Infraestructura para la INvestigación de ESpacios de DAtos distribuidos (INESData)

E6. Handbook (v2)

GOBIERNO DE ESPAÑA
MINISTERIO DE TRANSFORMACIÓN DIGITAL Y FUNCIÓN PÚBLICA
UNICO I+D Cloud
Financiado por la Unión Europea
NextGenerationEU

INFORMACIÓN DEL DOCUMENTO

Nombre del proyecto	Infraestructura para la INvestigación de Espacios de DAtos distribuidos
Acrónimo del proyecto	INESData
Proyecto de subvención	Unico I+D Cloud
URL del proyecto	https://dataspaces.oeg.fi.upm.es/
Fecha de inicio del proyecto	01/01/2023
Duración del proyecto	30 meses
Entregable	E6. Handbook (v2)
Paquete de trabajo	PT2
Tipo de entregable	Documento
Autores	Óscar Corcho (UPM), María Poveda (UPM), Paula Diez (UPM), Álvaro Morandeira (GMV), Fabián Avilés (GMV)
Fecha de entrega	30/06/2024
Versión	V2

RESUMEN EJECUTIVO

Esta guía práctica es un recurso que se actualiza continuamente a medida que avanza el proyecto INESData. En esta segunda versión, el enfoque principal ha sido la gobernanza de los espacios de datos, un aspecto clave para su desarrollo y consolidación. Por ello, el documento incorpora tres elementos fundamentales dentro de este marco: La Guía Práctica sobre Cuestiones de Cumplimiento con la normativa del Espacio de Datos; un documento de Definición de roles en la gobernanza del Espacio de Datos, estableciendo las responsabilidades y funciones de los distintos actores involucrados; y el documento de Modelos Contractuales Tipo, diseñados bajo el marco de gobernanza para facilitar acuerdos claros y estructurados entre las partes.

Además de servir como referencia para la creación y gestión de espacios de datos dentro del proyecto INESData, esta versión del *Handbook* recoge aprendizajes y referencias de iniciativas internacionales que fortalecen el marco de gobernanza. De cara a la próxima actualización, el documento ampliará su contenido con una visión más detallada del ecosistema nacional e internacional de los espacios de datos, incorporando documentación complementaria, como manuales de usuario.

Índice

Lista de figuras

Lista de acrónimos y abreviaciones

BDVA	Big Data Value Association
CAT	Catálogo
DCT	Validador de Contratos de Datos
DEL	Registro de Intercambio de Datos
DOME	Ecosistema de mercado abierto descentralizado
DSBA	Data Space Business Alliance
DSSC	Data Space Support Centre
EBSI	Infraestructura europea de servicios de cadena de bloque
eIDAS	Reglamento europeo de identificación digital
IA	Inteligencia Artificial
IAM	Gestión de acceso e identidad
IDS	International Data Space
IDS-RAM	International Data Space - Reference Architecture model
IDSA	International Data Space Association
INESData	Infraestructura para la Investigación de ESpacios de DAtos distribuidos
IoT	Internet de las cosas
OCM	Gestor de Credenciales Institucionales
ODRL	Lenguaje de derechos digitales abiertos
OID4VP	OpenID Connect for Verifiable Presentations
PCM	Gestor de Credenciales Personales
RGPD	Reglamento General de Protección de Datos
SETELECO	Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales
SIOPv2	Self-Issued OpenID Provider v2
VC	Credencial verificable
VP	Presentación verificable

1. Introducción

Los avances en tecnología e inteligencia artificial (IA) han puesto en evidencia la importancia de los datos. En la actualidad, es muy frecuente usar técnicas de aprendizaje profundo, Machine Learning en inglés, para la creación de sistemas y servicios. Dichas técnicas necesitan usar una cierta cantidad de datos; es más, dependiendo de la cantidad y la calidad de los datos usados, el sistema obtenido será de mayor o menor calidad.

A raíz de la importancia que están adquiriendo los datos, se han promovido diferentes programas e iniciativas, tanto a nivel europeo como español. El proyecto Infraestructura para la INvestigación de ESpacios de DAtos distribuidos en UPM (INESData) pretende crear una incubadora de espacios de datos y servicios a nivel nacional que haga uso de infraestructuras federadas en la nube y de borde (cloud-edge). Este proyecto está subvencionado por la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales (SETELECO) en el marco de financiación UNICO I+D Cloud, cuya finalidad es impulsar la investigación, la innovación y el desarrollo de infraestructuras en la nube y de borde, así como fomentar la colaboración público-privada.

Esta guía práctica es un documento vivo que evolucionará conforme avance el proyecto INESData. En esta segunda versión, nos hemos enfocado en los aspectos de gobernanza del espacio de datos, los cuales se encuentran recogidos en la sección de gobernanza (ver Gobernanza en INESData) y los anexos. En la próxima versión del documento, se actualizará todo el contenido relativo al ecosistema nacional e internacional de los espacios de datos y se incluirá documentación relevante, como manuales de usuario. El objetivo de este es presentar los espacios de datos creados en el proyecto INESData y explicar el proceso de creación, proporcionando una referencia práctica para quienes estén interesados en desarrollar sus propios espacios de datos. Ahora que el proyecto ha avanzado significativamente, esta versión profundiza en la gobernanza y toma como referencia diversas iniciativas internacionales para enriquecer el marco de desarrollo de los espacios de datos.

.

2. ¿Qué son los espacios de datos?

Un espacio de datos se puede definir como una infraestructura descentralizada para el intercambio de datos en un entorno confiable. Las principales características de los espacios de datos se pueden dividir en cuatro conjuntos o bloques de características, tal y come se puede observar en la Figura 1). El primero (en azul) aborda los principios que rigen los espacios de datos junto con la integración de las leyes europeas, como la ley de protección de datos o la ley de protección al consumidor. El segundo conjunto (en naranja) explica que los participantes pueden pertenecer tanto al sector público como al privado, y que pueden asumir varios roles: productores, consumidores y/o proveedores de datos. El tercer bloque (en verde) se centra en la gobernanza de datos, en otras palabras, la gestión de datos. Entre las características relacionadas con la gobernanza destacan: controlar quién puede acceder a los datos y las condiciones de acceso (acceso gratuito, con licencia paga, etc.); y el uso de formatos accesibles. Por último, el último conjunto (en amarillo) trata de las características de los espacios de datos a nivel tecnológico.

Los espacios de datos tienden a estar especializados en dominios o sectores. Algunos de los sectores registrados por las principales iniciativas internacionales (ver Sección 3) incluyen: agricultura, ciudades inteligentes, construcción, educación, energía, espacio, manufactura, finanzas, turismo, movilidad, medios, medicina, sector público, logística, ubicación, vida inteligente. Además, la Asociación Internacional de Espacios de Datos (IDSA) tiene un radar donde se registran los espacios de datos y los casos de uso. Del mismo modo, Gaia-X tiene una sección de 'Lighthouse Projects' en su sitio web.

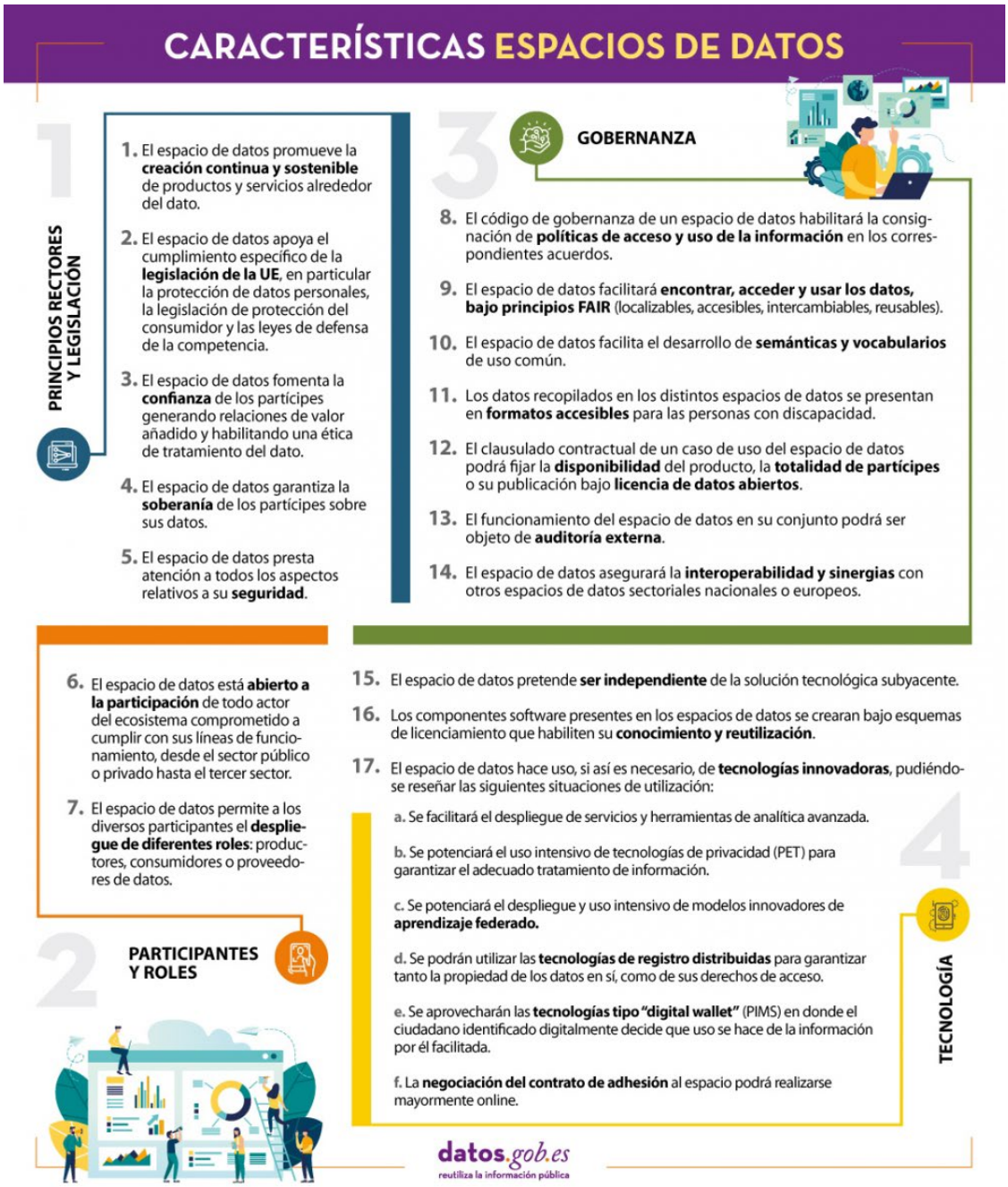

Figura 1: Características de los espacios de datos. Extraído de [1]

3. Iniciativas internacionales

Existen varias iniciativas internacionales que abordan la creación de espacios de datos. La Figura 2 muestra varias de las iniciativas europeas relacionadas con los datos. La Figura 2 indica: por un lado, en qué ámbitos de desarrollo trabaja cada una de ellas; y por el otro lado, el nivel de desarrollo de cada una. Las iniciativas que se abordarán en esta guía son cuatro: International Data Space Association (IDSA), Gaia-X, FIWARE Foundation, Big Data Value Association (BDVA). Asimismo, se usará como referencia la alianza creada entre estas cuatro iniciativas, llamada Data Space Business Alliance (DSBA) .

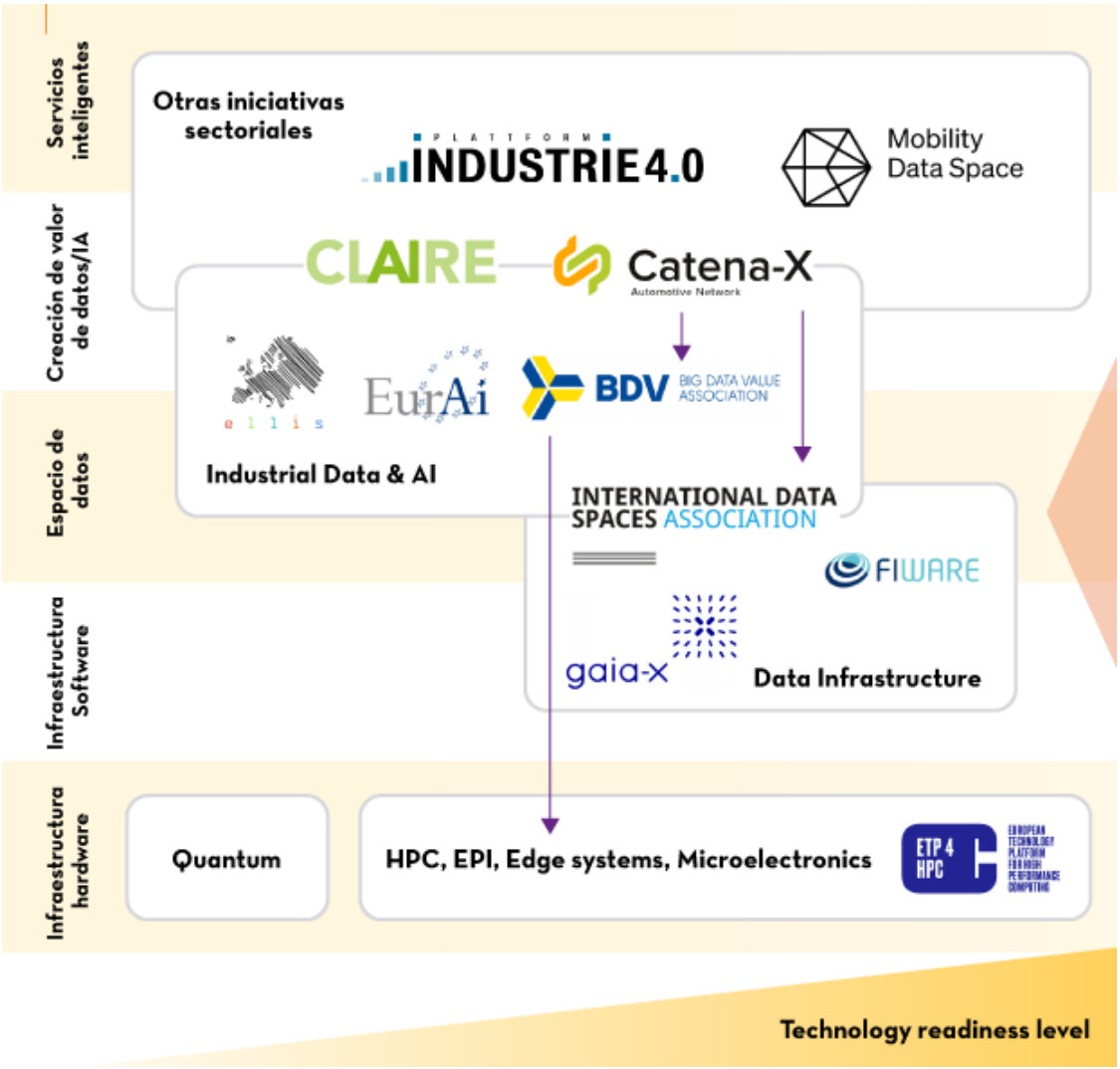

Figura 2: Iniciativas europeas relacionadas con los datos. Extraído de [2]

3.1. International Data Space Association (IDSA)

En 2015, la sociedad Fraunhofer inició el proyecto International Data Spaces (IDS), respaldado por la International Data Space Association (IDSA). La Figura 3 muestra el modelo conceptual de la arquitectura de referencia de IDS, en inglés *IDS Reference Architecture model (IDS-RAM)*. Como se puede observar, hay varios elementos, los cuales IDSA describe de la siguiente manera:

1. El Proveedor de Datos (*Data Provider*) es un dispositivo que transfiere los datos del propietario al espacio de datos a través del conector IDS. Permite que otros utilicen los datos manteniendo el control sobre quién, cómo, cuándo, por qué y a qué precio. Esta es la soberanía de los datos, la base para desbloquear el valor de los datos.

2. El Consumidor de Datos (*Data Consumer*) es un dispositivo que procesa datos en nombre del usuario. Los proveedores de datos ofrecen los datos según sus políticas de uso y con confianza en la calidad y confiabilidad de los datos. Así es como los datos entregan su valor. Esto también es soberanía de datos.

3. El Conector IDS (*IDS Connector*) es un componente de software que permite a los participantes adjuntar políticas de uso a sus datos, hacer cumplir las políticas de uso y rastrear sin problemas la procedencia de los datos. El Conector actúa como una puerta de enlace para datos y servicios, y como un entorno confiable para aplicaciones y software.

4. Los *Brokers* prioporcionan información sobre las fuentes de datos en términos de contenido, calidad de la estructura, moneda y otras características.

5. El Centro de Intercambio de Información (*Clearing House*) es el servicio de compensación y liquidación para los intercambios de datos y las transacciones financieras dentro del espacio de datos.

6. La Tienda de Aplicaciones (*App Store*) proporciona aplicaciones que se pueden implementar en los Conectores IDS para ejecutar tareas como transformación, agregación o análisis de datos.

7. El Proveedor de Identidad (*Identity Providers*) crea, mantiene, administra y valida la información de identidad de y para los participantes del espacio de datos.

8. Los Vocabularios (*Vocabularies*) proporcionan descriptores estandarizados para datos basados en las mejores prácticas aceptadas.

