad _____, Provincia _____, C.P._____, con D.N.I_____, del que acompaña copia, por medio del presente escrito ejerce el derecho de acceso, de conformidad con lo previsto en el artículo 15 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y en consecuencia,

SOLICITA,

Que se proceda a acordar la rectificación de los datos personales sobre los cuales se ejercita el derecho, que se realice en el plazo de diez días a contar desde la recogida de esta solicitud, y que se me notifique de forma escrita el resultado de la rectificación practicada.

Que en caso de que se acuerde, dentro del plazo de diez días hábiles, que no procede acceder a practicar total o parcialmente las rectificaciones propuestas, se me comunique motivadamente a fin de, en su caso, solicitar la tutela de la Agencia Española de Protección de Datos, al amparo del citado Reglamento.

Que si los datos rectificados hubieran sido comunicados previamente se notifique al responsable del fichero la rectificación practicada, con el fin de que también éste proceda a hacer las correcciones oportunas para que se respete el deber de calidad de los datos a que se refiere el artículo 5 del mencionado Reglamento (UE) 2016/679.

En _____ a _____de _____de 20____

Firmado:

1.2.2. Respuesta a la solicitud de rectificación de datos

Muy Sr./a. nuestro/a:

Recibida su solicitud de rectificación de los datos personales que sobre su persona obran incorporados en ficheros automatizados de los que es responsable esta empresa, le informamos de lo siguiente:

Datos sobre su persona (indicar los datos obrantes en el fichero):

Origen de los datos (indicar si son datos obtenidos directamente del interesado o por comunicación de un tercero):

Comunicaciones realizadas (indicar, en su caso, a qué terceros se han comunicado los datos):

Sin otro particular,

En _____, a ___ de _____ de 20___

_____ (Firma y sello)

1.3. Derecho de supresión/cancelación

1.3.1. Ejercicio del derecho

DATOS DEL RESPONSABLE DEL FICHERO

Nombre / razón social: _____, C.I.F./D.N.I. _____. Dirección de la Oficina / Servicio ante el que se ejercita el derecho de acceso: C/Plaza _____, nº____, C.P._____, Localidad _____, Provincia_____, Comunidad Autónoma _____.

DATOS DEL INTERESADO O REPRESENTANTE LEGAL

D./ Dª. _____, mayor de edad, con domicilio en la C/Plaza _____, nº_____, Localidad _____, Provincia _____, C.P._____, con D.N.I_____, del que acompaña copia, por medio del presente escrito ejerce el derecho de acceso, de conformidad con lo previsto en el artículo 15 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y en consecuencia,

SOLICITA,

Que se proceda, sin dilación indebida y de manera gratuita[3], a la supresión de sus datos de carácter personales del solicitante que estén en posesión de PLASMAC en el plazo máximo de diez días a contar desde la recepción de esta solicitud.

Que se comunique al solicitante de forma escrita a la dirección arriba indicada la cancelación de los datos una vez realizada.

Que, en el caso de que el responsable del fichero considere que dicha cancelación no procede, lo comunique igualmente, de forma motivada y dentro del mismo plazo de diez días. Si PLASMAC se niega a atender la presenta solicitud, se interpondrá la oportuna reclamación ante la Agencia de Protección de Datos para iniciar el procedimiento de tutela de derechos.

En _____ a ____ de _____ de _____

Firmado

1.3.2. Respuesta a la solicitud de cancelación/supresión de datos

Muy Sr./a. nuestro/a:

Recibida su solicitud de cancelación a los datos personales que sobre su persona obran incorporados en ficheros automatizados de los que es responsable esta empresa, le informamos se ha procedido a su destrucción, cancelación o, en su defecto, al bloqueo por las causas legalmente establecidas.

Sin otro particular,

En _____, a ___ de _____ de 20___

_____ (Firma y sello)

1.4. Derecho de oposición

1.4.1. Ejercicio del derecho

DATOS DEL RESPONSABLE DEL FICHERO

Nombre / razón social: _____, C.I.F./D.N.I. _____. Dirección de la Oficina / Servicio ante el que se ejercita el derecho de acceso: C/Plaza _____, nº____, C.P._____, Localidad

_____

[3] Excepto en los casos en que se formulen solicitudes manifiestamente infundadas o excesivas, especialmente por repetitivas.

_____, Provincia_____, Comunidad Autónoma _____.

DATOS DEL INTERESADO O REPRESENTANTE LEGAL

D./ Dª. _____, mayor de edad, con domicilio en la C/Plaza _____, nº_____, Localidad _____, Provincia _____, C.P._____, con D.N.I_____, del que acompaña copia, por medio del presente escrito ejerce el derecho de acceso, de conformidad con lo previsto en el artículo 15 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y en consecuencia,

EXPONGO,

(describir la situación en la que se produce el tratamiento de sus datos personales y enumerar los motivos por los que se opone al mismo)

Para acreditar la situación descrita, acompaño una copia de los siguientes documentos:

(enumerar los documentos que adjunta con esta solicitud para acreditar la situación que ha descrito)

SOLICITO,

Que sea atendido mi ejercicio del derecho de oposición en los términos anteriormente expuestos.

En _____ a _____ de _____ de 20___

Firmado:

1.4.2. Respuesta a la solicitud de oposición de datos

Muy Sr./a. nuestro/a:

Recibida su solicitud de oposición respecto a la cesión de los datos personales que sobre su persona obran incorporados en ficheros automatizados de los que es responsable esta empresa, le informamos que no se ha procedido a la cesión de los mismos.

Sin otro particular,

En _____, a ___ de _____ de 20___

_____ (Firma y sello)

1.5. Derecho de limitación

1.5.1. Ejercicio del derecho

DATOS DEL RESPONSABLE DEL FICHERO

Nombre / razón social: _____, C.I.F./D.N.I. _____. Dirección de la Oficina / Servicio ante el que se ejercita el derecho de acceso: C/Plaza _____, nº____, C.P._____, Localidad _____, Provincia_____, Comunidad Autónoma _____.

DATOS DEL INTERESADO O REPRESENTANTE LEGAL

D./ Dª. _____, mayor de edad, con domicilio en la C/Plaza _____, nº_____, Localidad _____, Provincia _____, C.P._____, con D.N.I_____, del que acompaña copia, por medio del presente escrito ejerce el derecho de acceso, de conformidad con lo previsto en el artículo 15 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y en consecuencia,

SOLICITA,

Que se proceda, de manera gratuita[4] y en el plazo de diez días a la limitación del tratamiento de los datos por parte PLASMAC debido a que: (SELECCIONE LA CASILLA CORRESPONDIENTE)

- Los datos se limiten durante el plazo que permita al responsable verificar la exactitud de los datos

mientras el solicitante se encuentra en un procedimiento de rectificación.

- El solicitante se opone a la supresión de datos personales que están siendo tratados de manera ilícita y en su lugar se solicita la limitación de su uso;

- El solicitante se opone a la supresión de datos personales que el responsable ya no necesite para los fines del tratamiento y en su lugar se solicita la limitación de su uso;

- El solicitante se opone al tratamiento mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

Que se comunique al solicitante de forma escrita a la dirección arriba indicada tanto la limitación realizada como el levantamiento de la misma antes de ambas acciones se lleven a cabo.

_____

[4] Excepto en los casos en que se formulen solicitudes manifiestamente infundadas o excesivas, especialmente por repetitivas.

Que, en el caso de que el responsable del fichero considere que la limitación del tratamiento no procede, lo comunique al solicitante de forma motivada y dentro del plazo de un mes. Si el responsable se niegue a atender la presenta solicitud, se interpondrá la oportuna reclamación ante la Agencia Española de Protección de Datos para iniciar el procedimiento de tutela de derechos.