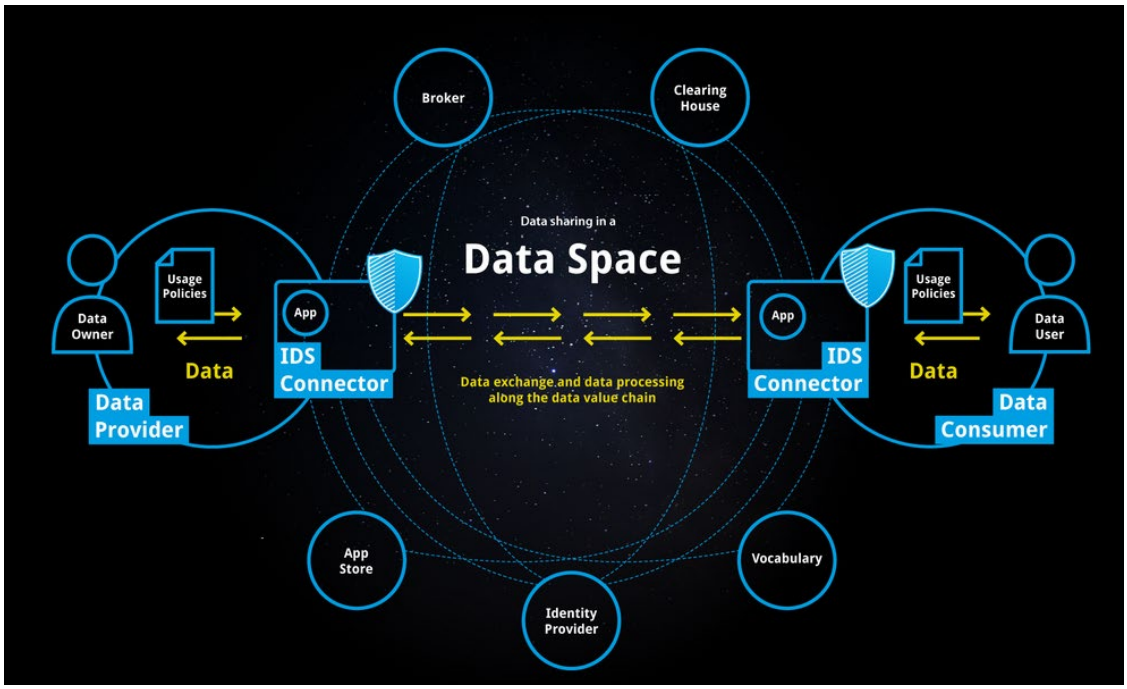

Figura 3: Modelo conceptual de IDSA sobre los espacios de datos. Extraído de [3]

3.2. Gaia-X

El proyecto Gaia-X se lanzó en 2019 y está estrechamente alineado con la Estrategia Europea de Datos y el Plan de recuperación para Europa . La Figura 4 muestra el modelo conceptual de Gaia-X. En este modelo existen tres tipos de Participantes (*Participants*): Proveedor (*Provider*), Consumidor (*Consumer*) y Fererador (*Federator*). Los Proveedores son los participantes que ofrecen sus datos y servicios. Por otro lado, los Consumidores son los que usan o consumen el dato o servicio. En cuanto a los Federadores, son los que manejan la Federación y los Servicios de la Federación. Una Federación se refiere a un conjunto de actores que interactúan y que, directa o indirectamente, consumen, producen o proporcionan recursos relacionados. En cuanto a los servicios de federación, son necesarios para habilitar una federación de infraestructura y datos, y para proporcionar interoperabilidad entre federaciones. Hay varios aspectos a tener en cuenta en relación con los Servicios de Federación:

1. Se necesita un Vocabulario común para la Gestión de Acceso e Identidad, en inglés, *Identity and Access Management (IAM)*.
2. El Marco de Confianza (*Trust Framework*) de Gaia-X garantiza que los Participantes cumplan el reglamento establecido.
3. Los portales y las API ayudarán a los participantes a interactuar con los servicios de federación a través de una interfaz de usuario.

4. El intercambio de datos en Gaia-X está habilitado por un conjunto de servicios de intercambio de datos que realiza cada participante y puede ser respaldado por la Federación. Gaia-X Federation Services proporciona varias herramientas para abordar algunas de las necesidades funcionales, como la identificación, los protocolos de datos, la contratación... Algunas de las herramientas son:

    a. Gestor de Credenciales Institucionales (*Organizational Credential Manager, OCM*);

    b. Gestor de Credenciales Personales (*Personal Credential Manager, PCM*);

    c. Validador de Contratos de Datos (*Data Contract Transaction, DCT*);

    d. Registro de Intercambio de Datos (*Data Exchange Logging, DEL*);

    e. Catálogo (*Catalog, CAT*).

Por último, el módulo Composición de Servicios (*Service Composition*) se ocupa de las solicitudes de servicios. Este módulo analiza las solicitudes y encuentra los servicios más adecuados.

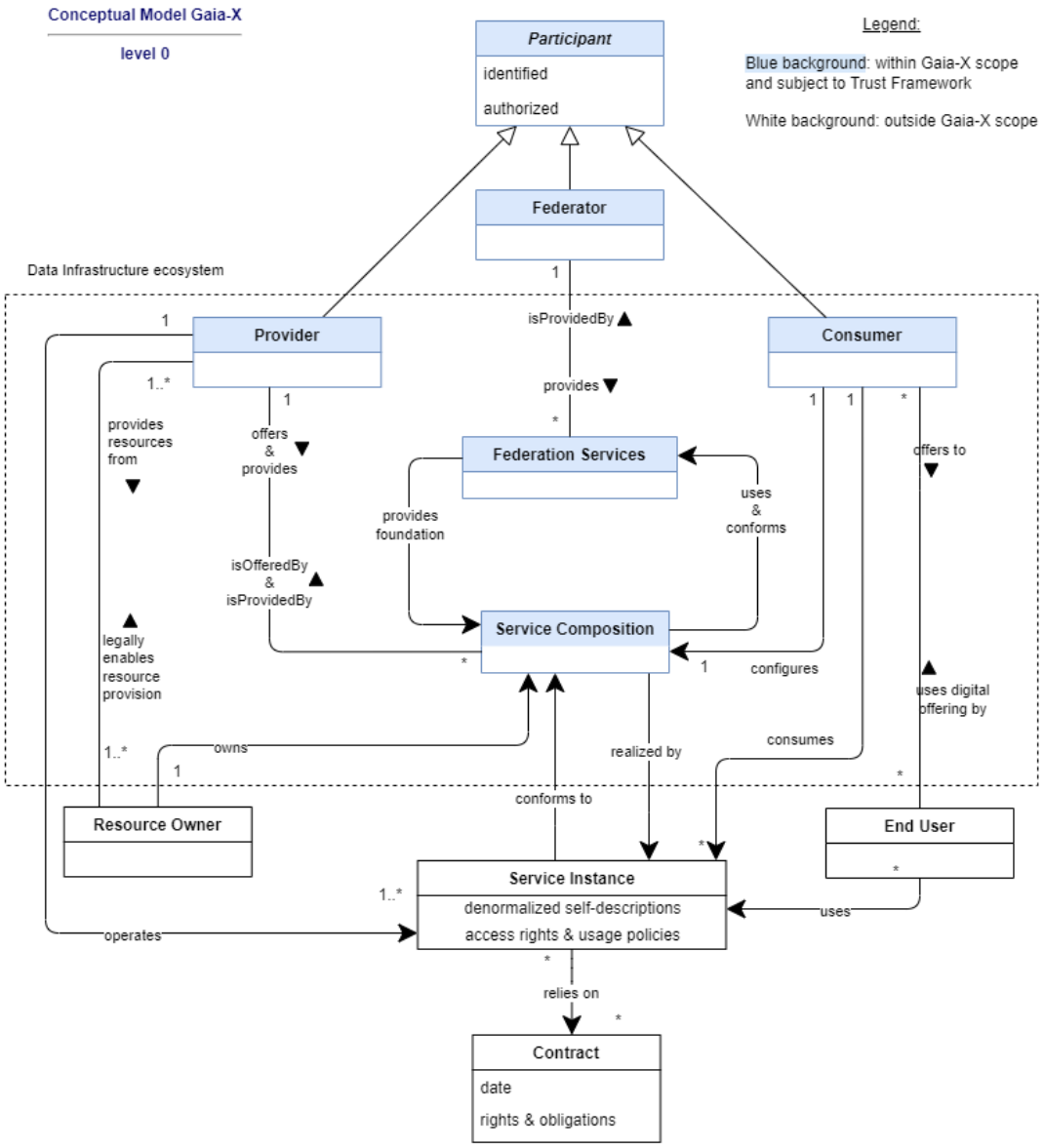

Figura 4: Modelo conceptual de Gaia-X sobre los espacios de datos. Extraído de [4, Ch. 4]

3.3. FIWARE Foundation

FIWARE Foundation trabaja activamente en el desarrollo de software de código abierto. En relación con los espacios de datos, FIWARE tiene componentes ya desarrollados que se pueden integrar, los cuales están disponibles en GitHub.

Big Data Value Association (BDVA)

Big Data Value Association (BDVA) es una organización impulsada por la industria que se centra en las áreas de: tecnologías y servicios de Big Data, plataformas de datos y espacios de datos, IA industrial, creación de valor basada en datos, estandarización y habilidades.

3.4. Data Space Business Alliance (DSBA)

En septiembre de 2021, se creó la alianza Data Space Business Alliance (DSBA) cuando IDSA, Gaia-X, FIWARE Foundation y BDVA se unieron para trabajar en la creación de un marco común. Cada miembro de la alianza aporta en un aspecto diferente. BDVA contribuye con el conocimiento general y la comprensión para el uso de los datos. FIWARE Foundation invierte más en componentes para el intercambio de datos de gemelos digitales e IAM. Gaia-X se dedica principalmente a la gobernanza entre espacios de datos. Por último, IDSA se enfoca en conectores de espacio de datos, negociación de contratos de uso y creación general de un espacio de datos. Cabe destacar que Gaia-X e IDSA están más enfocados en producir especificaciones, así como herramientas y procedimientos para probar el cumplimiento de los productos con esas especificaciones. Por otro lado, FIWARE Foundation tiene como objetivo influir en el desarrollo de especificaciones en los organismos relevantes y fomentar su rápida adopción en el mercado siguiendo un enfoque impulsado por la implementación de código abierto. La Figura 5 muestra la conexión entre las iniciativas.

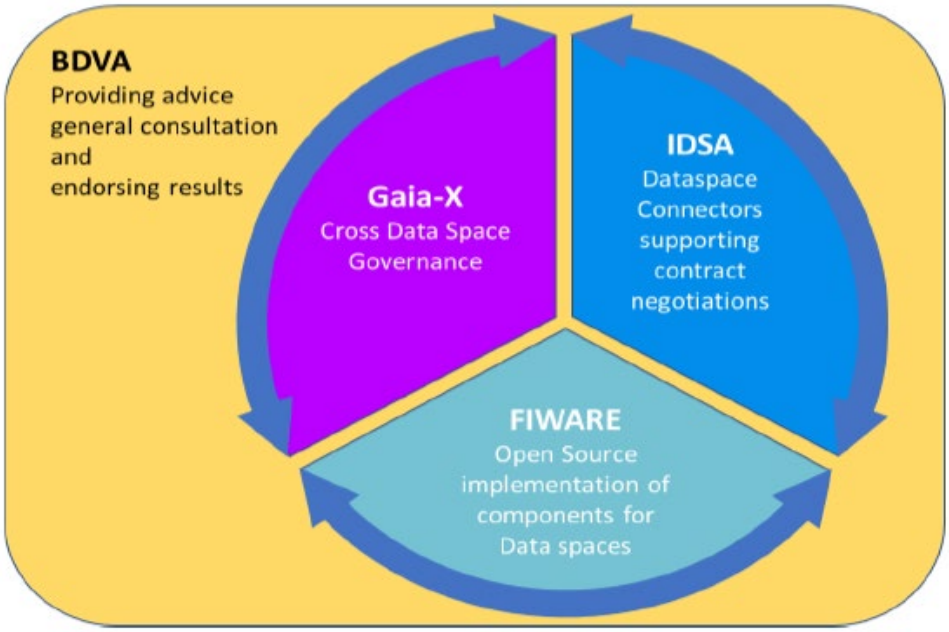

Figura 5: Contribuciones de los miembros de DSBA. Extraído de [5, p. 25]

Cabe mencionar que cada miembro de la DSBA cuenta con 'Hubs' en diferentes países. La Figura 6 muestra la localización de los Hubs de cada miembro DSBA.

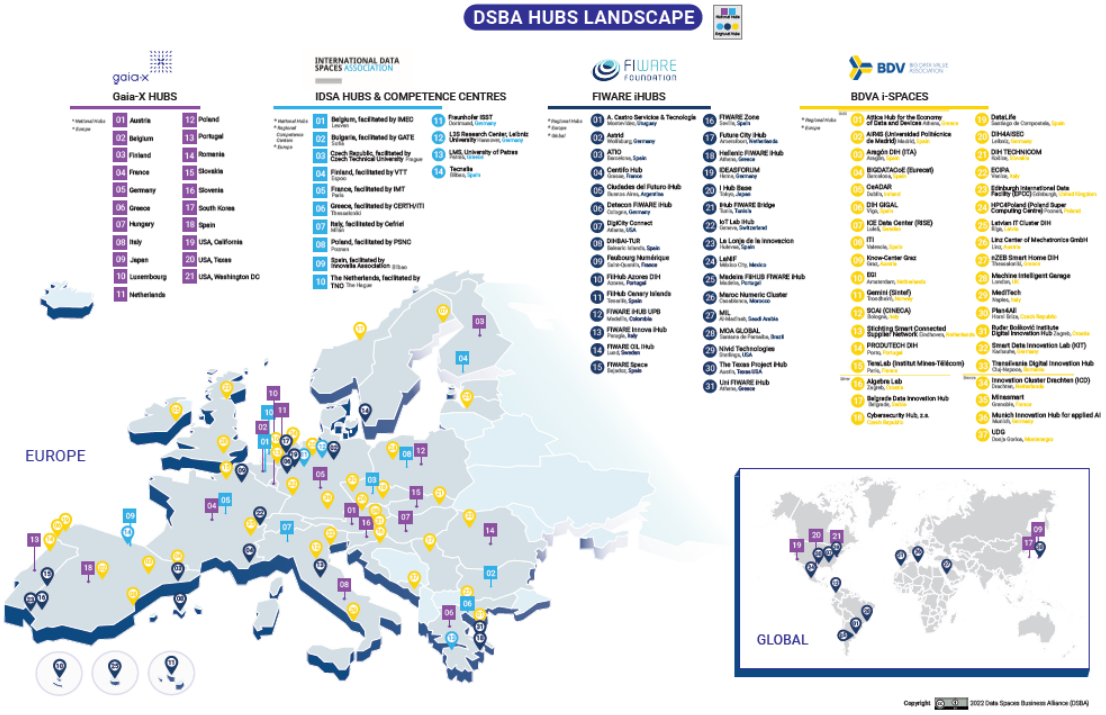

Figura 6: Distribución de los Hubs de DSBA. Extraído de [6, p. 11]

En abril de 2023, DSBA publicó su primer documento explicativo de la visión conjunta sobre los espacios de datos, su Convergencia Técnica. La Figura 7 muestra el modelo conceptual de la visión conjunta de Gaia-X, IDS-RAM y FIWARE Foundation.

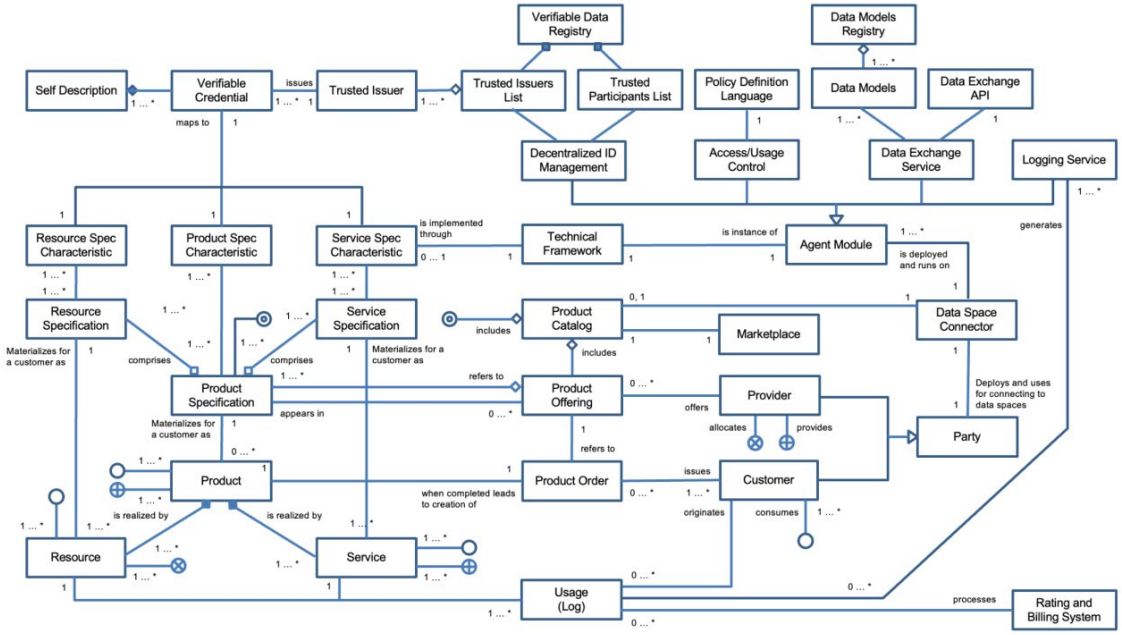

Figura 7: Modelo conceptual de DSBA sobre los espacios de datos. Extraído de [5, p. 17]

A la hora de crear e implementar los espacios de datos, DSBA sigue una taxonomía de componentes básicos (*Building Blocks*) adaptada de la desarrollada en el proyecto OpenDEI. Dicha taxonomía (Figura 8) cenda con cuatro pilares básicos: la interoperabilidad de datos (*Data Interoperability*); la soberanía de datos y confianza (*Data Sovereignty and Trust*); el valor del dato (*Data Value Creation*); y la gobernanza en los espacios de datos (*Data Space Governance*).

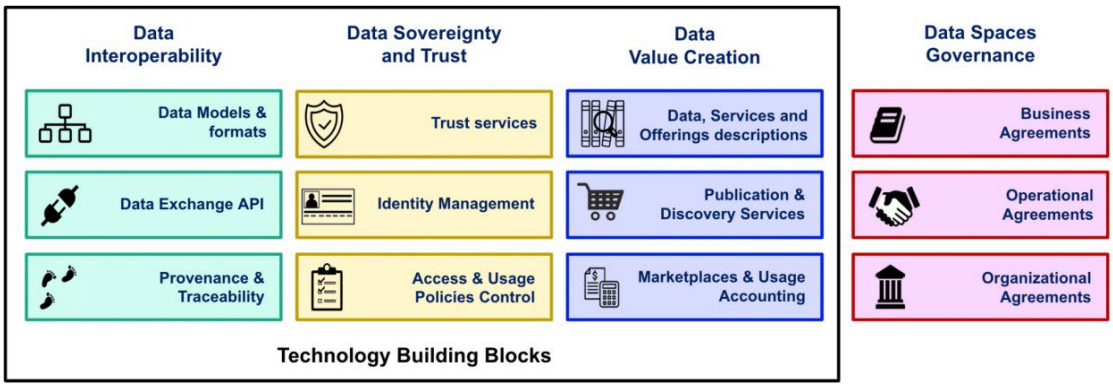

Figura 8: Componentes básicos en los espacios de datos. Extraído de [5, p. 11]

Los tres primeros pilares están relacionados con la creación de los espacios de datos a nivel tecnológico. La Figura 9 muestra cómo los componentes básicos tecnológicos se conectan entre sí. Como se puede observar, hay tres elementos fundamentales en la relación entre componentes:

el Registro del Espacio de Datos (*Data Space Registry*), los Conectores (*Data Space Connectors*), y los Servicios Federados (*Federated Services*).

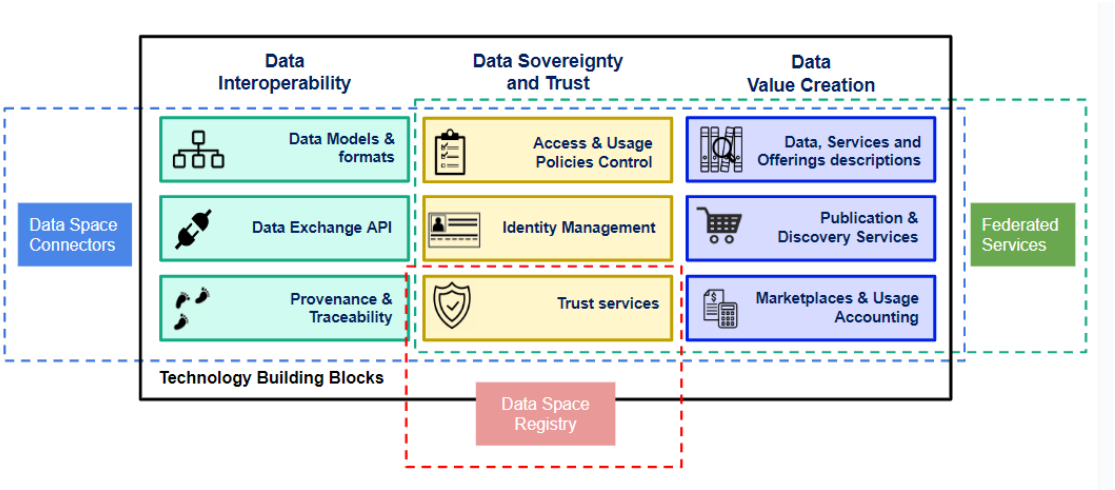

Figura 9: Comunicación entre componentes básicos a nivel tecnológico. Extraído de [5, p. 13]

El Registro del Espacio de Datos está a cargo de registrar a todos los participantes en el espacio de datos para establecer cierta confianza dentro del ecosistema. En el marco tecnológico de referencia de DSBA, dicha identificación se basa en el uso de credenciales verificables (*Verifiable Credentials, VC*) emitidas por emisores de confianza registrados o acreditados a través del Registro del Espacio de Datos. Hay varios modelos típicos que se pueden seguir (por ejemplo: enfoques centralizados, enfoques descentralizados o enfoques federados). Aunque la Convergencia Técnica se centra en un enfoque descentralizado, Gaia-X proporcionará los medios para la configuración de las tres opciones disponibles.

Los Conectores son sistemas que permiten las transacciones entre los participantes. La interacción debe hacer uso de estándares tanto como sea posible para lograr la interoperabilidad. En este aspecto, destaca el Protocolo de Espacio de Datos de IDSA. Este protocolo es un conjunto de especificaciones diseñadas para facilitar el intercambio interoperable de datos entre participantes de espacios de datos, regidos por el control de uso y basados en tecnologías Web.

El último elemento son los Servicios Federados, es decir, servicios que pueden existir dentro de un espacio de datos, a nivel global. Estos servicios pueden incluir: Servicios de Marketplace, Servicios de Catálogo, o Servicios de Intermediario de Metadatos.

Cabe destacar que el desarrollo y la unificación de la arquitectura de los espacios de datos está aún en proceso, según indica DSBA. La Figura 10 muestra las equivalencias terminológicas entre IDSA, Gaia-X y FIWARE Foundation.

FIWARE/TMForum	Gaia-X	IDSA
Party	Participant	Participant
Provider	Provider	Data Provider
Customer	Consumer	Data Consumer
Data Product (comprises resource and services)	Resource & Services	Data Asset
Trusted Participant List		IDS-DAPS + IDS-ParIS
(Data) Product Specification	Gaia-X Schema	IDS-Information Model + Vocabulary
(Data) Product Offering	Service Offering	Part of Self-Description
(Data) Product Catalogs.	Federated Catalogue	IDS-Meta-Data-Broker
Service Specification Characteristics.	Gaia-X Credentials (formerly known as Self-Description)	Connector Self Description
Logging Service	Data Exchange Services	Observability/Clearing House

Figura 10: Equivalencias terminológicas entre IDSA, Gaia-X y FIWARE Foundation. Extraído de [5, p. 20]

4. La creación de los espacio de datos INESData

Esta sección se centrará en el proceso de creación y despliegue de los espacios de datos desarrollados en el proyecto INESData. Dado que el proyecto aún se encuentra en sus primeras etapas, esta primera versión del manual se centrará en proporcionar algunos antecedentes y referencias para el trabajo futuro. El resto la sección está organizada de la siguiente manera: en primer lugar, se abordarán los componentes básicos tecnológicos (interoperabilidad de datos; soberanía y confianza de los datos; y, creación y valor de los datos). A continuación, se presentarán los componentes relacionados con la Gobernanza.

4.1. Interoperabilidad

La interoperabilidad es la capacidad de los sistemas o programas informáticos para intercambiar información, y es un aspecto clave en los espacios de datos. Se pueden distinguir dos niveles de interoperabilidad: interoperabilidad interna, que se ocupa de la interoperabilidad dentro de espacios de datos individuales; y la interoperabilidad entre espacios de datos, que maneja la interoperabilidad entre múltiples espacios de datos.

Se pueden destacar dos marcos de interoperabilidad: el Nuevo Marco Europeo de Interoperabilidad (*New European Interoperability Framework*) y el marco ISO/IEC 21823-1:2019. En primer lugar, el Nuevo Marco Europeo de Interoperabilidad, establece cuatro tipos o niveles de interoperabilidad: técnica, semántica, organizativa y legal. La interoperabilidad técnica y semántica está cubierta por los componentes básicos de la tecnología. La interoperabilidad legal y la interoperabilidad organizacional se pueden lograr mediante las Políticas de Uso que espacio de datos específica.

Además del Nuevo Marco Europeo de Interoperabilidad, que está orientado hacia los servicios públicos digitales, ISO/IEC 21823-1:2019 introdujo un modelo de cinco niveles para abordar la interoperabilidad en el área de Internet de las Cosas, en inglés *Internet of Things (IoT)*. El modelo cuenta con los siguientes niveles de interoperabilidad: de transporte, sintáctica, semántica, de comportamiento, y de políticas. La interoperabilidad de transporte se ocupa de la entrega de datos (es decir, el envío de los datos); la interoperabilidad sintáctica permite leer los datos en un formato y gramática conocidos; mientras que la interoperabilidad semántica es responsable del significado, permitiendo la interpretación y comprensión inequívocas de los datos.

Dentro del pilar de la interoperabilidad, encontramos tres componentes básicos: 1) los modelos y formatos de datos, 2) el intercambio de datos, y 3) las fuentes y la rastreabilidad.

4.1.1. Componente Básico 1: Modelos y formatos de datos

Los modelos y formatos de datos (*Data models and formats*) se encargan de la comprensión semántica de los datos en los espacios de datos. La iniciativa Smart Data Models de FIWARE Foundation aborda este aspecto. Proporciona una biblioteca de modelos de datos para los cuales se facilita la descripción y la representación en múltiples formatos de datos. La Figura 11 muestra la organización de Smart Data Models en GitHub.

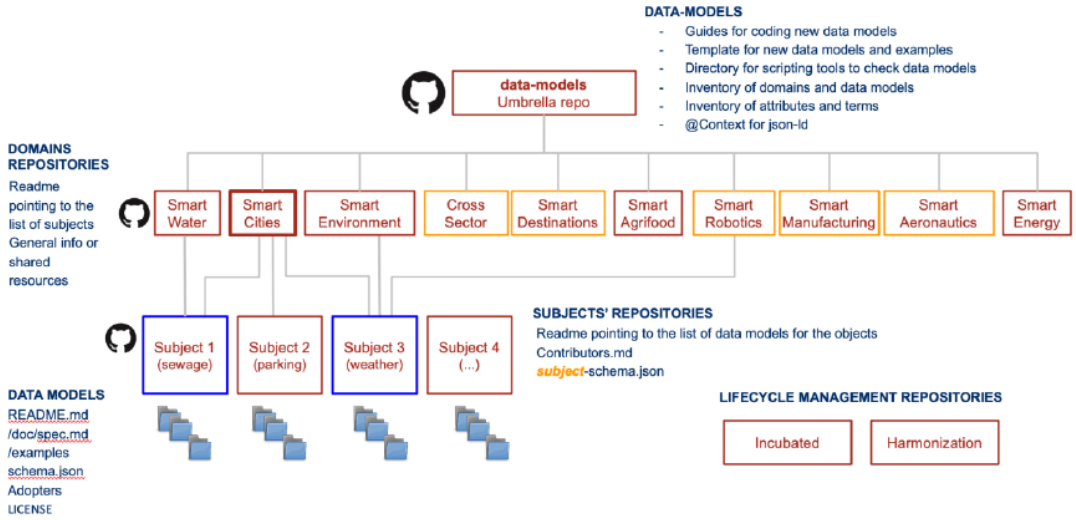

Figura 11: Organización del Github de la iniciativa Smart Data Models de FIWARE Foundation. Extraído de [5, p. 32]

4.1.2. Componente Básico 2: Intercambio de datos

El segundo componente básico se centra en las APIs para el intercambio de datos (*Data exchange API*). Para el intercambio de datos, se sugiere el modelo de datos NGSI-LD de FIWARE Foundation, ya que proporciona una API RESTful simple pero poderosa para obtener acceso a datos de gemelos digitales. Además, admite datos vinculados, gráficos de propiedades y semántica.

Asimismo, se proponen los Protocolos de Conectores de Espacios de Datos como base para la publicación de datos, la negociación de contratos, y el control del intercambio de datos. IDSA cuenta con una implementación de los Conectores de Espacios de Datos.

4.1.3. Componente Básico 3: Fuentes y rastreabilidad

El último componente básico relacionado con la interoperabilidad está relacionado con las fuentes y la rastreabilidad (*provenance and traceability)*. Los procesos de intercambio de datos

deben ser observables para mantener los datos regulados. Esto es importante tanto desde la perspectiva legal como desde la comercial.

Hay múltiples opciones para realizar un seguimiento de las transferencias de datos. En una arquitectura centralizada, se puede implementar un observador central (también conocido como cámara de compensación (*Clearing House*), auditor o agente de monitoreo). En una arquitectura descentralizada, los participantes mantienen la información de los acuerdos, lo que significa que siempre habrá al menos dos copias del registro de transacciones. Estas copias siempre se podrán identificar a través de un identificador que las vincule. IDS-RAM propone el Servicio de Cámara de Compensación (*Clearing House*) para implementar observabilidad, procedencia y trazabilidad.

4.2. Soberanía y confianza

El segundo pilar relacionado con la tecnología de los espacios de datos trata sobre la soberanía de los datos y la confianza en los ecosistemas. Cuenta con tres componentes básicos: los servicios para la confianza; el gestor de identidades; y, el acceso y las políticas de control.

4.2.1. Componente Básico 4: Servicios para la confianza

Se tienen en cuenta dos marcos para establecer confianza en un espacio de datos: Trust Anchor Framework (expansión de Gaia-X Trust Framework) y el Framework Descentralizado de Gestión de Identidad y Acceso basado. El marco Trust Anchor Framework establece un conjunto de reglas y aborda varios problemas, como, por ejemplo:

1. Vinculación de identidad: la verificación de una identidad del mundo real y su asignación de identificador.
2. Prueba de participación: para comprobar la participación, o para verificar una Credencial Verificable (*VC*, sigla en inglés), se sugiere el uso de una Lista de Participantes de Confianza.
3. Prueba de autoridad emisora: para comprobar la autorización de una entidad emisora, se sugiere el uso de una Lista de Emisores de Confianza.

En cuanto al marco de administración de identidad y acceso descentralizado, permite actividades transaccionales confiables dentro del DS. Aborda la identificación y la autorización.

4.2.2. Componente Básico 5: Gestor de identidad

Para identificar a los participantes, DSBA propone utilizar dos protocolos para la gestión de identidades: 1) OpenID Connect for Verifiable Presentations (OID4VP) y 2) Self-Issued OpenID Provider v2 (SIOPv2), que admite el uso de VC y VP, y, en el caso de SIOPv2, DIDs (identificadores descentralizados). De este modo, los participantes pueden emitir y verificar VCs. También permite compartir las credenciales entre participantes sin la necesidad de un Proveedor de Identidad Centralizado. La Figura 11 y la Figura 12 muestran el funcionamiento de los protocolos OID4VP y SIOP, respectivamente.

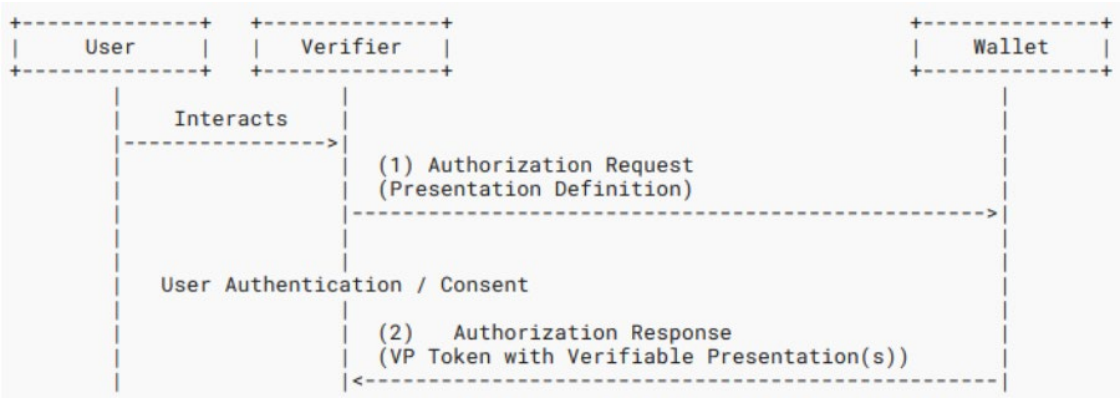

Figura 12: Flujo de trabajo del protocolo OID4VP. Adaptado de la especificación del protocólo [7]

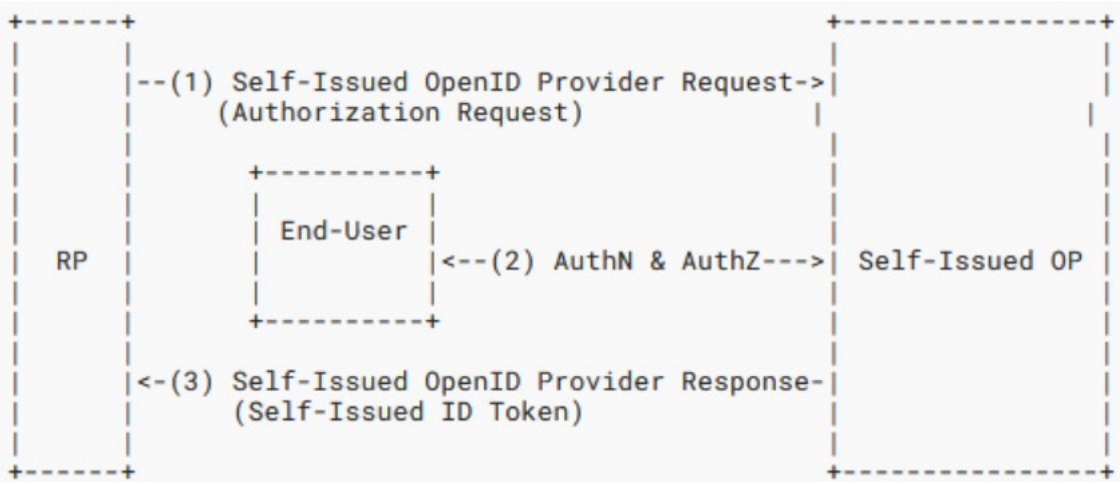

Figura 13: Flujo de trabajo del protocolo SIOP. Adaptado de la especificación del protocólo [8]

FIWARE Foundation cuenta con una implementación de código abierto de un componente de gestión de identidad. El estándar ISO/IEC 24760-1:2019 (Seguridad y privacidad de TI: un marco para la gestión de identidades) también se puede considerar para lograr la interoperabilidad entre las soluciones de gestión de identidades.

4.2.3. Componente Básico 6: Acceso y políticas de control

Para controlar el acceso y el uso de datos en espacios de datos, se deben: 1) negociar unas políticas de uso entre el proveedor y el consumidor; 2) aplicar y controlar dichas políticas.

Una negociación de póliza o contrato inglés involucra a un Proveedor y un Consumidor. La negociación obtiene un IRI como identificador, y puede ser rastreado a través de sus diferentes etapas. El Protocolo de Espacio de Datos para la Negociación de Contratos de IDSA ofrece más detalles respecto a este tema.

Una vez alcanzado un acuerdo, debe haber un proceso de control que se del cumplimiento del contrato. Hay dos niveles de control: el legal (mediante documentos vinculantes), y la técnica. Estas dos categorías están cubiertas por la arquitectura XACML, aunque DSBA menciona que no se limitan a dicha arquitectura.

Para que este proceso se pueda llevar a cabo, también es necesario el uso de un lenguaje de expresión de políticas. DSBA propone utilizar el lenguaje de derechos digitales abiertos (*ODRL*, siglas en inglés) como un estándar interoperable para la expresión de políticas. En la Figura 14 se muestra un diagrama del modelo de información ODRL.