En _____, a ___ de _____ de 20___

_____ (Firma)

1.5.2. Respuesta a la solicitud de limitación de datos

Muy Sr./a. nuestro/a:

Recibida su solicitud de limitación respecto al tratamiento de los datos personales que sobre su persona obran incorporados en ficheros automatizados de los que es responsable esta empresa, le informamos que hemos procedido a restringir el acceso a los mismos así como a adoptar las medidas necesarias para evitar su tratamiento y cesión.

Sin otro particular,

En _____, a ___ de _____ de 20___

_____ (Firma y sello)

1.6. Derecho de portabilidad

1.6.1. Ejercicio del derecho

DATOS DEL RESPONSABLE DEL FICHERO

Nombre / razón social: _____, C.I.F./D.N.I. _____. Dirección de la Oficina / Servicio ante el que se ejercita el derecho de acceso: C/Plaza _____, nº____, C.P._____, Localidad _____, Provincia_____, Comunidad Autónoma _____.

DATOS DEL INTERESADO O REPRESENTANTE LEGAL

D./ Dª. _____, mayor de edad, con domicilio en la C/Plaza _____, nº_____, Localidad _____, Provincia _____, C.P._____, con D.N.I_____, del que acompaña copia, por medio del presente escrito ejerce el derecho de acceso, de conformidad con lo previsto en el artículo 15 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27

de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y en consecuencia,

SOLICITA,

Que se proceda, sin dilación indebida y de manera gratuita[5], a la portabilidad de datos de carácter personal del solicitante que estén en posesión de PLASMAC en el plazo máximo de un mes** a contar desde la recepción de esta solicitud.

Que se comunique al solicitante de forma escrita a la dirección arriba indicada, la portabilidad de dichos datos, una vez que esta haya sido realizada.

Que, en caso de que el responsable del fichero considere que dicha portabilidad no procede, lo comunique igualmente, de forma motivada y dentro del mismo plazo de un mes[6]. Si PLASMAC se niega a atender la presente solicitud, se interpondrá la oportuna reclamación ante la Agencia de Protección de Datos para iniciar el procedimiento de tutela de susodichos derechos.

En _____, a _ ___de _____ de 20 __

_____ (firmado)

1.6.2. Respuesta a la solicitud de portabilidad de datos

Muy Sr./a. nuestro/a:

Recibida su solicitud de portabilidad respecto a los datos personales que sobre su persona obran incorporados en ficheros automatizados de los que es responsable esta empresa, le informamos de que se ha procedido a la portabilidad de todos sus datos.

Sin otro particular,

En _____, a ___ de _____ de 20___

_____ (Firma y sello)

2. Comunicaciones

2.1. Consentimiento para la recepción de mailing por vía electrónica

De conformidad con el Reglamento (UE) 2016/679, de 27 de abril de 2016, o Reglamento General de Protección de Datos (RGPD), y con la Ley Orgánica 3/2018, de 5 diciembre

---

[5] *Excepto en los casos en que se formulen solicitudes manifiestamente infundadas o excesivas, especialmente por repetitivas.*
[6] *En aquellos casos más complejos se concede un plazo de tres meses, pero siempre informando dentro del primer mes de las razones para dicho retraso.*

de Protección de Datos Personales y garantía de los derechos digitales, le informamos que:

Le solicitamos que nos confirme su consentimiento expreso para recibir comunicaciones que pudieran ser de su interés, en relación a servicios sociales, vía correo electrónico o medios análogos.

❑ ACEPTO RECIBIR COMUNICACIONES ELECTRÓNICAS

2.2. Cláusula para incorporar a la plantilla de correo electrónico

Este mensaje va dirigido, de manera exclusiva, a su destinatario y puede contener información confidencial y sujeta al secreto profesional, cuya divulgación no está permitida por Ley.

En caso de haber recibido este mensaje por error, le rogamos que, de forma inmediata, nos lo comunique mediante correo electrónico remitido a nuestra atención y proceda a su eliminación, así como a la de cualquier documento adjunto al mismo.

Asimismo, le comunicamos que la distribución, copia o utilización de este mensaje, o de cualquier documento adjunto al mismo, cualquiera que fuera su finalidad, están prohibidas por la ley.

En aras del cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, puede ejercer los derechos de acceso, rectificación, cancelación, limitación, oposición y portabilidad de manera gratuita mediante correo electrónico a: _____ o bien en la dirección: _____.

2.3. Cláusula para incorporar a la plantilla de fax

La información transmitida en este telefax va dirigida únicamente a la persona o entidad que se muestra como destinatario y puede contener datos confidenciales o privilegiados. Toda revisión, retransmisión, diseminación u otro uso o acción al respecto por parte de personas o entidades distintas al destinatario está prohibida por Ley.

En caso de haber recibido este telefax por error, le rogamos que, de forma inmediata, nos lo comunique al número de teléfono _____ y proceda a su eliminación.

En aras del cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, puede ejercer los derechos de acceso, rectificación, cancelación, limitación, oposición y portabilidad de manera gratuita mediante correo electrónico a: _____ o bien en la dirección: _____.

2.4. Cláusula de comunicación a usuarios de información detallada de protección de datos

Estimado usuario por medio de la presente y de acuerdo al Reglamento General de Protección de Datos 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 (RGPD), le facilitamos la siguiente información detallada del tratamiento de datos personales:

Responsable del tratamiento:

Sus datos pasarán a formar parte de un fichero titularidad de _____, con CIF/NIF nº: _____ y domicilio social en: _____.

Finalidad del tratamiento:

Desarrollar y cumplir con las obligaciones previstas en el presente contrato. Sus datos serán conservados durante el periodo de _____.

Legitimación:

La legitimación para la recogida de sus datos se basa en el contrato suscrito con _____.

Destinarios:

Sus datos no serán cedidos para otras finalidades distintas a las anteriormente descritas.

Derechos:

Puede ejercer sus derechos de acceso, rectificación, cancelación, limitación, portabilidad y oposición al tratamiento de sus datos cuando se den determinadas circunstancias, en cuyo caso únicamente serán conservados para el cumplimiento de las obligaciones legalmente previstas.

Para ejercer los derechos anteriormente descritos deberá dirigirse a _____, con CIF/NIF nº: _____ y domicilio social en: _____.

De igual modo, le informamos de que la Agencia Española de Protección de Datos es el órgano competente destinado a la tutela de estos derechos.

Con la finalidad de mantener actualizados los datos, el usuario deberá comunicar cualquier cambio que se produzca sobre los mismos.

Compromiso de confidencialidad:

De igual modo, de acuerdo al artículo 32 del RGPD, relativo al deber de secreto profesional, _____ se compromete a guardar la confidencialidad de los datos de carácter personal, subsistiendo esta obligación con posterioridad a la finalización, por cualquier causa, de la relación entre Usted y _____
.

En _____, a ___ de _____ de 20___

_____ (Firma)

3. Tratamiento de datos

3.1. Informe análisis de riesgos

¿QUÉ ES?

Se trata de un estudio previo que se debe realizar con todo nuevo tratamiento de datos personales.

La principal finalidad es establecer los controles y medidas de seguridad adecuadas que garanticen las libertades y los derechos de las personas afectadas.

¿EN QUÉ CONSISTE?

En este informe se identifican los riesgos y amenazas a los que están expuestos los activos más importantes que guardan relación con el departamento, proceso, o sistema objeto del estudio. A continuación, se deberán desarrollar las soluciones o medidas correspondientes para mitigar y/o eliminar los riesgos detectados y decidir cuáles de ellas se van a aplicar.