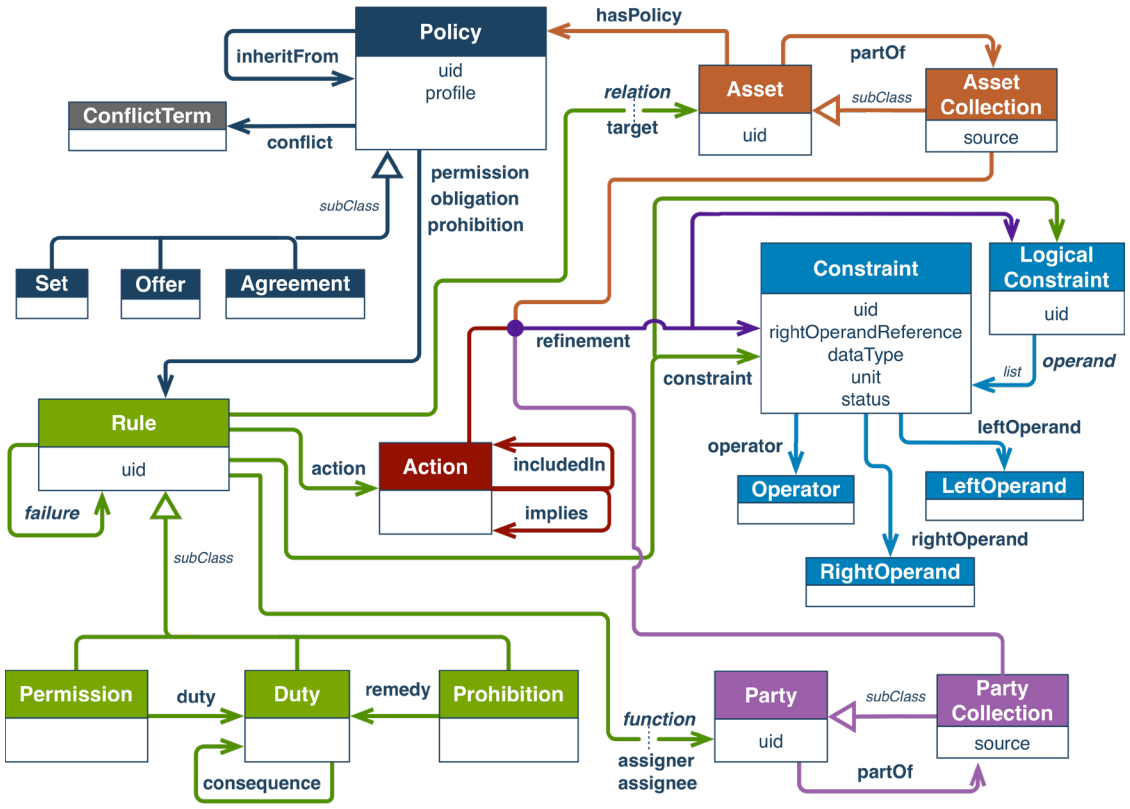

Figura 14: Modelo de información ODRL. Extraído de [9]

4.3. Valor del dato

Los espacios de datos buscan la creación del valor de los datos a partir del uso compartido. Pora lograr dicho objetivo, el pilar del valor del dato cuenta con tres componentes: 1) Descripción de datos, servicios y ofertas; 2) Servicios de publicación y descubrimiento; y, 3) Mercados y Servicios de Contabilidad

4.3.1. Componente Básico 7: Descripciones de los datos y servicios

Para que el Consumidor pueda describir los datos y servicios ofrecidos en el ecosistema, el Modelo de Información (*Information Model*) de IDSA proporciona un esquema para las Autodescripciones (*Self-Descriptions*) y sus componentes básicos, como, por ejemplo: contratos de uso, descripciones de *endpoints*, o la estructura interna de los activos de datos. Después de rellenar una Autodescripción, los datos deberían ser registrados en un Catálogo de Productos.

4.3.2. Componente Básico 8: Publicación y servicios de búsqueda

Mediante los Intermediarios de Metadatos (o *Metadara Brokers*) los Proveedores pueden hacer sus datos sean visibles y fáciles de encontrar. Un Intermediario de Datos es un componente del espacio de datos que se encarga del registro, la publicación, el mantenimiento y la consulta de las Autodescripciones. DSBA indica que el Intermediario de Metadatos de IDSA podría utilizarse como referencia.

4.3.3. Componente Básico 9: Mercado y finanzas

DSBA sugiere un ecosistema de mercado abierto descentralizado, en inglés *Descentralized Open Market Ecosystem (DOME)*, basado en la federación de mercados que se conectan a un catálogo compartido de servicios. Las organizaciones pueden adoptar seis roles diferentes en un espacio de datos vinculado a DOME:

1. Proveedores de servicios en la nube y perimetrales
2. Mercados federados
3. Clientes
4. Operadores de infraestructuras
5. Proveedores de Servicios Complementarios

6. Miembros de los órganos de gobierno y control.

En cuanto a la arquitectura técnica de DOME, hay cinco aspectos principales a tener en cuenta: el catálogo compartido y los libros de transacciones; el viaje de los proveedores de servicios; el viaje del cliente; y, la interoperabilidad con las plataformas de publicación de datos.

El catálogo compartido, así como los pedidos de productos y la información de uso, son administrados por la Capa Persistente Distribuida (*Distributed Persistent Layer*) de la arquitectura DOME. Esta capa se puede implementar sobre una serie de cadenas de bloques nacionales interconectadas (como Alastria o HashNet) compatibles con la infraestructura europea de servicios de cadena de bloques (EBSI). La Figura 15 muestra la arquitectura a alto nivel de la Capa Persistente Distribuida de DOME. Como se puede observar, los portales globales de DOME, los proveedores de servicios en la nube, y los mercados federados pueden acceder a la capa a través de algunos puntos de acceso.

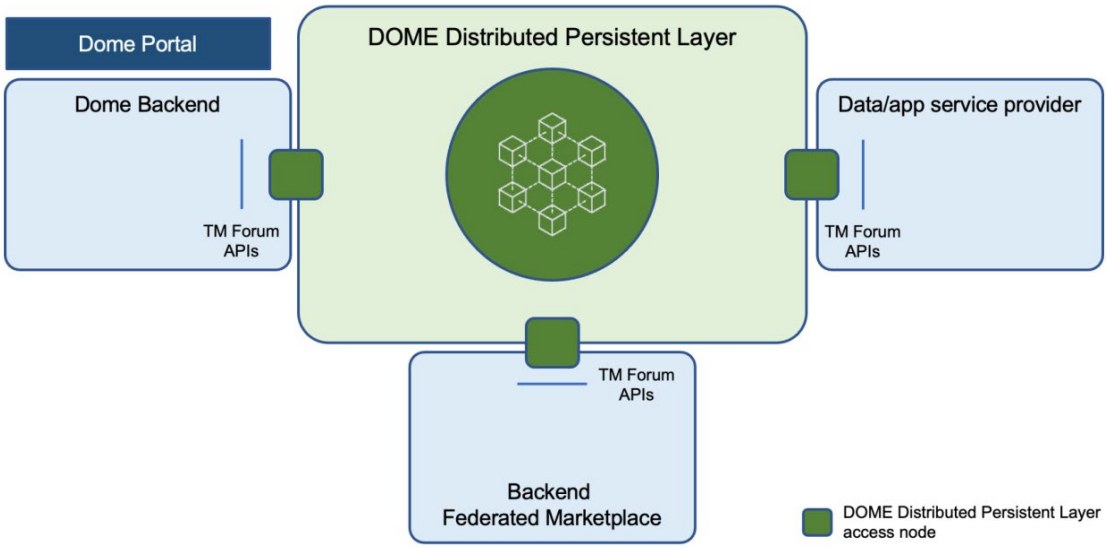

Figura 15: La Capa Persistente Distribuida de DOME. Extraído de [5, p. 65]

En cuanto al Viaje de los Proveedores de Servicios (*Consumer's Journey*), hay cuatro etapas: suscribirse, referenciar, vender y seguir. La Figura 16 muestra las etapas del viaje junto con los pasos en cada etapa. Por otro lado, el Viaje de los Consumidores (*Customer's Journey*), tiene cinco etapas y cada etapa tiene tres de cuatro pasos, como se ve en la Figura 17.

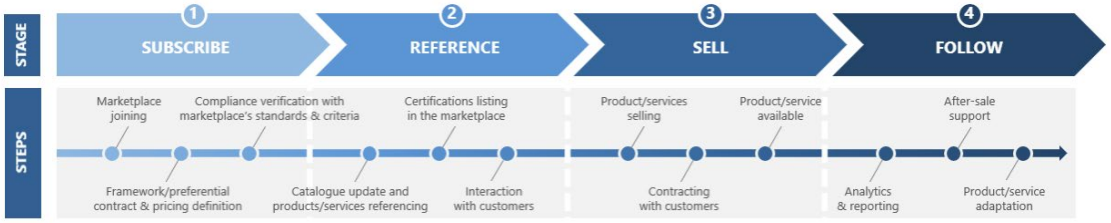

Figura 16: Viaje del Proveedor. Extraído de [5, p. 66]

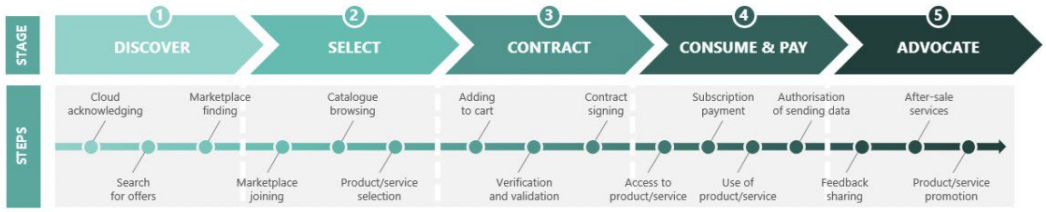

Figura 17: Viaje del Consumidor. Extraído de [5, p. 75]

Por último, en lo que respecta a la interoperabilidad con las plataformas de publicación de datos, DOME integrará funciones de publicación de datos que permitan la exposición de dichos recursos de datos de conformidad con las especificaciones DCAT definidas por W3C y la recomendación DCAT-AP de la CE. De esta forma, los recursos de datos vinculados a los servicios de datos ofrecidos a través de DOME pueden recolectarse a través de plataformas de publicación de datos externas (por ejemplo, el portal de datos europeo).

4.4. Gobernanza

4.4.1. Regulaciones

Se deben considerar las siguientes leyes y propuestas de regulación para procesar datos personales de ciudadanos de la UE y datos no personales generados en la UE.

Reglamento General de Protección de Datos (RGPD) [10]:

Ley que regula el tratamiento de datos personales de los ciudadanos de la Unión Europea. Las principales entidades implicadas son el interesado (persona física identificable a la que se refieren los datos), el responsable del tratamiento (entidad que define los fines del tratamiento de datos personales) y el encargado del tratamiento (entidad que trata datos personales en nombre del controlador). El RGPD establece los siguientes principios para el tratamiento de datos personales: (i) debe tratarse de manera lícita, leal y transparente (‘licitud, equidad y transparencia’); (ii) el procesamiento debe limitarse al propósito especificado por el interesado (‘limitación del propósito’); (iii) debe incluir sólo los datos mínimos relevantes para el propósito para el cual se está procesando (‘minimización de datos’); (iv) los datos deben ser exactos y posibles de corregir cuando sea necesario (‘exactitud’); (v) debe conservarse solo mientras sea necesario (‘limitación de almacenamiento’); (vi) deben garantizarse medidas técnicas y organizativas adecuadas para la seguridad de los datos personales (‘integridad y

confidencialidad'); y (vii) los controladores de datos deben contar con mecanismos para demostrar el cumplimiento de estos principios ('responsabilidad'). Estos principios deben ser respetados por los controladores y procesadores para tener sistemas que sean amigables con la privacidad por diseño y por defecto. Además, el Capítulo III define una serie de derechos de los interesados, p. ejem. el derecho al olvido o el derecho a oponerse, y el Capítulo IV una serie de disposiciones que los controladores de datos deben seguir para cumplir con la ley, p. ejem. creación y mantenimiento de registros de actividades de procesamiento o evaluaciones de impacto de protección de datos.

Reglamento europeo de identificación digital (eIDAS, sigla en inglés) [11][12]:

El Reglamento eIDAS establece un marco único e interoperable para la identificación electrónica y los servicios de confianza para garantizar que las interacciones electrónicas entre empresas sean más seguras, rápidas y eficientes en toda la UE. Los proveedores de servicios de confianza que cumplan con los requisitos de eIDAS también pueden utilizar sus servicios como prueba en procedimientos judiciales. Ejemplos de servicios de confianza son las firmas electrónicas (para la expresión del acuerdo de una persona con el contenido de un documento o conjunto de datos), los sellos electrónicos (sello comercial), los sellos de tiempo electrónicos (conecta un documento electrónico a un momento determinado, proporcionando evidencia de que el documento existía en ese momento), Certificados de Autenticación de Sitio Web (certificados electrónicos de que un sitio web es confiable y fiable), o servicios de entrega electrónica registrada (para enviar datos de manera digital). En 2021, el Parlamento Europeo lanzó una propuesta de modificación del Reglamento eIDAS que introduce una serie de nuevos requisitos en esta ley, entre los que destaca la creación de un Monedero Europeo de Identidad Digital que deberá ser certificado por organismos de certificación acreditados por los supervisores de protección de datos. autoridades.

Reglamento de Gobernanza de Datos [13][14]:

Con el objetivo de crear un espacio de datos europeo único, la Comisión Europea lanzó su 'estrategia para los datos' en 2020, siendo la Ley Europea de Gobernanza de Datos uno de sus pilares clave. Su objetivo principal es facilitar el intercambio intersectorial de datos en los países de la UE, incluidos los requisitos de transparencia y la posibilidad de que los ciudadanos de la UE compartan sus datos para el bien público. Además, regula la reutilización de ciertas categorías de datos del sector público e introduce una nueva entidad en el ecosistema, el proveedor de punto único de información, una entidad que debe intermediar el acceso de los usuarios de datos a este sector de datos en particular. Además, regula el mercado de proveedores de servicios de intermediación de datos y organizaciones de altruismo de datos para facilitar que los interesados y titulares de datos compartan sus datos con entidades confiables e introduce una nueva autoridad supranacional, el Consejo Europeo de Innovación de Datos, que supervisar y asesorar a las autoridades nacionales en sus actividades de supervisión.

Ley de Datos [15]:

La Ley de Datos es el último bloque de construcción horizontal de la estrategia europea de datos y revisa ciertos aspectos de la directiva de 1996 sobre la protección legal de las bases de datos para hacer que los datos generados a partir de dispositivos de Internet de las Cosas (IoT, sigla en inglés) estén disponibles para el acceso y reutilizar. Además, incluye medidas para garantizar condiciones justas en los contratos de intercambio de datos entre PYMES y grandes empresas tecnológicas, garantías para proteger a los proveedores de datos contra la transferencia ilegal de datos fuera de la UE, y medios para que los organismos del sector público accedan y reutilicen datos del sector privado en circunstancias excepcionales, en particular en caso de una emergencia pública.

Propuesta de un Espacio Europeo de Datos Sanitarios [16]:

Esta propuesta es la primera que surge en la UE para la regulación de un espacio europeo común de datos para ayudar a las personas a tomar el control de sus datos de salud a través de un mayor acceso digital a sus datos de salud personales electrónicos, tanto a nivel nacional como europeo, y para apoyar su libre circulación, así como fomentar un mercado único de sistemas de historiales médicos electrónicos, dispositivos médicos y sistemas de inteligencia artificial (IA). Además, proporciona un conjunto de medidas para asegurar un uso secundario consistente, confiable y eficiente de los datos, p. ejem. para fines altruistas, como una mejor prestación de atención médica, una mejor investigación, innovación y formulación de políticas.

Ley de Inteligencia Artificial (IA) [17]:

La Ley de IA propone un enfoque basado en el riesgo para regular la implementación de sistemas de IA en la UE, estableciendo obligaciones para los proveedores y usuarios de IA en función del nivel de riesgo que dichos sistemas puedan generar. Los sistemas de IA de alto riesgo con un nivel inaceptable de riesgo para la seguridad de las personas están estrictamente prohibidos, incluidos los sistemas que implementan deliberadamente técnicas de manipulación, se utilizan para puntuación social o identificación biométrica remota, o se implementan para influir en los votantes en campañas políticas. Los sistemas de IA de uso general se pueden implementar si pueden garantizar la protección de los derechos fundamentales de los ciudadanos de la UE y pueden proporcionar medidas de transparencia, como el registro de evaluaciones de impacto de la IA. También se proporcionan exenciones para el uso con fines de investigación o para componentes proporcionados bajo licencias de código abierto.

Propuesta de una Europa Interoperable [18]:

Esta propuesta busca garantizar un enfoque de la interoperabilidad de la UE centrado en el ser humano mediante la creación de una estructura de gobernanza de la interoperabilidad que ayude a las administraciones públicas y al sector privado a trabajar juntos y establecer un ecosistema de soluciones de interoperabilidad para el sector público de la UE. Para apoyar la implementación de tales soluciones y monitorear su progreso, se creará una Junta Europea Interoperable, así

como un Portal Europeo Interoperable que actúe como un mercado para la reutilización de estas soluciones. Además, se promoverá el desarrollo de sandboxes regulatorios y serán obligatorias las evaluaciones de interoperabilidad, utilizadas para evaluar el impacto de los cambios en los sistemas de TI relacionados con la interoperabilidad transfronteriza en la UE.

4.4.2. Acuerdos

IDSA, en su 'Rule Book' [19], propone un conjunto de diferentes acuerdos para regir las actividades de un espacio de datos, en particular, acuerdos legales (*Legal Agreements*), técnicos (*Technical Agreements*), funcionales (*Functional Agreements*) y operativos (*Operational Agreements*), como se ilustra en la Figura 18. Acuerdos similares a estos se pueden encontrar en otros documentos relacionados con los espacios de datos, como, por ejemplo, en el Starter Kit del Data Space Support Centre (DSSC) o la Convergencia Técnica de DSBA. El resto de esta sección proporcionará detalles sobre cada tipo de acuerdo, así como enlaces a los recursos existentes para ayudar en su desarrollo/generación. La Figura 19 muestra un "Lienzo del ecosistema de datos" que se puede usar para describir los detalles comerciales y operativos de un espacio de datos.

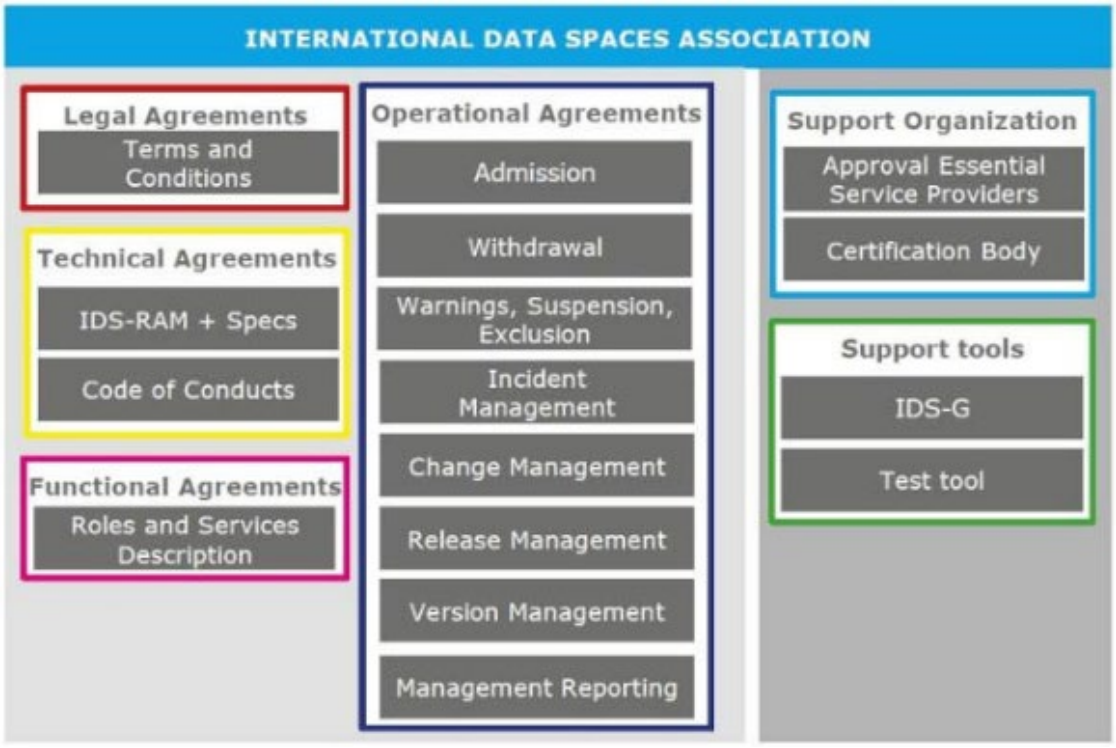

Figura 18: Tipos de acuerdos según IDSA. Extraído de [19, p. 7]

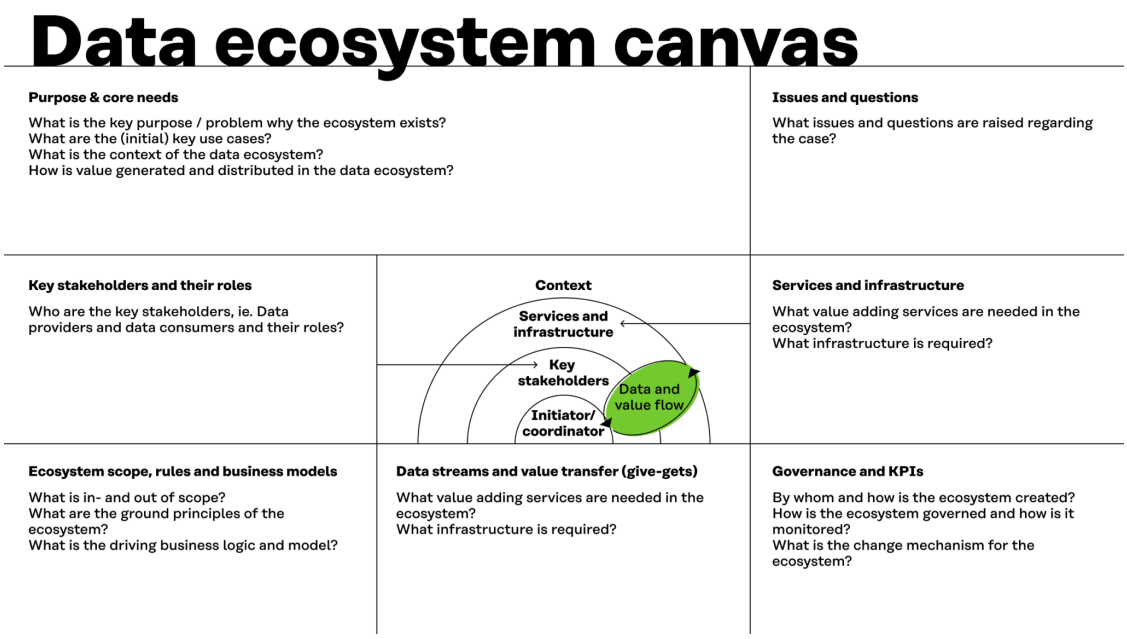

Figura 19: Lienzo de Sitra sobre los ecosistemas de datos. Extraído de [20, Ch. 3]

Acuerdos legales (o empresariales):

Los Términos y Condiciones y contratos que regulan el intercambio de datos entre los participantes del espacio de datos teniendo en cuenta los marcos legales aplicables mencionados en la sección anterior. El Sitra cuenta con plantillas para generar un documento de “Términos y condiciones generales", y un documento específico de “Términos de uso del conjunto de datos" para IDS, que también son promovidos por IDSA. La Figura 20 muestra una de las plantillas de Sitra para los Términos de Uso de un dataset.

DATA PROVIDER

_____ acts as the Data Provider.

SCHEDULES

Schedule	Description
1	Dataset Description [no. 1][29]
2	

BACKGROUND

The purpose of this Dataset Terms of Use is to define, the Data that the Data Provider makes available through the Network and to set out the terms and conditions for the use of such Data.

DEFINITIONS

As used in this Dataset Terms of Use, including the Schedules hereof, unless expressly otherwise stated or evident in the context, the following terms and expressions have the following meanings, the singular (where appropriate) includes the plural and vice versa, and references to Schedules and Sections mean the Schedules and Sections of this Dataset Terms of Use:

"Data Provider"	means the entity defined under section "Data Provider" above.
"User"	means any End User, Service Provider, Operator or Third Party End User who processes any Data that is made available by the Data Provider under these Dataset Terms of Use. [Otetaan kontrollilistaan kysymys siitä, että miten eri skenaarioissa mm. datan edelleen jakelu ja siihen liittyvät ehdot on määriteltävä]
"[defined term]"[30]	means [definition]

Figura 20: Plantilla para los Términos de Uso de un dataset. Extraído de [20]

Acuerdos técnicos:

Documentos que describen los componentes obligatorios y opcionales de los espacios de datos. Los acuerdos técnicos del marco IDS consisten en IDS-RAM y otras especificaciones para componentes, comunicación y control de uso, que se utilizan para crear los componentes básicos (ver Figura 8) de espacios de datos necesarios, así como los esquemas de certificación para garantizar la confianza en los componentes y participantes del espacio de datos, al tiempo que garantiza el cumplimiento de la RAM y las demás especificaciones. Además, Sitra cuenta con una herramienta de 'Modelo de madurez ética' (Figura 21) para ayudar en el desarrollo de dichos documentos.

	Security	Commitment to ethical practices	Transparency and communication	Sustainability	Human-centricity	Fair Networking	Purpose
Level 0	"I believe that this is very secure"	"We prefer not to commit, we are free"	"Just trust us"	"Let it burn"	"What this has to do with the people?"	"Anarchy"	"We do what we want to do"
Level 1	There are proper Antivirus, Firewall and other needed security tools in use and they are properly updated.	Organisation follows regulations and the best practices of its own field.	Organisation follows the regulations and uses truthful communication.	Organisation has documented sustainability plan/program.	The individuals are recognised as stakeholder and their rights are taken account.	Organisation aligns it rules and regulations to best practices of industry	Organization has stated reasons for data collection and usage
Level 2	There is a dedicated person to keep up with information security.	Organisation has implemented and is committed to following ethical code(s) or other codes of conduct.	Organisation supports open internal communication and responsible information sharing.	There is an evaluation model for sustainability with clear indicators.	The organisation collects information of the needs of individuals to improve people-centricity.	Organization defines and documents practices and provides the needed information for network partners	Organization has transparent rules how data can be used in the future
Level 3	There are clearly documented procedures for the preparation of security threats.	There are clear well documented procedures for actions to be taken when ethical issues occur.	There is a transparent, documented plan for internal and external communication	Organisation impact on the environment is neutral or positive.	Individuals have low-level ways to communicate with the organisation and their opinions are systematically noted.	Organisation supports and encourages a fair data sharing in ecosystems.	The organisation negotiates with information sources to gain mutual understanding of fair information use
Level 4	The whole organisation has internalised the importance of security and it is constantly monitored and developed through the organization.	Organisational policies and procedures are developed critically from ethical perspective together with all relevant stakeholders.	Organisation openly communicates its procedures and policies.	Organisation is actively advancing the sustainability of its business field.	Organisation will actively involve all relevant stakeholders in decision making.	Organisation actively seeks to ways to advance possibilities of whole ecosystems.	Organisation has clear, public, documented goals and procedure of information use

Figura 21: Modelo de madurez ética Sitra. Extraído de [20]

Acuerdos funcionales y operacionales:

Documentos que registren el ingreso y/o retiro de participantes en el espacio de datos, así como políticas de membresía, marcos de confianza y registros de sus roles, responsabilidades, actividades y políticas de acceso y uso de datos. Se debe proporcionar información sobre el descubrimiento de datos y los catálogos y recursos disponibles, además de los registros de incidentes, negociaciones de contratos, cambios o lanzamientos de servicios o cualquier otro cambio en los espacios de datos para el cumplimiento, la rendición de cuentas y la transparencia.

4.4.3. Auditorías

El registro de interacciones en el espacio de datos es un componente importante para un espacio de datos confiable y auditable. Diferentes iniciativas dan un nombre distinto a dicho servicio (Figura 10): FIWARE Foundation usa el término 'Servicio de registro' (*Logging Service*), mientras que Gaia-X usa 'Servicios de intercambio de datos' (*Data Exchange Services*) e IDSA 'Cámara de compensación' (*Clearing House*). Dichos servicios deben registrar una variedad de operaciones, desde intercambios de datos hasta pagos y registros de participantes, conectores, servicios o registros de uso de datos. Los registros de espacios de datos deben ser mantenidos y actualizados por las autoridades de espacios de datos y los desarrolladores de tecnología que utilizan tecnologías como el modelo de credenciales verificables para identificar a los participantes. Por ejemplo, Gaia-X proporciona un prototipo de un meta registro común que utiliza credenciales verificables, y tiene una instancia de API ejecutándose en https://registry.lab.gaia-x.eu/v1/docs/. La Figura 22 ilustra el proceso para registrarse como ancla de confianza en el Registro Gaia-X.

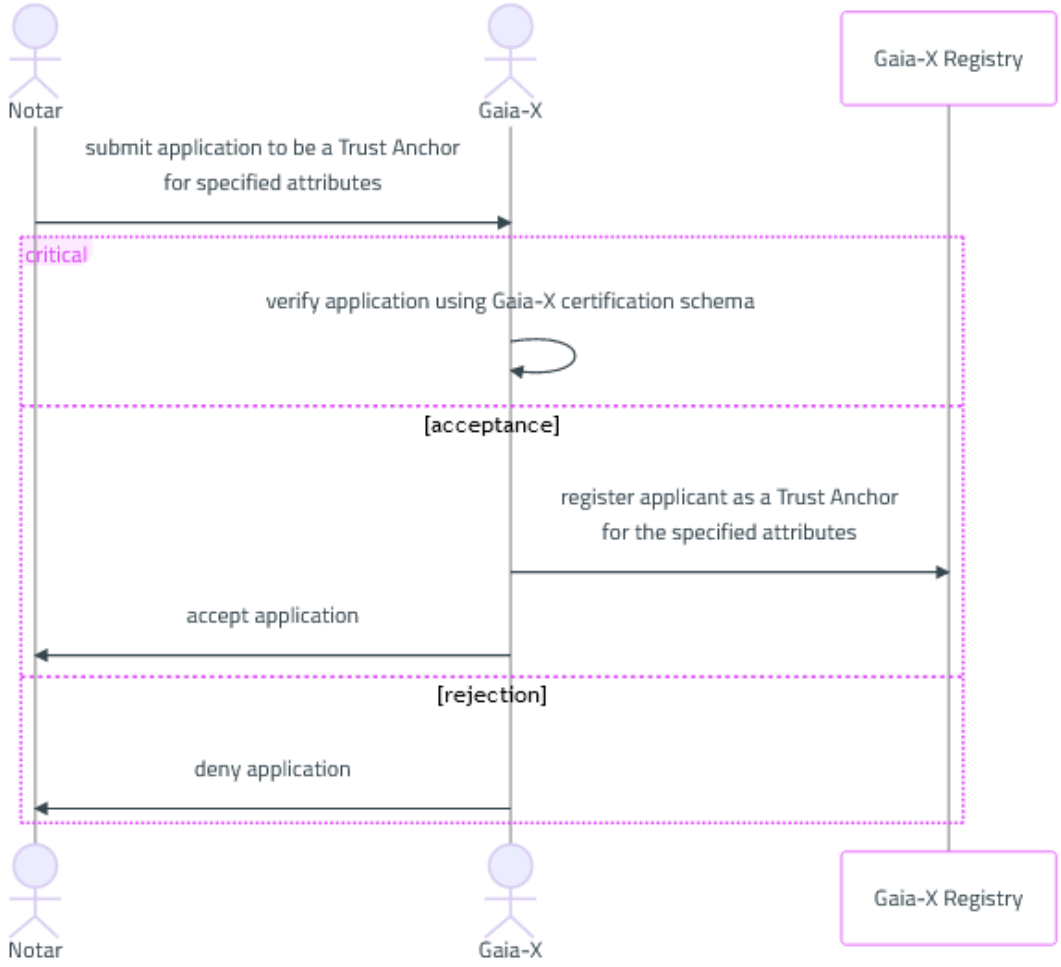

Figura 22: Diagrama de secuencia UML. Extraído de [21, Ch. 4]

La especificación de la Cámara de Compensación de IDSA proporciona un modelo para registrar información sobre el uso compartido y el uso de datos entre proveedores y consumidores, pagos y otros datos de procedencia, de acuerdo con los contratos de uso o las políticas de uso de datos. La Figura 23 ilustra las funciones de una Cámara de Compensación con respecto a las interacciones con los conectores IDS.

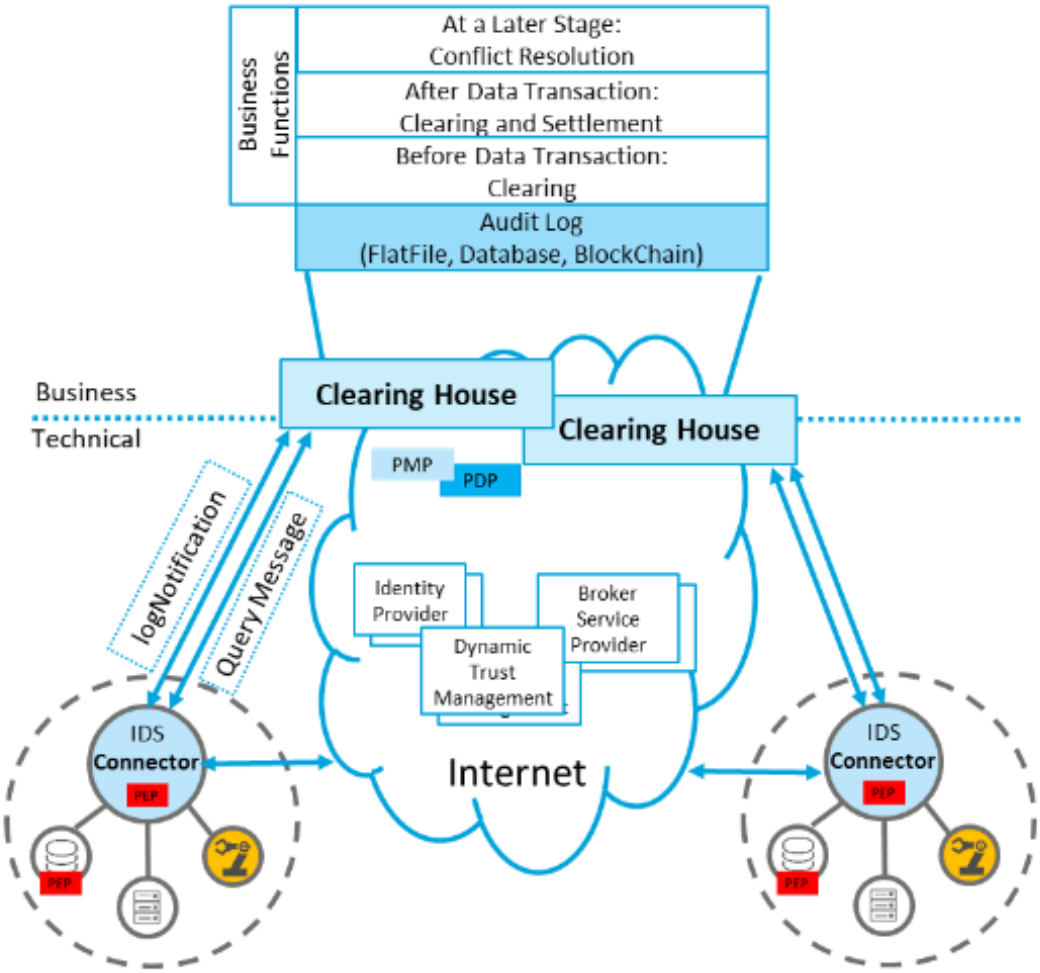

Figura 23: Las funciones de la Cámara de Compensación IDS. Extraído de [22, p. 5]

4.4.4. Gobernanza en INESData

En esta sección se presenta la definición del marco de Gobernanza necesario para la puesta en marcha del Espacio de Datos INESData. Con el fin de proporcionar una base sólida, se publican tres documentos básicos que actúan como guías y plantillas para la gobernanza de cualquier espacio de datos:

1) **Guía Práctica sobre Cuestiones de Cumplimiento con la normativa del Espacio de Datos** (ver Anexo 1):

El objetivo principal de este documento es ofrecer recomendaciones prácticas que promuevan un uso eficiente, seguro y alineado con la normativa vigente del Espacio de Datos Federado.