DESCRIPCIÓN DE LOS TRATAMIENTOS

La descripción de los tratamientos sujetos al análisis de riesgos, permite conocer el ciclo de vida de los datos, el uso que se va a dar a los mismos y cualquier elemento que interviene en esa utilización.

Se debe determinar para cada tratamiento si es riesgo es bajo o alto. El riesgo será alto siempre que realicemos los siguientes tratamientos:

- Elaboración de perfiles de "aspectos relacionados con el desempeño del interesado en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, ubicación o movimientos".
- Toma de decisiones automatizada con efecto legal o similar (produzca exclusión o discriminación).
- Monitorizar o controlar a los interesados.
- Tratar categorías especiales de datos.
- Datos relativos a las personas vulnerables (menores, ancianos…).
- Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas (huella dactilar, reconocimiento facial…).
- Cuando el procesamiento en sí mismo "impide que los interesados ejerzan un derecho o utilicen un servicio o contrato".

NECESIDAD DEL INFORME

El Reglamento 679/2016 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en cuanto al tratamiento y la libre circulación de datos personales, en adelante, RGPD establece la necesidad de realizar un análisis de riesgos con la finalidad de implantar medidas de seguridad y control para garantizar los derechos y libertades de las personas.

Una descripción adecuada de las actividades de tratamiento es fundamental para poder garantizar los derechos y libertades de los interesados. La fase de diseño de un tratamiento define el flujo de los datos personales, así como todos los elementos que intervendrán a lo largo del mismo.

También es el momento adecuado para definir las medidas de control y seguridad para garantizar los derechos y libertades de los interesados con el objetivo de cumplir con el principio de responsabilidad proactiva y que un tratamiento se inicie respetando las exigencias de privacidad según el riesgo a la que está expuesto.

PRINCIPALES RIESGOS

Protección de la información:

- Integridad de los datos personales:
- Riesgo: Modificación o alteración de datos personales no intencionada
- Disponibilidad de los datos personales:
- Riesgo: Pérdida o borrado no intencionado de datos personales
- Confidencialidad de los datos personales:
- Riesgo: Acceso no autorizado a los datos personales

Riesgos asociados al cumplimiento:

- Garantizar el ejercicio de los derechos de los interesados:
- Riesgo: Ausencia de procedimientos para el ejercicio de derechos
- Garantizar los principios relativos al tratamiento:
- Riesgos: Ausencia de legitimidad para el tratamiento de los datos personales; Tratamiento ilícito de datos personales

MEDIDAS DE CONTROL PARA REDUCIR LOS RIESGOS

Modificación o alteración de datos personales no intencionada:

- Segregación de funciones mediante perfiles de acceso.
- Controles de monitorización de amenazas en red.

Pérdida o borrado no intencionado de datos personales:

- Copias de seguridad.
- Almacenamiento en dos ubicaciones diferentes.

Acceso no autorizado a los datos personales:

- Mecanismos de control de acceso

- Segmentación de la red

Ausencia de procedimientos para el ejercicio de derechos:

- Procedimientos y canales para el ejercicio de derechos

Ausencia de legitimidad para el tratamiento de los datos personales:

- Cláusulas informativas y base legitimadora para el tratamiento de datos

Tratamiento ilícito de datos personales:

- Monitorización del uso de datos personales

3.2. Análisis de riesgos

TIPOLOGÍA DE DATOS

¿Se van a tratar datos personales?

❑ Sí

❑ No

FINALIDADES DEL TRATAMIENTO

¿La recogida de los datos tiene como finalidad el tratamiento a gran escala?

Por favor, detalle los puntos indicados a continuación para poder analizar si se trata de un tratamiento a gran escala:

El número de sujetos afectados (es decir, cuantos interesados van a ser objeto de este tratamiento)

❑ de 0 a 10.000

❑ de 10.000 a 100.000

❑ + de 100.000

Las categorías de datos tratados:

❑ Datos especialmente protegidos

❑ Datos de carácter identificativo

❑ Características personales

❑ Circunstancias sociales

❑ Datos académicos y profesionales

❑ Detalles del empleo

❑ Información comercial

❑ Datos económicos, financieros y de seguro

❑ Transacciones de bienes y servicios

La duración del tratamiento:

❑ Instantáneo

❑ Días

❑ Semanas

❑ Meses

❑ Años

La extensión geográfica del tratamiento:

❑ Regional

❑ Nacional

❑ Internacional

¿La recogida de los datos tiene como finalidad la monitorización o evaluación sistemática y exhaustiva de aspectos personales? (tratamiento para monitorizar, observar y/o controlar a los interesados, a través del cual, se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables)

❑ Sí

❑ No

¿La recogida de los datos tiene como finalidad el tratamiento de datos especialmente protegidos?

❑ Ideología u opiniones políticas

❑ Afiliación sindical

❑ Religión u opiniones religiosas

❑ Creencias o creencias filosóficas

❑ Origen étnico o racial

❑ Datos relativos a salud

❑ Vida sexual u orientación sexual

❑ Datos de violencia de género y malos tratos

❑ Datos biométricos

❑ Datos genéticos que proporcionan una información única sobre la fisiología o la salud del

identificado obtenidas del análisis de una muestra biológica

❑ Datos solicitados para fines policiales sin consentimiento de las personas afectadas

❑ Datos relativos a condenas y delitos penales"

¿El tratamiento implica un contacto con los interesados de manera que, dicho contacto, pueda resultar intrusivo o se prevé el uso de tecnologías que se pueden percibir como especialmente intrusivas en la privacidad?

Por ejemplo, las llamadas telefónicas podrían considerarse intrusivas y la vigilancia electrónica, la minería de datos, la biometría, las técnicas genéticas o la geolocalización.

❑ Sí

❑ No

¿Se van a usar específicamente datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad (p.e.: menores de 14 años, ancianos, personas con riesgo de exclusión social)?

❑ Sí

❑ No

¿Se van a tratar datos personales para elaborar perfiles, categorizar/segmentar, hacer ratings/scoring o para la toma de decisiones?

Por ejemplo, la segmentación de clientes en base a sus datos personales con el objetivo de realizar comunicaciones comerciales

❑ Sí

❑ No

¿El tratamiento de los datos implica una toma de decisiones automatizada sin que haya ninguna persona que intervenga en la decisión o valore los resultados?

A modo de ejemplo, autorizar o denegar un tipo de producto a un cliente mediante un algoritmo automatizado sin que ningún gestor valore el resultado para confirmar las decisiones

❑ Sí

❑ No

¿Se enriquece la información de los interesados mediante la recogida de nuevas categorías de datos o se usan las existentes con nuevas finalidades que antes no se

contemplaban, en particular, si estas finalidades son más intrusivas o inesperadas para los afectados, o incluso pueda llegar a bloquear el disfrute de algún servicio?

Por ejemplo, usar la información contenida en ficheros externos de morosos como ASNEF

❑ Sí

❑ No

¿El tratamiento implica que un elevado número de personas tenga acceso a los datos personales

tratados?

❑ Sí

❑ No

¿Se van a tratar datos relativos a la observación de zonas de acceso público?

❑ Sí

❑ No

TECNOLOGÍAS EMPLEADAS PARA EL TRATAMIENTO

¿Se prevé el uso de tecnologías que se pueden percibir como inmaduras, de reciente creación o salida al mercado, cuyo alcance no puede ser previsto por el interesado de forma clara o razonable e implique elevado riesgo para el acceso no autorizado?

Por ejemplo, la combinación de tecnologías ya existentes, como el uso de dispositivos inteligentes de nueva creación y reconocimiento facial para aumentar la seguridad del acceso físico a las instalaciones, se considera una tecnología inmadura.