La guía ofrece recomendaciones prácticas en temas y procesos específicos relacionados con el cumplimiento bajo la lente de las regulaciones que incidirán sobre el Espacio de Datos, entre las

que se encuentran la Protección de Datos, la Gobernanza, la Calidad de los datos, la promoción de una adecuada competencia empresarial, y el alineamiento con la regulación de Inteligencia Artificial, todos ellos aspectos imprescindibles para la correcta gestión en este tipo de entornos.

Asimismo, esta Guía Práctica sobre Cuestiones de Cumplimiento está dirigida principalmente a los actores clave que desempeñan roles de responsabilidad en la gestión del Espacio de Datos, así como a los usuarios y consumidores finales que interactúan con este entorno.

2) **Definición de roles en la gobernanza del Espacio de datos** (ver Anexo 2):

Este documento aborda la definición de roles y un estudio de aplicabilidad inicial para establecer un sistema de gobernanza en el espacio de datos. Se centra en:

- Roles de Gobernanza: Identificar los principales roles para la toma de decisiones, basándose en normativas, modelos reconocidos y documentos de autoridades relevantes.
- Estudio de Aplicabilidad: Analizar cómo se aplican normativas de gobernanza, seguridad, privacidad y legislación sectorial al proyecto.

El documento es un estudio preliminar, limitado a ciertos roles concretos, y está sujeto a ajustes y mejoras a medida que el proyecto avanza, que serán recogidas en la versión final del *Handbook.*

3) **Modelos Contractuales Tipo definidos bajo el marco de gobernanza:** (ver Anexo 3)

Este documento define un **marco jurídico y operativo** para regular las relaciones entre los actores que participan en el acceso, intercambio y uso de datos en un Espacio de Datos. Este marco abarca varios documentos clave que definen las condiciones generales de participación, las responsabilidades de las partes, los derechos sobre los datos y las normas de gobernanza del Espacio. Incluye:

- **Acuerdo de Adhesión**: Formaliza la incorporación de nuevas partes al Espacio, especificando los términos y condiciones de adhesión. Tras el Acuerdo de Adhesión, las partes acuerdan suscribirse al Convenio Constitutivo, mediante el cual se establecen las bases para la creación y funcionamiento del Espacio de Datos.
- **Condiciones Generales**: Define responsabilidades, términos de participación, normas de confidencialidad, seguridad y cumplimiento normativo.
- **Modelo de Gobernanza**: Regula la organización y toma de decisiones, asegurando transparencia, equidad y eficiencia.
- **Condiciones Específicas de Uso del Conjunto de Datos**: Establece normas particulares para el tratamiento de datos dentro del Espacio. Estas condiciones incluyen aspectos relacionados con la licencia de uso de los datos, la protección de la privacidad y la seguridad, las limitaciones de uso y las responsabilidades en caso de incumplimiento.

Estos documentos sirven como punto de partida para abordar la compleja tarea de implementar un marco de gobernanza efectivo y confiable. INESData asume este desafío con el objetivo de

garantizar una gestión transparente, equitativa y eficiente en la puesta en marcha del Espacio de Datos INESData. Estos tres documentos se incluyen como Anexos a este entregable.

Bibliografía

[1] datos.Gob.es, "Características para la creación de espacios de datos," 2022.

[2] datos.Gob.es, "La importancia de desplegar espacios europeos de datos," 2022.

[3] IDSA, "Página web de IDSA - data spaces."

[4] Gaia-X, *Gaia-x architecture document - 22.10 release*. 2022.

[5] DSBA, *Technical convergence - discussion document. Version 2.0*. 2023.

[6] DSBA, *Data spaces business alliance hubs: Potential for synergies and impact*.

[7] K. Yasuda, M. Jones, and T. Lodderstedt, *OpenID for verifiable presentations - draft 18*. 2023.

[8] O. Terbu, T. Lodderstedt, K. Yasuda, and T. Looker, *Self-issued OpenID provider v2*. 2023.

[9] R. Iannella and S. Villata, "ODRL information model 2.2," *W3C*, 2018.

[10] "Reglamento (UE) 2016/679 del parlamento europeo y del consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la directiva 95/46/CE (reglamento general de protección de datos) [2016] OJ l 119/1."

[11] "Reglamento (UE) 910/2014 del parlamento europeo y del consejo, del parlamento europeo y del consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la directiva 1999/93/CE [2014] OJ l 257."

[12] "Propuesta de reglamento del parlamento europeo y del consejo por el que se modifica el reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un marco para una identidad digital europea) [2021] COM/2021/281 final."

[13] "Reglamento (UE) 2022/868 del parlamento europeo y del consejo de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el reglamento (UE) 2018/1724 (reglamento de gobernanza de datos)."

[14] "Comunicación de la comisión al parlamento europeo, al consejo, al comité econónimo y social europeo, y al comité de las regiones - una estrategia europea de datos [2020]."

[15] "Propuesta de reglamento del parlamento europeo y del consejo sobre normas armonizadas para un acceso justo a los datos y su utilización (ley de datos)."

[16] "Propuesta de reglamento del parlamento europeo y del consejo sobre el espacio europeo de datos sanitarios [2022] COM/2022/197 final."

[17] "Propuesta de reglamento del parlamento europeo y del consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la unión [2021] COM/2021/206 final."

[18] "Propuesta de reglamento del parlamento europeo y del consejo por el que se establecen medidas para un alto nivel de interoperabilidad del sector público en toda la unión (ley de europa interoperable)."

[19] S. Steinbuss, K. Ottradovetz, J. Langkau, M. Punter, and et.al, *IDSA rule book*. International Data Spaces Association, 2021.

[20] Sitra, *Rulebook for a fair data economy, version 2.0*. 2022.

[21] Gaia-X, *Gaia-x trust framework - 22.10 release*. 2022.

[22] S. Steinbuss, S. Bader, and et.al, *Specification: IDS clearing house*. International Data Spaces Association, 2020.

Anexo 1: Guía Práctica sobre Cuestiones de Cumplimiento con la normativa del Espacio de Datos

Contenido

1. Introducción

1.1 Propósito

Esta Guía Práctica sobre Cuestiones de Cumplimiento tiene el objetivo de proporcionar recomendaciones esenciales para el uso eficiente, seguro y alineado con la normativa vigente del Espacio de Datos Federado. A lo largo de la Guía, se abordarán aspectos cruciales como la Protección de los Datos, la Gobernanza, la Competencia y la Inteligencia Artificial, todos ellos imprescindibles para la correcta gestión en este tipo de entornos.

1.2 Alcance

En cuanto al alcance objetivo de esta Guía Práctica sobre Cuestiones de Cumplimiento, se proporcionarán recomendaciones prácticas en temas y procesos específicos relacionados con el cumplimiento bajo la lente de las regulaciones que incidirán sobre el Espacio de Datos, entre las que se encuentran la Protección de Datos, la Gobernanza, la Calidad de los datos, la promoción de una adecuada competencia empresarial, y el alineamiento con la regulación de Inteligencia Artificial.

Asimismo, esta Guía Práctica sobre Cuestiones de Cumplimiento está dirigida principalmente a los actores clave que desempeñan roles de responsabilidad en la gestión del Espacio de Datos, así como a los usuarios y consumidores finales que interactúan con este entorno.

1.3 Acrónimos

Acrónimo	Concepto
AEPD	Agencia Española de Protección de Datos.
CDO	Director del Dato.
DPD	Delegado de Protección de Datos.
EIPD	Evaluación de Impacto de Protección de Datos.
HRIA	Sistemas de Inteligencia Artificial de alto riesgo.
IA	Inteligencia Artificial.
LDC	Ley de Defensa de la Competencia.
LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
RAT	Registro de Actividades de Tratamiento.
RIA	Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial.
RGPD	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.

2. Recomendaciones prácticas

Las Recomendaciones Prácticas que se presentan a continuación están diseñadas para proporcionar una hoja de ruta detallada que guíe a los miembros del Espacio de Datos en la implementación de algunos puntos específicos. Estas directrices abarcan aspectos esenciales como la Protección de Datos, la Gobernanza y la Cadena de Custodia y Transferencia de Custodia, cada uno de los cuales desempeña un papel fundamental en la gestión de la información.

La Protección de Datos es el pilar que garantiza que toda la información gestionada dentro del Espacio se gestione de manera segura y conforme 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 (Reglamento General de Protección de Datos, en adelante "RGPD") y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante "LOPDGDD"). Este apartado ofrece recomendaciones específicas para mitigar riesgos en el ámbito del tratamiento de los datos, acorde con la Guía "Gestión del riesgo y evaluación de impacto en tratamientos de datos personales", publicada en junio de 2021 por la AEPD, así como aclaraciones sobre el papel del Delegado de Protección de Datos (en adelante, "DPD"), de los Encargados de Tratamiento y de la importancia del Registro de Actividades de Tratamiento en el contexto de los Espacios de Datos.

La Gobernanza del Espacio de Datos es crucial para establecer roles claros, responsabilidades y procesos que aseguren la alineación de la gestión de datos con sus objetivos. Para ello, se establecerán puntos de contacto claros, como la Oficina del Dato y el Director del Dato, quienes serán responsables de coordinar y supervisar todas las actividades relacionadas con la gestión de datos. Asimismo, se detallará el procedimiento administrativo aplicable al proveedor de servicios de intermediación de datos y se enfatizará la importancia de un registro exhaustivo de la procedencia, calidad e integridad de los datos, lo cual es esencial para asegurar la confianza en el uso de la información.

La Cadena de Custodia y Transferencia de Custodia se centra en asegurar un control continuo sobre el acceso y transferencia de datos a lo largo de su ciclo de vida. Este proceso garantiza que la trazabilidad y la integridad de la información se mantengan, especificando quiénes tienen acceso en cada fase y cómo se maneja cada traslado de los datos entre entornos, preservando así la seguridad y confiabilidad de la información.

Además de estos aspectos fundamentales, la Competencia es otro factor a tener en cuenta para asegurar que el Espacio de Datos se opera dentro de un marco justo y transparente. Atendiendo a la normativa española de competencia, la Ley 15/2007, de 3 de julio, de Defensa de la Competencia (en adelante, "LDC"), se proporcionarán los principios generales a seguir para no incurrir en conductas anticompetitivas y, así, fomentar la innovación y cooperación equitativa.

Por último, la integración de sistemas de Inteligencia Artificial en un Espacio de Datos plantea nuevos desafíos y responsabilidades relacionados con el cumplimiento normativo, la ética y la protección de derechos fundamentales. En este contexto, es esencial que el marco de gobernanza

del Espacio de Datos se alinee con el Reglamento de Inteligencia Artificial (Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo de 13 de junio de 2024) y con estándares internacionales como la ISO/IEC 42001:2023 y la ISO/IEC 23894:2023.

1.4 Protección de Datos

La Protección de Datos es un componente esencial en un Espacio de Datos, no solo para asegurar el cumplimiento del RGPD y de la LOPDGDD, sino que también fortalece la confianza de los usuarios finales en la gestión de los datos. Como tal, en este apartado se desglosan las mejores prácticas y requisitos esenciales para poder garantizar que los datos son tratados de manera responsable y conforme a la ley.

2.1.1. Encargados de Tratamiento

Dentro del proyecto es previsible que desplieguen distintos roles con relevancia para la regulación en protección de datos. Uno de ellos será la figura del encargado de tratamiento regulada por el artículo 28 del RGPD, que en el contexto de los Espacios de Datos se subsume en el rol de cualquier Proveedor de Servicios que tenga acceso a datos personales, independientemente de su papel dentro del Espacio. Por su parte, el Operador del Espacio de Datos actuaría como responsable del tratamiento, puesto que se erigiría como el garante de los derechos a la protección de datos de los interesados acorde a su definición en el artículo 24 del RGPD. Según lo estipulado en el artículo 28 del RGPD el Encargado es aquel que va a realizar un tratamiento por cuenta del responsable y que tendrá que cumplir con ciertas obligaciones. El responsable del Tratamiento puede elegir los Encargados de Tratamiento que considere, siempre y cuando estos ofrezcan garantías suficientes en cuanto a la implantación y el mantenimiento de las medidas técnicas y organizativas adecuadas.

En este sentido, el tratamiento de datos por parte del Encargado debe regirse por un contrato que le vincule con el Responsable. Para tal efecto, en el Anexo A de este documento, se pone a disposición un modelo de Contrato de Encargado de Tratamiento. Este contrato servirá como modelo estándar para formalizar la relación entre el Espacio de Datos, como Responsable del Tratamiento, y los proveedores de servicios que se subcontraten en el Espacio de Datos, asegurando que se cumplan todas las obligaciones legales.

2.1.2. Delegado de Protección de Datos

La figura del DPD es un rol clave en la estructura de cumplimiento del RGPD, cuya designación es obligatoria en ciertos casos específicos, conforme al artículo 37 del RGPD.

De esta forma, atendiendo al apartado 1 del artículo anteriormente mencionado, la designación de un DPD seria obligatoria en el caso de que, en el Espacio de Datos y concretamente acorde a su naturaleza, alcance y/o fines, se requiera de una observación habitual y sistemática de interesados a gran escala[1] o que se traten categorías especiales de datos (que abarcarían datos sanitarios,

[1] Según las Directrices sobre los delegados de protección de datos (DPD) redactadas por el Grupo de Trabajo de Protección de Datos del Artículo 29, para determinar que un tratamiento se realiza “a gran escala”, se debe tener en cuenta cuatro factores: el número de interesados afectados; el

afiliación política, creencias religiosas…), o datos personales relacionados con condenas e infracciones penales, a gran escala.

Sin embargo, incluso cuando no se cumple con uno de estos criterios, la designación de un DPD en el contexto de los Espacios de Datos es altamente recomendable debido a la complejidad tecnológica inherente a estos entornos y a su relevancia jurídica.

Concretamente, dado que los Espacios de Datos son entornos avanzados que implican el procesamiento de grandes volúmenes de información a través de tecnologías emergentes, se pueden generar riesgos de seguridad y privacidad de diversa naturaleza, es por ello que consideramos esencial la designación de un DPD que pueda alinear las exigencias tecnológicas con los requisitos legales, y ofrecer claridad jurídica en la toma de decisiones.

Además, la importancia jurídica de los Espacios de Datos radica en el tratamiento masivo de datos que realizan, por lo que se busca cumplir el principio de responsabilidad proactiva (artículo 5.2 del RGPD) y la designación de un DPD es una den las materializaciones directas de ese principio.

Por otra parte, la designación de un DPD es considerada una medida preventiva para evitar el incumplimiento normativo, puesto que este debe contar con conocimientos especializados de las prácticas en protección de datos, así como un profundo entendimiento de la naturaleza tecnológica necesaria para asesorar sobre la normativa vigente y su aplicación al contexto del Espacio de Datos. Es importante aclarar que el DPD debe actuar con un alto grado de independencia, lo que significa que este rol no puede asumir simultáneamente funciones directivas, asegurando así que sus decisiones sean tomadas de forma objetiva y centradas exclusivamente en la protección de datos.

Por último, cabe resaltar que el DPD tiene diversas responsabilidades que incluyen: supervisar el cumplimiento del RGPD y de la LOPDGDD; asesorar a los miembros del Espacio de Datos; coordinar y supervisar las Evaluaciones de Impacto; actuar como punto de contacto con la Agencia Española de Protección de Datos (en adelante, “AEPD”); entre otras.

2.1.3. Gestión de Riesgos

La Gestión de Riesgos en materia de protección de datos es un proceso que busca identificar, evaluar y mitigar las posibles amenazas que puedan afectar la seguridad y privacidad de los datos. Este proceso incluye una serie de acciones, que debe comenzar con la concepción y descripción del tratamiento de datos, asegurando el cumplimiento de los principios recogidos en el artículo 5 del RGPD.

Una vez esté garantizado el cumplimiento normativo del tratamiento, se deben identificar los riesgos que afectan al tratamiento de datos. De esta forma, se recomienda llevar a cabo una evaluación general de amenazas y riesgos del tratamiento, para identificar la probabilidad de los incidentes, y el impacto de su posible materialización. Las normas y estándares de seguridad de la

volumen de datos o la variedad de elementos de datos que son objeto de tratamiento; la duración, o permanencia, de la actividad de tratamiento de datos; y, el alcance geográfico de la actividad de tratamiento.

información pueden ayudar a detectar vulnerabilidades, identificando así también los requisitos y contramedidas que deben establecerse para la protección y seguridad de los datos.

Durante la evaluación de riesgos se deberán identificar las posibles consecuencias de distintas amenazas o escenarios para la seguridad del Espacio de Datos, y de los datos tratados, con el objetivo de valorar la probabilidad de que se produzca un incidente no deseado.

El resultado de la evaluación de riesgos debe compararse con el nivel de tolerancia de riesgos de privacidad. Si el nivel de riesgo es superior al nivel de riesgo aceptable, deberán aplicarse las medidas técnicas y organizativas adecuadas.

Si durante la evaluación del nivel de riesgo del tratamiento se detecta que el riesgo inherente de algún tratamiento conlleva un elevado riesgo, o se encuadra dentro de las situaciones propuestas en el artículo 35 del RGPD, es obligatorio realizar para ese tratamiento en concreto una evaluación de impacto, tal y como se describe en la siguiente sección.

Evaluación de Impacto de Protección de Datos (EIPD)

Después de realizar un análisis de riesgos general, y teniendo en cuenta las categorías de datos y las características de los tratamientos llevados a cabo por el Espacio de Datos, se debería elaborar lo que se conoce como una EIPD.

Según lo estipulado en el artículo 35.1 del RGPD, el objetivo de esta evaluación en el contexto del proyecto INESData sería valorar el impacto que la nueva tecnología utilizada sobre la correcta protección de los datos. Además, considerando lo establecido en el apartado 4 del artículo mencionado, la AEPD ha publicado un listado de los tipos de tratamientos de datos que requieren EIPD. En este sentido, bajo nuestro punto de vista, los Espacios de Datos federados que traten datos personales a gran escala se subsumen en el punto 10 de dicha lista, ya que son considerados una "tecnología a una nueva escala". Por lo tanto, se recomendaría la realización de una EIPD cuyo objetivo final es garantizar que dicho tratamiento sea lícito, adecuado e imprescindible para la finalidad pretendida, habiéndose adoptado, en su caso, las medidas técnicas y organizativas necesarias.

La evaluación de impacto de datos que deberá desarrollarse contendrá como mínimo:

- Una descripción sistemática de las operaciones de tratamiento previstas y los fines del tratamiento.
- Una evaluación de la necesidad y proporcionalidad del tratamiento en relación con los fines.
- Una evaluación de los riesgos para los derechos y libertades de los interesados.
- Las medidas técnicas y organizativas previstas para hacer frente a los riesgos, incluidas las garantías, medidas de seguridad y mecanismos para garantizar la protección de los datos y demostrar el cumplimiento de la normativa de protección de datos teniendo en cuenta los derechos e intereses legítimos de las personas afectadas.

En los casos en los que la evaluación de impacto indique que el tratamiento supondrá un alto riesgo a pesar de haber adoptado las medidas disponibles para mitigarlo, se procederá a la correspondiente consulta previa a la Autoridad de Protección de Datos, según estipula el artículo 36.1 del RGPD.

2.1.4. Registro de Actividades de Tratamiento (RAT)

La implementación de un RAT está estipulada en el artículo 30 del RGPD y es obligatoria cuando el tratamiento de datos conlleve un riesgo elevado. Dada la naturaleza tecnológica de los Espacios de Datos, que involucran grandes volúmenes de información y procesos complejos, el cumplimiento de este requisito es indispensable.

Aparte del cumplimiento normativo, el RAT tendría como función proporcionar transparencia y control de cómo se gestionan los datos dentro del Espacio de Datos. Además, podría servir como apoyo a la Gobernanza de Datos, puesto que en un entorno como el Espacio de Datos, donde actúan varios miembros involucrados en el tratamiento de la información, el RAT se convierte en una herramienta que facilita la coordinación entre ellos.

Por otra parte, puede ayudar a monitorear la calidad e integridad de los datos a lo largo de su ciclo de vida. Por último, también puede ser relevante en el caso de darse un incidente de seguridad o una auditoría de cumplimiento, puesto que facilita tanto la identificación de los datos que se vieron comprometidos, así como la preparación para demonstrar la conformidad con el RGPD.

Según el artículo 30 del RGPD, el RAT debe incluir información específica sobre cada actividad de tratamiento que se lleve a cabo dentro del Espacio de Datos. Los elementos que deben figurar en el registro son, entre otros:

- Nombre y datos de contacto del responsable del tratamiento.
- Explicación de los fines del tratamiento.
- Descripción de las categorías de interesados y de datos tratados.
- Categorías de destinatarios a quienes se comunican los datos personales.
- Identificación de cualquier transferencia de datos a países fuera del Espacio Económico Europeo.
- Tiempo durante el cual se conservarán los datos.
- Descripción general de las medidas de seguridad implementadas para proteger la información.

Es importante mencionar que es esencial que el RAT se mantenga actualizado, reflejando cualquier cambio en las actividades de tratamiento, por lo que requiere un proceso continuo de revisión y actualización.

Así, seria altamente recomendable la implementación de un RAT en el ámbito de la Protección de Datos, pues no solo cumple con las exigencias del RGPD, sino que también proporciona beneficios operativos significativos.

1.5 Gobernanza

La Gobernanza en el contexto de los Espacios de Datos federados se ha convertido en un pilar muy importante a través de los últimos avances regulatorios, ya que entre otras funciones permite que la información sea gestionada de manera adecuada, eficiente y segura dentro de estructuras organizacionales complejas, como es el caso de INESData. Por ello, se ha decidido dedicar en esta guía un apartado específico a esta materia, abordando las principales recomendaciones prácticas para una gobernanza efectiva, y definiendo los puntos de contacto clave en este contexto.

2.1.5. Provisión de servicio de intermediación de datos

En primer lugar, es importante aclarar que los servicios de intermediación de datos son aquellos que se ocupan de facilitar la conexión entre el titular de los datos y el usuario de los datos en el intercambio de datos. Por lo tanto, teniendo en cuenta esta definición, entendemos que los Espacios de Datos federados se encuadran en este concepto.

En este sentido, el Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724, establece, entre otros, un marco de notificación y supervisión para la prestación de servicios de intermediación de datos.

Como tal, los proveedores de servicios de intermediación de datos están sujetos al control y supervisión de la autoridad competente y deben cumplir con las obligaciones establecidas en el Reglamento anteriormente mencionado, que incluyen la notificación de su actividad, así como de cualquier cambio o cese.

Dicho esto, en este apartado se va a detallar el procedimiento de notificaciones de actividad y solicitudes (artículo 11.1 del Reglamento), teniendo en cuenta las indicaciones publicadas en la Página Web Oficial por la Secretaría del Estado de Digitalización e Inteligencia Artificial y la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

La solicitud telemática remitida al Ministerio debe incluir la siguiente información (artículo 11.6 del Reglamento):

- El nombre del proveedor que ofrece los servicios de intermediación de datos.
- Los detalles legales sobre el proveedor.
- La dirección principal del proveedor.
- La página web pública.
- La información de contacto del proveedor, incluyendo a las personas responsables y sus datos de contacto.
- Descripción del servicio de intermediación de datos, con una indicación de la categoría específica mencionada en el artículo 10 a que corresponda al servicio prestado.
- Una estimación de cuándo comenzará a ofrecer el servicio, si no es la misma fecha en que se notifica.

Para acceder al Formulario de Notificación de Actividad de Proveedores de Servicios de Intermediación de Datos, es necesario acceder mediante el siguiente enlace perteneciente a la Sede Electrónica.

2.1.6. Registro de la Actividad de Intermediación de Datos

Según lo establecido en el artículo 12 apartado o) del Reglamento de Gobernanza de Datos, que estipula las condiciones para la prestación de servicios de intermediación de datos, se deberá conservar un registro completo y actualizado de la actividad de intermediación de datos. En el caso del Proyecto INESData, el Operador sería el responsable por llevar a cabo esta tarea (véase el apartado 5.2.3. 15. p) de las Condiciones Generales).

Para que el registro sea considerado completo, debe contener, si se conoce la información y como mínimo el siguiente contenido:

- Una descripción adecuada del conjunto de datos.
- El título del conjunto de datos y el dominio.
- Una lista de los diccionarios de datos disponibles.
- Una lista de formatos disponibles.
- Una lista de los tipos de datos.
- Una lista de todas las políticas empleadas en la recopilación y preparación del conjunto de datos.
- Un historial de revisiones.
- Transformaciones preexistentes.
- La fecha en que se inició y la fecha de la última entrada del conjunto de datos.
- Un resumen estadístico.

A continuación, se desglosarán tres frentes en las que se debe actuar para hacer cumplir con el contenido anteriormente detallado y con el requisito del artículo 12 o) del Reglamento de Gobernanza de Datos.

Registro de procedencia de los datos

Para el tratamiento fiable de los datos compartidos en los Espacios de Datos Federados, es preciso conocer cada dato para establecer la confianza con los usuarios finales. Por ello, siguiendo estipulaciones similares contenidas en los estándares ISO/IEC 23751:2022, en las Especificaciones UNE 0080 y UNE 0079, se recomienda establecer un proceso de gestión de calidad e integridad de los datos, de manera que se garantice la trazabilidad de estos hasta su origen.

De esta forma, con respecto al Registro de Procedencia, este debe incluir información sobre la creación, actualización, transcripción, abstracción, validación y transferencia de la propiedad de los datos. Por lo tanto, se recomienda que este registro sea actualizado periódicamente e incluya, como mínimo, los siguientes apartados:

- Origen: lista de los agentes que han recopilado los datos.

- Titulares de los datos: información sobre el titular original y actual del conjunto de datos, así como todos los poseedores anteriores.
- Cambios: lista de actualizaciones, transcripciones, abstracciones o validaciones que se han aplicado a los datos compartidos.

Registro de Calidad e Integridad de los Datos

En cuanto a la Calidad de los Datos, los participantes en un proyecto de compartición de datos deben determinar sus propias características y requisitos. Es importante señalar que la Integridad de los Datos es un aspecto intrínseco de su calidad y afecta al resultado de las acciones sobre los datos. En este sentido, la integridad de los datos se define como la garantía de que los datos no han sido modificados o eliminados de manera no autorizada y no detectada, asegurando así que su significado no ha cambiado.

El rol particularmente importante en este ámbito es el Proveedor de Servicios (véase el apartado 5.2.6 de las Condiciones Generales) y el del Operador del Espacio de Datos. El primero es el responsable por crear conjuntos de datos completos y de calidad, colaborando, con el segundo en la conservación del registro de actividad.

Por lo tanto, el seguimiento detallado de la calidad e integridad de los datos puede permitir al usuario final determinar si el conjunto de datos cumple con sus requisitos:

- Precisión: establecer una lista de normas, tecnologías o técnicas utilizadas para garantizar la exactitud de los datos; una lista de los márgenes de error o incertidumbre conocidos para cada campo numérico del conjunto de datos; y, por último, una lista de métodos utilizados para garantizar que se respeta el formato de datos especificado para cada campo.
- Distribución: reflejar la distribución de los datos.
- Número de instancias duplicadas: si se conoce, determinar el número de instancias duplicadas en el conjunto de datos.
- Número de entradas que faltan: si se conoce, enumerar las entradas omitidas o nulas en el conjunto de datos.
- Valores atípicos: determinar el número de muestras de cada campo del conjunto de datos que se consideran valores atípicos.
- Datos imputados: reflejar en una lista los campos del conjunto de datos que incluyen datos imputados, así como los métodos utilizados para imputar datos en el Espacio de Datos.
- Datos sintetizados: del mismo modo, reflejar en una lista los campos del conjunto de datos que incluyen datos sintetizados, así como los métodos utilizados para sintetizar los datos.
- Integridad: reflejar en una lista cuales son los métodos utilizados para garantizar que no se ha alterado el significado de los datos del conjunto de datos.

Un modelo de evaluación recomendado por la Especificación UNE 0080 para verificar el cumplimiento del proceso de calidad de los datos establece cinco niveles de capacidad:

- Nivel 0. Incompleto: el proceso no está implementado.
- Nivel 1. Realizado: existe evidencia de la realización del proceso.

- Nivel 2. Gestionado: el proceso se gestiona y los productos de trabajo se establecen, controlan y mantienen.
- Nivel 3. Establecido: se utiliza un proceso adaptado basado en un proceso estándar.
- Nivel 4. Predecible: el proceso se gestiona usando técnicas cuantitativas.
- Nivel 5. Innovado: el proceso se mejora de forma continua para cumplir con los objetivos de negocio actuales y futuros.

Por su parte, la Especificación UNE 0079, una especificación para la Gestión de la Calidad del Dato que tiene en cuenta las características de calidad de la ISO/IEC 25012:2008, puede ayudar a determinar el nivel de capacidad en el que se encuentra el estado del dato. Las características a considerar son las siguientes:

- Exactitud: los datos representan correctamente el verdadero valor de los atributos previstos de un concepto en el Espacio de Datos.
- Completitud: los datos asociados tienen valores para todos los atributos esperados relacionados con el Espacio de Datos.
- Consistencia: los datos son coherentes con otros datos del Espacio de Datos.
- Credibilidad: los datos son considerados verdaderos y creíbles.
- Actualidad: los datos poseen atributos que tienen la edad adecuada.
- Accesibilidad: se puede acceder fácilmente a los datos.
- Cumplimiento: los datos se ajustan a las normas, convenciones o reglamentos vigentes y a normas similares relativas a la calidad de los datos.
- Confidencialidad: se puede garantizar que los datos sólo son accesibles e interpretables por miembros autorizados.
- Eficiencia: los datos pueden procesarse y proporcionar los niveles de rendimiento esperados utilizando las cantidades y tipos de recursos adecuados en un contexto de los Espacios de Datos.
- Precisión: los datos tienen atributos que son exactos o que proporcionan discriminación.
- Trazabilidad: los datos tienen atributos que proporcionan una pista de auditoría del acceso a los datos y de cualquier cambio realizado en los datos.
- Comprensibilidad: los datos poseen atributos que permiten su lectura e interpretación por parte de los usuarios, y se expresan en lenguajes, símbolos y unidades apropiados en el contexto de los Espacios de Datos.
- Disponibilidad: los datos poseen atributos que permiten su recuperación por los miembros del Espacio de Datos.
- Portabilidad: los datos poseen atributos que permiten instalarlos, sustituirlos o trasladarlos de un sistema a otro preservando la calidad existente.
- Recuperabilidad: los datos poseen atributos que les permiten mantener y preservar un nivel especificado de operaciones y calidad, incluso en caso de fallo.

Por lo tanto, considerando todo lo expuesto anteriormente, se recomienda implementar el siguiente plan de acción, compuesto por cuatro fases, en el ámbito del proceso de Calidad del Dato:

1. Planificación de calidad del dato.
2. Control y monitorización de calidad del dato.

3. Aseguramiento de la calidad del dato.
4. Mejora de calidad del dato.

Registro de Cadena Y de transferencia de custodia

Debido a lo recogido en el artículo 12 j) del Reglamento de Gobernanza de Datos se concluye que recae en las responsabilidades del Operador aplicar las medias técnicas, jurídicas y organizativas necesarias para las transferencias de los datos no personales.

Por lo tanto, de acuerdo con lo establecido en la ISO/IEC 23751:2022 y en línea con lo mencionado anteriormente, para garantizar la fiabilidad del tratamiento de los datos se debe registrar todas las acciones sobre los datos durante todo su ciclo de vida, manteniendo, de esta manera, una trazabilidad del mismo. Estas acciones forman parte de la Cadena de Custodia de los Datos e incluyen la creación de registros, la copia, la transferencia, la actualización, la transformación, el análisis, la elaboración de informes, el archivo y la eliminación.

A diferencia del mecanismo de Calidad del Dato explicado anteriormente, la Cadena de Custodia de los Datos no garantiza que el dato no haya sido alterado, pero sí asegura que cualquier alteración queda registrada.

Para mantener la trazabilidad en la cadena de custodia y realizar una prueba de conformidad, se debe registrar, como mínimo:

- Ingesta de datos: registrar cómo el titular de los datos transferirá la información compartida al usuario de los datos, y cómo este último la transferirá a su propio sistema de almacenamiento de datos.
- Almacenamiento de datos: las ubicaciones y tipos de almacenamiento que utilizará el usuario de los datos.
- Transformación de datos: las transformaciones que el titular de los datos ha aplicado a los datos, así como las que el usuario tiene previsto aplicar.
- Combinación con otros datos: todos los datos que el usuario planea cambiar con los datos compartidos.
- Otros tipos de tratamiento de datos: lista de otros tipos de tratamiento que el usuario tiene previsto aplicar a los datos compartidos.

En cuanto a la Transferencia de la Custodia, esta solo puede ser realizada por el usuario si el titular de los datos no ha impuesto ninguna restricción para dichas transferencias. Es necesario tener en cuenta los requisitos establecidos por el titular, tales como:

- Transferencias de custodia: lista de transferencias de custodia que el usuario tenga previsto aplicar a los datos.
- Finalidad de las transferencias: objetivo de la transferencia de custodia que el usuario tiene previsto aplicar a los datos.
- Datos que el usuario tiene previsto transferir: lista de destinatarios a quienes el usuario tiene previsto transferir el conjunto de datos compartido.

- Condiciones de transferencia de datos: términos y condiciones que se aplicarán a cualquier transferencia de custodia del conjunto de datos compartido.

2.1.7. Puntos de Contacto

En un entorno donde la gestión de datos implica múltiples roles, los puntos de contacto actúan en nombre del Operador como facilitadores del flujo de información, así como agentes de soporte en la gestión del dato. Como tal, sería recomendable que el Operador de Espacio de Datos estableciera estos Puntos de Contacto. Por último, es importante mencionar que para establecer las responsabilidades de estos agentes tuvimos en cuenta las directrices de la Especificación UNE 0077 de Gobierno del Dato publicada en marzo de 2023.

Director del Dato

El Director del Dato (*Chief Data Officer*, CDO) asume un papel estratégico y de representación del Gobierno del Dato dirigido por el Operador del Espacio de Datos. De esta forma, sus responsabilidades se centran en:

- Dirigir las iniciativas de datos en el entorno y gestionar la llevanza de la Gobernanza.
- Elaborar la estrategia de datos del Espacio de Datos, así como las respetivas prácticas y procedimientos.
- Supervisar la implementación del marco de gobernanza de datos desarrollado por la Oficina del Dato.
- Colaborar con los demás miembros del Espacio de Datos para asegurar que las políticas y procedimientos de Gobernanza son coherentes con las necesidades operativas.
- Junto al Comité Directivo establecer las estructuras organizativas necesarias y asignar los miembros adecuados para desempeñar las responsabilidades asignadas en la gestión de datos.
- Diseñar e implantar el sistema de Gobierno del Dato.
- Anticipar los requisitos de los datos a largo plazo.
- Influir en la mejora de la eficiencia y la efectividad de los procesos de gobierno, gestión y calidad del dato.
- Tomar decisiones estratégicas de política del dato para el Espacio de Datos.

Oficina del Dato

Por su parte, la Oficina del Dato es el equipo de trabajo que coordina el desarrollo de los diferentes componentes del sistema de gobernanza y gestión del dato. Sus responsabilidades de soporte al CDO se centran en:

- Asistir al director del Dato en la elaboración y ejecución de la estrategia de datos del Espacio de Datos, para lo cual contará con la participación del Comité Directivo, de los Comités Técnicos y de los Subcomités Especializados.
- Facilitar la coordinación entre los diferentes miembros para asegurar la alineación con la estrategia general de datos.
- Asegurar la correcta implementación de políticas y procedimientos relacionados con la gestión de datos.

- Supervisar que todos miembros del entorno cumplen con las políticas de datos establecidas, asesorándoles siempre que haga falta.
- Definir y aplicar métricas para evaluar la calidad e integridad de los datos en colaboración con los demás miembros del Espacio de Datos.
- Mantener un inventario actualizado de todos los datos gestionados por el Espacio de Datos.
- Crear y gestionar un catálogo de datos que facilite la accesibilidad y reutilización de los datos dentro del Espacio de Datos.
- Apoyar al Director del Dato en la identificación y catalogación de los riesgos asociados a los datos y desarrollar planes de mitigación para abordar los riesgos identificados. Para estas tareas puede contar con el apoyo de los miembros del Espacio de Datos, con el Comité Directivo y con el DPO.
- Apoyar al Director en la optimización de la calidad de los datos.
- Apoyar al Director del Dato en el diseño e implantación del sistema de Gobierno del Dato.
- Actuar como enlace entre el Director del Dato y el Comité Directivo para asegurar una gobernanza cohesiva.

En resumen, la Oficina del Dato es responsable por la operativización de la estrategia de datos, actuando principalmente como un centro de coordinación y soporte.