❑ Sí

❑ No

CESIONES DE DATOS Y TRANSFERENCIAS INTERNACIONALES DE DATOS

¿Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo? (en caso afirmativo detallar cuáles)

❑ Sí

❑ No

Nombre:

¿Se realizan transferencias internacionales de datos a países fuera de la Unión Europea y que no

cuenten con medidas de protección de datos de carácter personal similares a las establecidas por la Autoridad de Control? (en caso afirmativo detallar cuáles)

El siguiente listado contiene los países considerados seguros para las transferencias de datos: Andorra, Argentina, Canadá, Suiza, Islas Feroe, Guernsey, Israel, Isla de Man, Jersey, Nueva Zelanda, Uruguay.

❑ Sí

❑ No

Cuáles:

PERCEPCIÓN DE LA EXISTENCIA UN RIESGO ELEVADO POR PARTE DEL RESPONSABLE DE LA

ACTIVIDAD DE TRATAMIENTO

¿Este tratamiento puede conllevar una pérdida o alteración de la información?

❑ Sí

❑ No

¿Se utilizada documentación en papel para tratar datos personales?

❑ Sí

❑ No

En tal caso, indicar las medidas aplicadas:

❑ Se guarda bajo llave

❑ Se destruye de forma confidencial

❑ Se guarda con un registro de accesos

❑ Otros

TERCEROS QUE INTERVENGAN EN EL TRATAMIENTO

¿Interviene algún proveedor en el proceso?

❑ Sí

❑ No

En caso afirmativo, indicar su denominación social:

3.3. Registro de actividades de tratamiento

RESPONSABLE DEL TRATAMIENTO

Datos identificativos del Responsable del tratamiento: nombre, DNI/CIF, dirección, etc.

Datos identificativos del Delegado de Protección de Datos (si corresponde): nombre, DNI/CIF,

dirección, etc.

DESCRIPCIÓN DE LA ACTIVIDAD DE TRATAMIENTO

Actividad de tratamiento	Descripción de la actividad de tratamiento: Gestión de clientes, Gestión de asociados, RRHH, etc

Finalidad	Finalidad de la actividad de tratamiento
Interesados	Listado de personas y usuarios interesados y/o afectados por la actividad de tratamiento
Categorías de datos	Tipos de datos gestionados en el tratamiento de datos: Datos identificativos, datos financieros, datos de salud, otros.

TRANSFERENCIAS INTERNACIONALES Y CESIONES

Cesiones	Identificación de los destinatarios de las cesiones Previstas.
Transferencias previstas	Detalle de las transferencias internacionales de datos previstas: países, legitimación, etc.
Periodo de conservación	Plazo previsto para la conservación de la información.

CICLO DE VIDA DE LA ACTIVIDAD DE TRATAMIENTO

1. CAPTURA DE LOS DATOS

Actividades del proceso	Detalle de los procesos que intervienen en la captura de la información: formularios, encuestas, etc.
Datos tratados	Tipos de datos que se recopilan.
Intervinientes	Personas y usuarios que intervienen en la recogida de la información.
Tecnologías	Tecnología que interviene en la recogida de la información.

2. ALMACENAMIENTO DE LOS DATOS

Actividades del proceso	Detalle del proceso de almacenamiento de la información
Datos tratados	Tipos de datos que se almacenan.
Intervinientes	Personas y usuarios que intervienen en el almacenamiento de la información.
Tecnologías	Tecnología que interviene en el almacenamiento de la información.

3. USO Y TRATAMIENDO DE LOS DATOS

Actividades del proceso	Detalle de los diferentes usos de la información.
Datos tratados	Tipos de datos que se gestionan.
Intervinientes	Personas y usuarios que intervienen en la gestión de la información.
Tecnologías	Tecnología que interviene en el uso de la información.

4. TRANSFERENCIAS Y CESIONES PREVISTAS

Actividades del proceso	Detalle del proceso de cesión de la información.
Datos tratados	Tipos de datos que se ceden.
Intervinientes	Personas y usuarios que intervienen.
Tecnologías	Tecnología que interviene en la cesión de la información.

5. DESTRUCCIÓN

Actividades del proceso	Detalle del proceso de destrucción de la información.
Datos tratados	Tipos de datos que se destruyen.
Intervinientes	Personas y usuarios que intervienen.
Tecnologías	Tecnología que interviene en la destrucción de la información.

MEDIDAS DE SEGURIDAD DEL RESPONSABLE DE TRATAMIENTO

Medidas de seguridad	Referencia a las medidas de seguridad implantadas. Hacer referencia a diferentes procedimientos existentes en la estructura.

ENCARGADO DEL TRATAMIENTO

1. DATOS DEL ENCARGADO DE TRATAMIENTO

Encargado del tratamiento	Datos identificativos del encargado de tratamiento: nombre DNI/CIF, dirección, etc.
Delegado de Protección de Datos	Datos identificativos del DPD: nombre, DNI/CIF dirección, etc.

2. DESCRIPCIÓN DE LOS TRATAMIENTOS DE DATOS

Encargado del tratamiento	Datos identificativos del encargado de tratamiento: nombre DNI/CIF, dirección, etc.
Categorías de tratamiento	Tipos de datos gestionados en el tratamiento de datos: Datos identificativos, datos financieros, datos de salud, otros

3. TRANSFERENCIAS Y CESIONES

Transferencias y cesiones previstas	Identificación de los destinatarios de las cesiones previstas Detalle de las transferencias internacionales de datos previstas: países, legitimación, etc

4. MEDIDAS DE SEGURIDAD DEL ENCARGADO DE TRATAMIENTO

Medidas de seguridad	Referencia a las medidas de seguridad implantadas. Hacer referencia a diferentes procedimientos existentes en la estructura.

4. Brechas de seguridad

4.1. Notificación de brecha de seguridad a la AEPD

1. Nombre del proveedor:

2. Identidad y datos de contacto del responsable de protección de datos:

3. Indicación de si se trata de una primera o segunda notificación Información inicial sobre el caso de violación de datos personales (en su caso, complétese en notificaciones posteriores):

4. Fecha y hora del incidente (si se conocen; en caso necesario, puede efectuarse una estimación) y de detección del incidente:

5. Circunstancias en que se ha producido la violación de datos personales (por ejemplo, pérdida, robo, copia, etc.):

6. Naturaleza y contenido de los datos personales en cuestión:

7. Medidas técnicas y de organización que ha aplicado (o aplicará) el proveedor a los datos personales en cuestión:

8. Información suplementaria sobre el caso de violación de datos personales:

9. Resumen del incidente que ha causado la violación de datos personales (con indicación de la ubicación física de la violación y del soporte de almacenamiento):

10. Número de abonados o particulares afectados:

11. Posibles consecuencias y efectos negativos en los abonados o particulares:

12. Posible notificación adicional a los abonados o particulares:

13. Contenido de la notificación a los afectados:

14. Medios de comunicación utilizados:

15. Número de abonados o particulares a los que se ha remitido la notificación Posibles cuestiones de carácter transfronterizo:

16. Caso de violación de datos personales que afecta a abonados o particulares de otros Estados miembros:

17. Notificación a otras autoridades nacionales competentes:

En _____ a _____ de _____ de 20 __

Firma (Responsable del tratamiento o responsable de seguridad)

4.2. Notificación de brecha de seguridad a afectado

1. Nombre del proveedor:

2. Identidad y datos de contacto del responsable de protección de datos:

3. Resumen del incidente que ha causado la violación de datos personales:

4. Fecha estimada del incidente:

5. Naturaleza y contenido de los datos personales en cuestión:

6. Posibles consecuencias de la violación de datos personales para el abonado o particular afectado:

7. Circunstancias en que se ha producido la violación de datos personales:

8. Medidas adoptadas por el proveedor para subsanar la violación de datos personales:

9. Medidas recomendadas por el proveedor para paliar los posibles efectos negativos:

En _____ a _____ de _____ de 20__

Firma (Responsable del tratamiento o responsable de seguridad)

5. Web

5.1. Aviso legal

_____, provisto con NIF/CIF _____, dirección _____, no puede asumir ninguna responsabilidad derivada del uso incorrecto, inapropiado o ilícito de la información aparecida en la página de Internet de _____.

Con los límites establecidos en la ley, _____ no asume ninguna responsabilidad derivada de la falta de veracidad, integridad, actualización y precisión de los datos o informaciones que se contienen en sus páginas de Internet.

Los contenidos e información no vinculan a _____ ni constituyen opiniones, consejos o asesoramiento legal de ningún tipo pues se trata meramente de un servicio ofrecido con carácter informativo y divulgativo.

La página de Internet de _____ puede contener enlaces (links) a otras páginas de terceras partes que _____ no puede controlar. Por lo tanto, _____ no puede asumir responsabilidades por el contenido que pueda aparecer en páginas de terceros.

Los textos, imágenes, sonidos, animaciones, software y el resto de contenidos incluidos en este website son propiedad exclusiva de _____ o sus licenciantes. Cualquier acto de transmisión, distribución, cesión, reproducción, almacenamiento o comunicación pública total o parcial, debe contar con el consentimiento expreso de _____

Asimismo, para acceder a algunos de los servicios que _____ ofrece a través del website deberá proporcionar algunos datos de carácter personal. En cumplimiento de lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos le informamos que, mediante la cumplimentación de los presentes formularios, sus datos personales quedarán incorporados y serán tratados en los ficheros de _____ con el fin de poderle prestar

y ofrecer nuestros servicios así como para informarle de las mejoras del sitio Web. Asimismo, le informamos de la posibilidad de que ejerza los derechos de acceso, rectificación, cancelación y oposición de sus datos de carácter personal, manera gratuita mediante email a _____ o en la dirección _____.

5.2. Política de cookies

El sitio web www.miweb.es utiliza cookies propias y de terceros para recopilar información que ayuda a optimizar su visita a sus páginas web. No se utilizarán las cookies para recoger información de carácter personal. Usted puede permitir su uso o rechazarlo, también puede cambiar su configuración siempre que lo desee. Encontrará más información en nuestra Política de Cookies.

Aceptar cookies	Modificar su configuración

NOTA - Si hace clic en el botón:

- "Aceptar cookies": continúa navegando por la página web y el mensaje puede desaparecer.

- "Modificar su configuración": accede al apartado "Cómo modificar la configuración de las cookies" del siguiente texto.

NOTA

En las siguientes páginas exponemos el texto legal para incluir en su página web advirtiendo del uso de cookies, en este caso sólo las de Google Analytics que suponemos que podrán utilizar.

En caso de que utilicen otras cookies, deben ofrecer información sobre la utilización de las cookies que se van a instalar y, en su caso, indicar los fines del tratamiento de los datos personales que se llevará a cabo a través de ellas. Por ejemplo: "cookie PHPSESSID – permite al usuario visualizar la página web e interactuar con ella".

También es necesario que incluyan un aviso como el del ejemplo al entrar en la página web, antes de que se le instalen las cookies al usuario.

5.2.1. Texto legal para incluir en la web

Política de cookies

_____(PLASMAC)_____ informa acerca del uso de las cookies en su página web: *www.plataforma-plasmac.es*

¿Qué son las cookies?

Las cookies son archivos que se pueden descargar en su equipo a través de las páginas web. Son herramientas que tienen un papel esencial para la prestación de numerosos servicios de la sociedad de la información. Entre otros, permiten a una página web almacenar y recuperar información sobre los hábitos de navegación de un usuario o de

su equipo y, dependiendo de la información obtenida, se pueden utilizar para reconocer al usuario y mejorar el servicio ofrecido.

Tipos de cookies

Según quien sea la entidad que gestione el dominio desde donde se envían las cookies y trate los datos que se obtengan se pueden distinguir dos tipos:

- Cookies propias: aquéllas que se envían al equipo terminal del usuario desde un equipo o dominio gestionado por el propio editor y desde el que se presta el servicio solicitado por el usuario.
- Cookies de terceros: aquéllas que se envían al equipo terminal del usuario desde un equipo o dominio que no es gestionado por el editor, sino por otra entidad que trata los datos obtenidos través de las cookies.

En el caso de que las cookies sean instaladas desde un equipo o dominio gestionado por el propio editor, pero la información que se recoja mediante éstas sea gestionada por un tercero, no pueden ser consideradas como cookies propias.

Existe también una segunda clasificación según el plazo de tiempo que permanecen almacenadas en el navegador del cliente, pudiendo tratarse de:

- Cookies de sesión: diseñadas para recabar y almacenar datos mientras el usuario accede a una página web. Se suelen emplear para almacenar información que solo interesa conservar para la prestación del servicio solicitado por el usuario en una sola ocasión (p.e. una lista de productos adquiridos).
- Cookies persistentes: los datos siguen almacenados en el terminal y pueden ser accedidos y tratados durante un periodo definido por el responsable de la cookie, y que puede ir de unos minutos a varios años.

Por último, existe otra clasificación con cinco tipos de cookies según la finalidad para la que se traten los datos obtenidos:

- Cookies técnicas: aquellas que permiten al usuario la navegación a través de una página web, plataforma o aplicación y la utilización de las diferentes opciones o servicios que en ella existan como, por ejemplo, controlar el tráfico y la comunicación de datos, identificar la sesión, acceder a partes de acceso restringido, recordar los elementos que integran un pedido, realizar el proceso de compra de un pedido, realizar la solicitud de inscripción o participación en un evento, utilizar elementos de seguridad durante la navegación, almacenar contenidos para la difusión de vídeos o sonido o compartir contenidos a través de redes sociales.
- Cookies de personalización: permiten al usuario acceder al servicio con algunas características de carácter general predefinidas en función de una serie de criterios en el terminal del usuario como por ejemplo serian el idioma, el tipo de navegador a través del cual accede al servicio, la configuración regional desde donde accede al servicio, etc.

- Cookies de análisis: permiten al responsable de las mismas, el seguimiento y análisis del comportamiento de los usuarios de los sitios web a los que están vinculadas. La información recogida mediante este tipo de cookies se utiliza en la medición de la actividad de los sitios web, aplicación o plataforma y para la elaboración de perfiles de navegación de los usuarios de dichos sitios, aplicaciones y plataformas, con el fin de introducir mejoras en función del análisis de los datos de uso que hacen los usuarios del servicio.
- Cookies publicitarias: permiten la gestión, de la forma más eficaz posible, de los espacios publicitarios.
- Cookies de publicidad comportamental: almacenan información del comportamiento de los usuarios obtenida a través de la observación continuada de sus hábitos de navegación, lo que permite desarrollar un perfil específico para mostrar publicidad en función del mismo.
- Cookies de redes sociales externas: se utilizan para que los visitantes puedan interactuar con el contenido de diferentes plataformas sociales (facebook, youtube, twitter, linkedIn, etc..) y que se generen únicamente para los usuarios de dichas redes sociales. Las condiciones de utilización de estas cookies y la información recopilada se regulan por la política de privacidad de la plataforma social correspondiente.

Desactivación y eliminación de cookies

Tienes la opción de permitir, bloquear o eliminar las cookies instaladas en tu equipo mediante la configuración de las opciones del navegador instalado en su equipo. Al desactivar cookies, algunos de los servicios disponibles podrían dejar de estar operativos. La forma de deshabilitar las cookies es diferente para cada navegador, pero normalmente puede hacerse desde el menú Herramientas u Opciones. También puede consultarse el menú de Ayuda del navegador dónde puedes encontrar instrucciones. El usuario podrá en cualquier momento elegir qué cookies quiere que funcionen en este sitio web.

Puede usted permitir, bloquear o eliminar las cookies instaladas en su equipo mediante la configuración de las opciones del navegador instalado en su ordenador:

- *Microsoft Internet Explorer o Microsoft Edge*: http://windows.microsoft.com/es-es/windows-vista/Block-or-allow-cookies
- *Mozilla Firefox*: http://support.mozilla.org/es/kb/impedir-que-los-sitios-web-guarden-sus-preferencia
- *Chrome*: https://support.google.com/accounts/answer/61416?hl=es
- *Safari*: http://safari.helpmax.net/es/privacidad-y-seguridad/como-gestionar-las-cookies/
- *Opera*: http://help.opera.com/Linux/10.60/es-ES/cookies.html

Además, también puede gestionar el almacén de cookies en su navegador a través de herramientas como las siguientes:

- *Ghostery:* www.ghostery.com/
- *Your online choices:* www.youronlinechoices.com/es/

Cookies utilizadas en *www.plataforma-plasmac.es*

A continuación, se identifican las cookies que están siendo utilizadas en este portal, así como su tipología y función:

Cookie	Descripción

Aceptación de la Política de cookies

www. plataforma-plasmac.es asume que usted acepta el uso de cookies. No obstante, muestra información sobre su Política de cookies en la parte inferior o superior de cualquier página del portal con cada inicio de sesión con el objeto de que usted sea consciente.

Ante esta información es posible llevar a cabo las siguientes acciones:

- *Aceptar cookies*. No se volverá a visualizar este aviso al acceder a cualquier página del portal durante la presente sesión.
- *Cerrar*. Se oculta el aviso en la presente página.
- *Modificar su configuración*. Podrá obtener más información sobre qué son las cookies, conocer la Política de cookies de www.miweb.es y modificar la configuración de su navegador.

5.3. Política de privacidad

Protección de datos de carácter personal según la LOPDGDD

_____, en aplicación de la normativa vigente en materia de protección de datos de carácter personal, informa que los datos personales que se recogen a través de los formularios del Sitio web:

_____, se incluyen en los ficheros automatizados específicos de usuarios de los servicios de _____.

La recogida y tratamiento automatizado de los datos de carácter personal tiene como finalidad el mantenimiento de la relación comercial y el desempeño de tareas de información, formación, asesoramiento y otras actividades propias de _____.

Estos datos únicamente serán cedidos a aquellas entidades que sean necesarias con el único objetivo de dar cumplimiento a la finalidad anteriormente expuesta.

_____ adopta las medidas necesarias para garantizar la seguridad, integridad y confidencialidad de los datos conforme a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a

la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos.

El usuario podrá en cualquier momento ejercitar los derechos de acceso, oposición, rectificación y cancelación reconocidos en el citado Reglamento (UE). El ejercicio de estos derechos puede realizarlo el propio usuario a través de email a: _____ o en la dirección: _____.

El usuario manifiesta que todos los datos facilitados por él son ciertos y correctos, y se compromete a mantenerlos actualizados, comunicando los cambios a _____.

Finalidad del tratamiento de los datos personales:

¿Con qué finalidad trataremos tus datos personales?

En PLASMAC, trataremos tus datos personales recabados a través del Sitio Web: www.plataforma-plasmac.es, con las siguientes finalidades:

1. En caso de contratación de los bienes y servicios ofertados a través de _____, para mantener la relación contractual, así como la gestión, administración, información, prestación y mejora del servicio.
2. Envío de información solicitada a través de los formularios dispuestos en _____.
3. Remitir boletines (newsletters), así como comunicaciones comerciales de promociones y/o publicidad de _____ y del sector.

Te recordamos que puedes oponerte al envío de comunicaciones comerciales por cualquier vía y en cualquier momento, remitiendo un correo electrónico a la dirección indicada anteriormente.

Los campos de dichos registros son de cumplimentación obligatoria, siendo imposible realizar las finalidades expresadas si no se aportan esos datos.

¿Por cuánto tiempo se conservan los datos personales recabados?

Los datos personales proporcionados se conservarán mientras se mantenga la relación comercial o no solicites su supresión y durante el plazo por el cuál pudieran derivarse responsabilidades legales por los servicios prestados.

Legitimación:

El tratamiento de tus datos se realiza con las siguientes bases jurídicas que legitiman el mismo:

1. La solicitud de información y/o la contratación de los servicios de _____, cuyos términos y condiciones se pondrán a tu disposición en todo caso, de forma previa a una eventual contratación.
2. El consentimiento libre, específico, informado e inequívoco, en tanto que te informamos poniendo a tu disposición la presente política de privacidad que,

tras la lectura de la misma, en caso de estar conforme, puedes aceptar mediante una declaración o una clara acción afirmativa, como el marcado de una casilla dispuesta al efecto.

En caso de que no nos facilites tus datos o lo hagas de forma errónea o incompleta, no podremos atender tu solicitud, resultando del todo imposible proporcionarte la información solicitada o llevar a cabo la contratación de los servicios.

Destinatarios:

Los datos no se comunicarán a ningún tercero ajeno a _____, salvo obligación legal.

Como encargados de tratamiento, tenemos contratados a los siguientes proveedores de servicios, habiéndose comprometido al cumplimiento de las disposiciones normativas, de aplicación en materia de protección de datos, en el momento de su contratación:

- (ENCARGADO) _____, con domicilio en _____, NIF/CIF nº _____, presta servicios de _____.
    - Puede consultar la política de privacidad y demás aspectos legales de la compañía en el siguiente enlace:
- (ENCARGADO) _____, con domicilio en _____, NIF/CIF nº _____, presta servicios de _____.
    - Puede consultar la política de privacidad y demás aspectos legales de la compañía en el siguiente enlace:

Datos recopilados por usuarios de los servicios

En los casos en que el usuario incluya ficheros con datos de carácter personal en los servidores de alojamiento compartido, _____no se hace responsable del incumplimiento por parte del usuario del RGPD.

Propiedad intelectual del software

El usuario debe respetar los programas de terceros puestos a su disposición por _____, aun siendo gratuitos y/o de disposición pública.

___(PLASMAC)_____dispone de los derechos de explotación y propiedad intelectual necesarios del software.

Para toda actuación que exceda del cumplimiento del servicio, el usuario necesitará autorización por escrito por parte de _____(PLASMAC)_____, quedando prohibido al usuario acceder, modificar, visualizar la configuración, estructura y ficheros de los servidores propiedad de _____(PLASMAC)_____, asumiendo la responsabilidad civil y penal derivada de cualquier incidencia que se pudiera producir

en los servidores y sistemas de seguridad como consecuencia directa de una actuación negligente o maliciosa por su parte.

Propiedad intelectual de los contenidos alojados

Se prohíbe el uso contrario a la legislación sobre propiedad intelectual de los servicios prestados por _____(PLASMAC)_____ y, en particular de:

- La utilización que resulte contraria a las leyes españolas o que infrinja los derechos de terceros.
- La publicación o la transmisión de cualquier contenido que, a juicio de ____(PLASMAC)____, resulte violento, obsceno, abusivo, ilegal, racial, xenófobo o difamatorio.
- Los cracks, números de serie de programas o cualquier otro contenido que vulnere derechos de la propiedad intelectual de terceros.
- La recogida y/o utilización de datos personales de otros usuarios sin su consentimiento expreso o contraviniendo lo dispuesto en 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 los mismos.
- La utilización del servidor de correo del dominio y de las direcciones de correo electrónico para el envío de correo masivo no deseado.

El usuario es responsable respecto a las leyes y reglamentos en vigor y las reglas que tienen que ver con el funcionamiento del servicio online, derechos de autor, mantenimiento del orden público, así como principios universales de uso de Internet.

El usuario indemnizará a _____(PLASMAC)_____ por los gastos que generara la imputación de _____(PLASMAC)_____ en alguna causa cuya responsabilidad fuera atribuible al usuario, incluidos honorarios y gastos de defensa jurídica, incluso en el caso de una decisión judicial no definitiva.

Protección de la información alojada

_____(PLASMAC)_____ realiza copias de seguridad de los contenidos alojados en sus servidores, sin embargo, no se responsabiliza de la pérdida o el borrado accidental de los datos por parte de los usuarios. De igual manera, no garantiza la reposición total de los datos borrados por los usuarios, ya que los citados datos podrían haber sido suprimidos y/o modificados durante el periodo del tiempo transcurrido desde la última copia de seguridad.

Los servicios ofertados, excepto los servicios específicos de backup, no incluyen la reposición de los contenidos conservados en las copias de seguridad realizadas por _____, cuando esta pérdida sea imputable al usuario; en este caso, se determinará una tarifa acorde a la complejidad y volumen de la recuperación, siempre previa aceptación del usuario.

La reposición de datos borrados sólo está incluida en el precio del servicio cuando la pérdida del contenido sea debida a causas atribuibles a _____.

5.4. Ejemplo de formulario en web

6. Contrato PLASMAC – profesional encargado del tratamiento de los datos

Se presenta un contrato tipo entre un responsable de los datos (rol de PLASMAC) y un encargado del tratamiento de los datos:

REUNIDOS

De una parte, Don_____provisto de DNI nº_____actuando como representante legal de_____con domicilio en_____y CIF nº _____en adelante RESPONSABLE DEL FICHERO.

De otra parte, Don_____provisto de DNI nº_____actuando como legal representante de NOMBRE DEL PROVEEDOR, con domicilio en_____y CIF nº en adelante ENCARGADO DEL TRATAMIENTO.

Ambas partes se reconocen mutuamente la capacidad legal suficiente para suscribir este contrato de encargo de tratamiento de datos personales y para quedar obligadas en la representación en que respectivamente actúan, en los términos convenidos en él. A tal fin,

MANIFIESTAN

1. Que ambas partes se encuentran vinculadas por una relación contractual de carácter mercantil para la prestación de____ (en adelante SERVICIO).

2. Que para la prestación de dicho servicio es necesario que el ENCARGADO DEL TRATAMIENTO tenga acceso y realice tratamientos de datos de carácter personal de los _____ responsabilidad del RESPONSABLE DEL FICHERO, por lo que asume las funciones y obligaciones que el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, estipula para los Encargados de Tratamiento
3. Ambas partes reconocen cumplir con todas las obligaciones derivadas de la normativa comunitaria y nacional en materia de protección de datos, en especial las relativas al derecho de información, consentimiento y deber de secreto, y a la adopción de las medidas de seguridad técnicas y organizativas que garanticen la seguridad de los datos personales
4. Que, en cumplimiento del artículo 28 del RGPD, ambas partes de forma libre y espontánea voluntad acuerdan regular este acceso y tratamiento de datos de carácter personal de conformidad con las siguientes:

ESTIPULACIONES

PRIMERO: OBJETO DEL CONTRATO

Mediante las presentes cláusulas se habilita a la entidad ENCARGADA DE TRATAMIENTO, para tratar por cuenta del, RESPONSABLE DEL TRATAMIENTO, los datos de carácter personal necesarios para prestar el servicio anteriormente descrito.

SEGUNDO: IDENTIFICACIÓN DE LA INFORMACIÓN AFECTADA

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el RESPONSABLE DEL TRATAMIENTO, pone a disposición del ENCARGADO DEL TRATAMIENTO, la

información que se describe a continuación:

- _____
- _____

TERCERO: DURACIÓN

El presente acuerdo tiene una duración de _____

Una vez finalice el presente contrato, el ENCARGADO DE TRATAMIENTO debe suprimir/devolver al RESPONSABLE, o devolver a otro encargado que designe el RESPONSABLE los datos personales y suprimir cualquier copia que esté en su poder.

CUARTO: OBLIGACIONES DEL ENCARGADO DE TRATAMIENTO

El ENCARGADO DEL TRATAMIENTO y todo su personal se obliga a:

1-. Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

2-. Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento. Si el ENCARGADO DEL TRATAMIENTO considera que alguna de las instrucciones infringe el Reglamento (UE) 2016/679 o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.

3-. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga[7]:

_____

[7] NOTA: Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, salvo que el

A. El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.

B. Las categorías de tratamientos efectuados por cuenta de cada responsable.

C. En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del Reglamento (UE) 2016/679, la documentación de garantías adecuadas.

D. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:

- La seudoanimización y el cifrado de datos personales.
- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

4-. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles. El encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación. Si el encargado debe transferir datos personales a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

5. Subcontratación.

---

tratamiento que realice pueda suponer un riesgo para los derechos y las libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1 del Reglamento (UE) 2016/679, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 de dicho Reglamento.

(Escoger una de las opciones)

Opción A

No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del ENCARGADO. Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de 72 horas, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. **La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo establecido**. El subcontratista, que también tendrá la condición de ENCARGADO DEL TRATAMIENTO, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el ENCARGADO DEL TRATAMIENTO y las instrucciones que dicte el responsable.

Corresponde al ENCARGADO inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

Opción B

Se autoriza al ENCARGADO a subcontratar con la empresa _____ las prestaciones que comporten los tratamientos siguientes:_____.

Para subcontratar con otras empresas, el encargado debe comunicarlo por escrito al responsable, identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo de 72 horas.

El subcontratista, que también tiene la condición de ENCARGADO DEL TRATAMIENTO, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el ENCARGADO DEL TRATAMIENTO y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación, de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad…) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del sub-encargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

6-. El ENCARGADO DEL TRATAMIENTO deberá observar en todo momento, y en relación con los ficheros de datos de carácter personal a los que tuviera acceso o le

pudieren ser entregados por el Responsable, para la realización en cada caso de los trabajos y servicios que pudieren acordarse, el deber de confidencialidad y secreto profesional que, de conformidad con lo dispuesto en la normativa de Protección de Datos, subsistirá aun después de finalizar la relación de los trabajos encargados en relación con cualquier fichero así como, en su caso, tras la finalización por cualquier causa del presente contrato.

7-. Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente[8].

8-. Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

9-. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

10-. Asistir al responsable del tratamiento en la respuesta al ejercicio de los derechos de:

- Acceso, rectificación, supresión y oposición
- Limitación del tratamiento
- Portabilidad de datos
- A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

El ENCARGADO DEL TRATAMIENTO debe resolver, por cuenta del responsable, y dentro del plazo establecido, las solicitudes de ejercicio de los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, en relación con los datos objeto del encargo.

11-. Derecho de información

El ENCARGADO DEL TRATAMIENTO, en el momento de la recogida de los datos, debe facilitar la información relativa a los tratamientos de datos que se van a realizar. La redacción y el formato en que se facilitará la información se debe consensuar con el responsable antes del inicio de la recogida de los datos.

12-. Notificación de violaciones de la seguridad de los datos

[8] Si existe una obligación de confidencialidad de naturaleza estatutaria o legal (por ejemplo, abogados) deberá quedar constancia expresa de la naturaleza y extensión de esta obligación.

El ENCARGADO DEL TRATAMIENTO notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 72 horas, y a través de correo electrónico con confirmación de lectura, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia. No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

- Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
- El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
- Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.
- Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

(Escoger alguna o las dos opciones)[9]

Opción A

- Corresponde al RESPONSABLE DEL TRATAMIENTO comunicar las violaciones de la seguridad de los datos a la Autoridad de Protección de Datos y a los interesados.

La comunicación contendrá, como mínimo, la información siguiente:

- Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

[9] Pese a que la notificación de las violaciones de seguridad a la autoridad de control o a los interesados corresponde al responsable del tratamiento, en aquellos supuestos en que los datos se traten exclusivamente con los sistemas del encargado puede ser recomendable atribuir dichas funciones al encargado.

- Nombre y datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

- Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

- Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos. Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

Opción B

- Corresponde al ENCARGADO DEL TRATAMIENTO comunicar en el menor tiempo posible las violaciones de la seguridad de los datos a los interesados, cuando sea probable que la violación suponga un alto riesgo para los derechos y las libertades de las personas físicas.

La comunicación debe realizarse en un lenguaje claro y sencillo y deberá, como mínimo:

- Explicar la naturaleza de la violación de datos.

- Indicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.

- Describir las posibles consecuencias de la violación de la seguridad de los datos personales.

- Describir las medidas adoptadas o propuestas por el RESPONSABLE DEL TRATAMIENTO para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

13-. Dar apoyo al RESPONSABLE DEL TRATAMIENTO en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

14-. Dar apoyo al RESPONSABLE DEL TRATAMIENTO en la realización de las consultas previas a la autoridad de control, cuando proceda.

15-. Poner disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.

16-. Implantar las medidas de seguridad siguientes:

Todas aquellas necesarias para:

- Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

- Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

- Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

- Seudonimizar y cifrar los datos personales, en su caso.

17-. Designar un delegado de protección de datos y comunicar su identidad y datos de contacto al responsable.

18-. Destino de los datos:

(Escoger una de las 3 opciones siguientes)

Opción A

Devolver al RESPONSABLE DEL TRATAMIENTO los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación. La devolución debe comporta el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado. No obstante, el ENCARGADO puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

Opción B

Devolver al ENCARGADO que designe por escrito el RESPONSABLE DEL TRATAMIENTO, los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida prestación. La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por el encargado. No obstante, el ENCARGADO puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

Opción C

Destruir los datos, una vez cumplida la prestación. Una vez destruidos, el encargado debe certificar su destrucción por escrito y debe entregar el certificado al RESPONSABLE DEL TRATAMIENTO. No obstante, el ENCARGADO puede conservar una copia, con los datos debidamente boqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

QUINTO: OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

Corresponde al RESPONSABLE DEL TRATAMIENTO:

1-. Entregar al encargado los datos a los que se refiere la cláusula 2 de este documento.

2-. Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado.

3-. Realizar las consultas previas que corresponda.

4-. Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del Reglamento (UE) 2016/679 por parte del encargado.

5-. Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

SEXTO: RESPONSABILIDAD DEL ENCARGADO DE TRATAMIENTO

1-. El ENCARGADO DEL TRATAMIENTO será considerado responsable del tratamiento en el caso de que destine los datos a otra finalidad, los comunique o los utilice incumpliendo el presente contrato. En estos casos, el ENCARGADO DEL TRATAMIENTO responderá de las infracciones en que hubiera incurrido personalmente.

2.- El ENCARGADO DEL TRATAMIENTO indemnizará al RESPONSABLE DEL TRATAMIENTO por los daños y perjuicios, de cualquier naturaleza, que pudieran resultar del incumplimiento de las obligaciones contraídas en virtud del presente contrato.

3.- A título enunciativo, y no limitativo, dicha indemnización incluirá los daños morales e imagen, costes publicitarios o de cualquier otra índole que pudieran resultar para su reparación. El ENCARGADO DEL TRATAMIENTO, asimismo, deberá responder de cualquier indemnización que a resultas de su incumplimiento tuviera que satisfacer a terceros.

4.- La responsabilidad del ENCARGADO DEL TRATAMIENTO incluirá, además, el importe de cualquier sanción administrativa y/o resolución judicial condenatoria que pudiera resultar contra el RESPONSABLE DEL TRATAMIENTO, como resultado del incumplimiento del ENCARGADO DEL TRATAMIENTO de la normativa y de las obligaciones exigidas en el presente contrato. La indemnización comprenderá, además del importe de la sanción y/o resolución judicial, el de los intereses de demora, costas judiciales y el importe de la defensa del RESPONSABLE DEL TRATAMIENTO en cualquier proceso en el que pudiera resultar demandada por cualquiera de las causas anteriormente expuestas.

SÉPTIMO: CONTROLES Y AUDITORÍA

El RESPONSABLE DEL TRATAMIENTO, en su condición, se reserva el derecho de efectuar en cualquier momento los controles y auditorías que estime oportunos para comprobar el correcto cumplimiento por parte del ENCARGADO DEL TRATAMIENTO del presente contrato. Por su parte, el Encargado deberá facilitar al RESPONSABLE DEL TRATAMIENTO cuantos datos o documentos le requiera para el adecuado cumplimiento de dichos controles y auditorías.

OCHO: NOTIFICACIONES

1.- Cualquier notificación que se efectúe entre las partes se hará por escrito y será entregada personalmente o de cualquier otra forma que certifique la recepción por la parte notificada.

2.- Cualquier cambio de domicilio de una de las partes deberá ser notificado a la otra de forma inmediata y por un medio que garantice la recepción del mensaje.

NUEVE: CLÁUSULAS GENERALES

1.- La no exigencia por cualquiera de las partes de cualquiera de sus derechos, de conformidad con el presente Contrato, no se considerará que constituye una renuncia a dichos derechos en el futuro.

2.- La relación jurídica que se constituye entre las partes se rige por este único Contrato, siendo el único válido existente entre las partes y sustituye a cualquier tipo de acuerdo o compromiso anterior acerca del mismo objeto, ya sea escrito o verbal, y sólo podrá ser modificado por un acuerdo firmado por ambas partes.

3.- Si se llegara a demostrar que alguna de las estipulaciones contenidas en este Contrato es nula, ilegal o inexigible, la validez, legalidad y exigibilidad del resto de las estipulaciones no se verán afectadas o perjudicadas por aquélla.

4.- El presente Contrato y las relaciones entre el RESPONSABLE DEL TRATAMIENTO y el ENCARGADO DEL TRATAMIENTO no constituyen en ningún caso sociedad, empresa conjunta, agencia o contrato de trabajo entre las partes.

5.-Los encabezamientos de las distintas cláusulas son sólo a efectos informativos, y no afectarán, calificarán o ampliarán la interpretación de este Contrato.

En testimonio de lo cual formalizan el presente contrato, por duplicado, en el lugar y fecha indicados en el encabezamiento.

D:/Dña. _____ D:/Dña. _____

En nombre de «EL RESPONSABLE» En nombre de «EL ENCARGADO»

7. Menores

(Nombre del menor) ha indicado que eres su padre, madre o tutor.

De conformidad con el Reglamento (UE) 2016/679, de 27 de abril de 2016, o Reglamento General de Protección de Datos (RGPD), y con la Ley Orgánica 3/2018, de 5 diciembre

de Protección de Datos Personales y garantía de los derechos digitales, le informamos que:

Le solicitamos que nos confirme su consentimiento expreso para utilizar los datos personales de **(nombre del menor)** y así, recibir comunicaciones que pudieran ser de su interés, en relación a servicios sociales, vía correo electrónico o medios análogos.

Introduzca su información

Nombre del padre, madre o tutor

Apellidos del padre, madre o tutor

Fecha de nacimiento

Soy el tutor legal de **(nombre del menor)** y estoy autorizando a dar mi aprobación.