1.6 Competencia

La LDC regula las prácticas que afectan a la competencia en el mercado. Por ello, es fundamental que los Espacios de Datos se alineen con esta normativa para garantizar el normal funcionamiento del mercado y prevenir conductas que puedan distorsionar la competencia.

Como tal, los Espacios de Datos deben operar respetando los principios generales de competencia, que incluyen:

- Prohibición de prácticas anticompetitivas: No perseguir prácticas anticompetitivas, como el bloqueo, la limitación o dificultar de cualquier modo el acceso de otros usuarios terceros a los datos.
- Prevención de abuso de posición dominante: El Espacio de Datos debe abstenerse de realizar prácticas que puedan considerarse abusivas, tales como la imposición de precios excesivos, la restricción de acceso al Espacio de Datos para determinados proveedores o la imposición de condiciones comerciales injustas.
- Acceso no discriminatorio: Debe garantizarse que todos los proveedores de datos y usuarios tengan acceso equitativo al Espacio, sin discriminación basada en el origen, tamaño o influencia de los participantes.
- Transparencia en las condiciones generales: El modelo contractual "Condiciones Generales" deben ser transparentes y accesibles para todos los interesados, incluyendo la información sobre los precios y tarifas. De esta forma, se evitará la imposición de cláusulas que puedan distorsionar la competencia.
- Control de concentraciones: En el caso de que se produzcan concentraciones empresariales que afecten a la estructura del Espacio de Datos, estas deben ser previamente evaluadas y aprobadas, cuando proceda.

1.7 Inteligencia Artificial

El Reglamento de Inteligencia Artificial establece un conjunto de obligaciones para los operadores que desarrollan, implementan, utilizan o forman parte de sistemas de IA. Estas obligaciones

también se aplican a los miembros de un Espacio de Datos, ya que estos entornos federados pueden implicar el uso y gestión de sistemas de IA.

En primer lugar, es necesario clasificar el nivel de riesgo del sistema IA utilizado en el Espacio de Datos, determinando si se categoriza como riesgo inaceptable, alto, otros o no regulado. Teniendo en consideración las características del Espacio de Datos INESData, no se anticipa que el nivel de riesgo sea considerado alto. Sin embargo, si tras la realización de un proceso de gestión de riesgos y respetiva evaluación de impacto, el sistema de IA se clasifica como de "alto riesgo", los requisitos que deben cumplir los proveedores de HRAI's son:

- Establecer un sistema de gestión de riesgos.
- Gobernanza de los datos.
- Elaborar documentación técnica.
- Registrar automáticamente los eventos relevantes.
- Dar instrucciones de uso a los encargados de la implantación.
- Diseñar el sistema para permitir supervisión humana.
- Diseñar el sistema AI para alcanzar los niveles adecuados de precisión, solidez y ciberseguridad.
- Establecer un sistema de gestión de la calidad para garantizar cumplimiento.

En caso de incumplimiento de estas obligaciones, podríamos estar ante penalizaciones como: multas, responsabilidad civil y penal (por daños a terceros o violaciones de derechos fundamentales) y disminución de la confianza del mercado.

2.1.8. Sistema de Gestión de Sistemas de IA

Como se ha mencionado anteriormente, uno de los requisitos que deben cumplir los proveedores de HRAI's es implementar un Sistema de Gestión de la IA. Este marco estructurado y completo está destinado a validar la implementación, supervisión y mejora continua de los sistemas de IA. De esta forma, permitirá la alineación con el RIA y con el estándar ISO/IEC 42001:2023 sobre Sistemas de Gestión de la IA, garantizando que se utiliza la IA de manera ética y responsable.

En primer lugar, la creación de una política de uso de IA que incluya objetivos claros, compromiso con los requisitos regulatorios y enfoque en la mejora continua. En segundo lugar, las funciones en cuanto a la gestión de la IA deben definirse y comunicarse claramente mediante una política específica para asegurar la organización interna del Espacio de Datos. Además, el estándar enfatiza el proceso de evaluación continua del ciclo de vida del sistema de IA para medir el rendimiento y eficacia del sistema, lo cual puede incluir auditorías internas para verificar el cumplimiento y ajustar el sistema de gestión según los resultados.

Por otro lado, se resalta la importancia de documentar y gestionar los datos empleados, especificando, a través de un inventario, su procedencia, categorías y calidad. Este inventario permite asegurar la transparencia y trazabilidad requeridas por el RIA. Igualmente, es vital la identificación de riesgos y su evaluación continua permiten mitigar impactos potenciales sobre derechos fundamentales, teniendo en cuenta la criticidad de la tecnología y la sensibilidad de los

datos procesados. En ese caso, se debe realizar una evaluación de impacto alineada con los requisitos del RIA.

El último requisito que analizar seria asegurarse de que todas las partes y terceros comprenden sus responsabilidades. Una distribución clara de los riesgos, en función de los roles y responsabilidades, asegura un uso de la IA transparente y equitativo, tanto dentro del Espacio de Datos como a lo largo de toda la cadena de suministro.

EU AI Act	ISO/IEC 42001:2023
Sistema de gestión de riesgos	Requisitos 8.2-4 (llama a 6.1).
Gobernanza de los datos	Controles A.7.x (datos).
Documentación técnica	Controles A.6.x (CV sistema IA)
Registro automático eventos	Control A.6.2.8 (registro eventos).
Instrucciones de uso	Control A.8.2 (documentación usuario).
Supervisión humana	Controles A.3.2 (roles), A.4.6 (recursos), A.6.1.3 (CV), A.8.2 (doc. usuario) y A.9.x (uso responsable).
Niveles adecuados de precisión, solidez y ciberseguridad	Controles A.3.x (roles), A.4.x (recursos), A.5.x (evaluación del impacto), A.6.x (CV), A.7.x (datos), A.8.2 (doc. usuario), A.9.3 (uso responsable) y A.10.x (proveedores).
Sistema de gestión de la calidad	ISO 42001

Figura 1-1: Correlación de obligaciones entre el RIA y la ISO/IEC 42001:2023

El cumplimiento de los requisitos de la ISO/IEC 42001:2023 aporta múltiples beneficios que refuerzan la integración de la IA en un Espacio de Datos. La norma permite posicionar la IA como un elemento estratégico, asegurando que su implementación esté alineada con los objetivos del Espacio y contribuyendo a consolidad la IA como un activo para la competitividad. Además, fomenta el desarrollo de una política de uso responsable, estableciendo directrices para el uso ético de la IA. También garantiza la calidad y seguridad de los datos empleados, aspectos cruciales para la precisión y fiabilidad de los sistemas de IA. De igual manera, la ISO/IEC 42001:2023 impulsa una cultura de gestión de riesgos, orientada a identificar, evaluar y mitigar posibles efectos de la IA en las operaciones y derechos de los usuarios.

Por último, pero no menos importante, este marco facilita el cumplimiento de las obligaciones impuestas por el RIA en el contexto de los Espacios de Datos y se extiende a la cadena de suministro, asegurando coherencia normativa en todas las interacciones y operaciones relacionadas

con IA. La adopción de la ISO/IEC 42001:2023 permite así alcanzar un nivel elevado de cumplimiento y fomentar prácticas de IA que contribuyan de manera positiva en el entorno.

2.1.9. Documentación Técnica de modelos de IA

La Documentación Técnica, establecida en el artículo 11 del RIA, tiene como objetivo proporcionar transparencia y garantizar la trazabilidad de los sistemas de IA, en este caso, en los Espacios de Datos. Esta documentación debe estar detallada y actualizada, proporcionándose de manera clara y completa todos los aspectos técnicos del sistema, desde su diseño hasta su implementación y mantenimiento. Es importante destacar que esta documentación técnica debe mantenerse adecuadamente actualizada durante toda la vida útil del sistema de IA (Considerando 71 del RIA).

Los componentes esenciales de la documentación técnica están descritos en el Anexo IV del RIA, son:

- Descripción general del sistema de IA;
- Descripción detallada de los elementos del sistema de IA y de su proceso de desarrollo;
- Modelos y datos utilizados;
- Información detallada acerca de la supervisión, el funcionamiento y el control del sistema de IA;
- Evaluaciones de rendimiento y seguridad;
- Procedimientos de mantenimiento y actualización;
- Descripción detallada del sistema de gestión de riesgos;
- Descripción de los cambios pertinentes realizados por el proveedor en el sistema a lo largo de su ciclo de vida;
- Una lista de las normas armonizadas, aplicadas total o parcialmente;
- Registro de incidencias y soluciones;
- Una copia de la declaración UE de conformidad;

Así, en el caso de que, después de realizar un análisis de riesgo, se concluya que el sistema se clasifica como de "alto riesgo", habría que cumplir con los requisitos del Anexo IV, referentes al artículo 11 del RIA.

2.1.10. Análisis de Riesgos y Evaluación de Impacto

Para cumplir con el requisito de realizar un análisis de riesgos, tanto proveniente del RIA como de la ISO/IEC 42001:2023, el Espacio de Datos puede alinearse con la "ISO/IEC 23894:2023 Tecnologías de la Información — Inteligencia Artificial — Directrices en la Gestión de Riesgos" que proporciona orientaciones sobre la gestión de riesgos en el contexto de la IA. Este estándar es fundamental para garantizar que los sistemas de IA operan de manera segura, confiable y ética, ayudando a identificar y mitigar posibles impactos técnicos, éticos y legales en la operación de los sistemas. Además, refuerza la gobernanza de la IA, aportando un soporte esencial en la toma de decisiones y planificación estratégica.

La ISO/IEC 23894:2023 subraya la necesidad de un enfoque de gestión de riesgos integrado en todas las actividades y funciones del entorno, de forma que la gestión de riesgos en IA sea un

elemento central y no un proceso aislado. Esta integración requiere compromiso de los miembros, especialmente del responsable que es quien debe comunicar políticas y declaraciones claras relacionadas con los riesgos de IA y su gestión, lo cual fortalece la confianza de las partes interesadas en el uso responsable de estos sistemas.

El estándar proporciona directrices detalladas para evaluar y abordar factores organizativos externos e internos, tales como los factores sociales, culturales, políticos, legales, tecnológicos y económicos. Entender este contexto amplio es esencial para una gestión de riesgos efectiva, ya que los riesgos de IA pueden variar significativamente en función de estos aspectos.

Así, se identifica varias fuentes de riesgo específicas para sistemas de IA, cada una de las cuales puede afectar la fiabilidad y seguridad de los sistemas. Estas incluyen los riesgos inherentes a entornos complejos, donde el sistema puede enfrentarse a condiciones impredecibles; la falta de transparencia y explicabilidad, que pone en riesgo la capacidad de los usuarios y otras partes interesadas para comprender las decisiones de IA y su fundamentación; y el nivel de automatización, donde la toma de decisiones automatizada puede afectar la seguridad o equidad de los resultados.

Asimismo, se enfatiza los riesgos en los procesos de aprendizaje automatizado, especialmente en lo referente a la calidad y representatividad de los datos, así como la protección durante la recolección y entrenamiento de los modelos. En cuanto a los riesgos de infraestructura, el estándar considera los posibles problemas derivados de hardware defectuoso, restricciones de red o ineficacias en la transferencia de modelos entrenados. Además, destaca la importancia de una planificación exhaustiva durante todas las fases del ciclo de vida del sistema, desde el diseño, la verificación, hasta la validación, asegurando así que el sistema de IA se ajuste a los diferentes contextos de uso para los que está destinado.

Por otro lado, el estándar recalca la necesidad de la mejora continua de los procesos de gestión de riesgos, de manera que estos se ajusten a cambios dentro del entorno, avances en técnicas de IAA y la incorporación de nuevas prácticas o normativas. Esta mejora continua también exige una documentación rigurosa y mantenimiento de registros sobre la gestión de riesgos, lo cual refuerza la transparencia y facilita la trazabilidad de las decisiones tomadas a lo largo del ciclo de vida del sistema de IA.

Para realizar el análisis de riesgos, primero se deben identificar y documentar amenazas y vulnerabilidades. Luego, los riesgos deben evaluarse en términos de probabilidad de ocurrencia y el impacto potencial. Por último, se priorizarán aquellos riesgos con mayor criticidad, considerando factores como impacto en privacidad, seguridad, reputación y continuidad de negocio.

En caso de que el análisis de riesgos clasifique al sistema de IA como “alto riesgo”, será necesario llevar a cabo una evaluación de impacto, conforme al artículo 27 del RIA, para mitigar efectos en derechos y libertades. Esta evaluación deberá incluir, como mínimo, la descripción de los procesos en los que se usará el sistema, el período de uso, la frecuencia prevista, los colectivos afectados,

los riesgos identificados, las medidas de supervisión humana aplicadas, y una propuesta de mitigación y monitoreo continuo.

ANEXO A

Modelo de Contrato de Encargado de Tratamiento:

Modelo Contrato de Encargado de Tratamiento

De una parte,

[*], con C.I.F. **[*]** y domicilio social en **[*]**, representada en este acto por D./Dña. **[*]**, mayor de edad, con D.N.I. número **[*]**. Actúa en su calidad de apoderado/a, según resulta de la escritura de poder otorgada ante el Notario de **[*]**, D./Dña. **[*]**, el **[día]** de **[mes]** de **[año]**, con el número **[*]** de su protocolo, debidamente inscrita en el Registro Mercantil de **[*]**.

En adelante, esta entidad será denominada la "**Operador**" o el "**Responsable del Tratamiento**".

De otra parte,

[*], con C.I.F. **[*]** y domicilio social en **[*]**, representada en este acto por D./Dña. **[*]**, mayor de edad, con D.N.I. número **[*]**. Actúa en su calidad de apoderado/a, según resulta de la escritura de poder otorgada ante el Notario de **[*]**, D./Dña. **[*]**, el **[día]** de **[mes]** de **[año]**, con el número **[*]** de su protocolo, debidamente inscrita en el Registro Mercantil de **[*]**.

En adelante, esta entidad será denominada el "**Proveedor**" o el "**Encargado del Tratamiento**".

En lo sucesivo el Operador y el Proveedor serán denominados conjuntamente como las "**Partes**" e individual e indistintamente como la "**Parte**".

Las Partes se reconocen recíprocamente capacidad legal suficiente para suscribir el presente Contrato de Encargado del Tratamiento de datos de carácter personal (el "**Contrato**") y a tal efecto,

EXPONEN

I. Que entre las Partes existe una relación contractual de prestación de servicios de **[*]** (los "**Servicios**") en cuya virtud el Proveedor deberá acceder a datos de carácter personal responsabilidad del Operador.

II. Que, en virtud de las disposiciones contenidas en el Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (el "**RGPD**"), resulta necesario regular las obligaciones asumidas por las Partes en virtud de su relación contractual en materia de protección de datos.

III. Que, conforme a los expositivos anteriores, las Partes convienen la celebración de este Contrato, que se regirá por lo establecido en el artículo 28 del RGPD, y especialmente por las siguientes:

ESTIPULACIONES

Primera.- Objeto

Para la prestación de los Servicios y ejecución de las prestaciones derivadas del cumplimiento de la relación contractual existente entre las Partes, el Proveedor podrá tener acceso a determinados datos de carácter personal responsabilidad del Operador y, en particular, a los siguientes:

Identificación de la información afectada. Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, el Operador, responsable del tratamiento, pone a disposición del Proveedor, encargado del tratamiento, la información que se describe a continuación:

- **[*]**
- **[*]**
- **[*]**

Categorías de interesados. Interesados cuyos datos puedan estar contenidos en la documentación que el Proveedor pueda llegar a solicitar por muestreo en el marco de la prestación de los Servicios (usuarios finales, proveedores, empleados, etc.).

Naturaleza de los tratamientos. Mediante las presentes cláusulas se habilita al Proveedor, encargado del tratamiento, para tratar por cuenta del Operador, responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio de **[*]**.

El tratamiento consistirá en: **(descripción detallada del servicio)**.

La prestación de servicios por parte del Proveedor implica la realización de los siguientes tratamientos: recogida, registro, estructuración, conservación, extracción, consulta, cotejo, limitación, supresión y destrucción **(eliminar los que no se apliquen)**.

Segunda.- Entrada en vigor y duración

El presente Contrato entrará en vigor en la fecha de su firma y estará vigente hasta la finalización de los Servicios.

Una vez finalice el presente contrato, el encargado del tratamiento debe ***suprimir/devolver al responsable/devolver a otro encargado que designe el responsable*** **(indicar la opción que proceda)** los datos personales y suprimir cualquier copia que esté en su poder.

Tercera.- Obligaciones del Encargo del Tratamiento

El Proveedor, en su calidad de encargado del tratamiento, declara y garantiza al Operador lo siguiente:

a) Que cuenta con suficiente capacidad técnica para cumplir las obligaciones derivadas de la relación contractual que mantiene con el Operador con pleno respeto a la normativa en

materia de protección de datos de carácter personal, pudiéndose comprometer, en la medida en que la prestación de los Servicios lo requiera, al cumplimiento de las exigencias del RGPD.

b) Que mantendrá el secreto y la confidencialidad de los datos de carácter personal responsabilidad del Operador a los que tendrá acceso.

c) Que tratará los datos de carácter personal a los que tendrá acceso exclusivamente por cuenta del Operador y, en todo caso, de conformidad con las instrucciones que le sean transmitidas por el Operador. Del mismo modo, se obliga a destinar los citados datos únicamente a la prestación de los Servicios y, en consecuencia, a no utilizarlos o aplicarlos de ninguna forma que exceda dicha finalidad.

d) Que no comunicará a terceros, ni siquiera para su conservación, los datos a los que tenga acceso en virtud de la prestación de los Servicios, ni tampoco las elaboraciones, evaluaciones o procesos similares que lleve a cabo con dichos datos, ni duplicará o reproducirá toda o parte de la información, resultados o relaciones sobre dichos datos, exceptuando aquellos supuestos en que legalmente resulte exigible.

e) Que pondrá a disposición del Operador toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realice el Operador, u otro auditor en su nombre.
Las auditorías podrán realizarse periódicamente, sobre una base planificada o "ad hoc", previa notificación con un plazo de preaviso razonable, en el horario laboral habitual del Proveedor. Los requisitos anteriores no serán de aplicación en caso de que la auditoría sea iniciada por una autoridad competente o en caso de que el Operador considere de forma razonable que estos requisitos previos podrían poner en peligro el propósito de la auditoría.
En caso de que la auditoría diese como resultado que el Proveedor, o los tratamientos de datos de carácter personal realizados por el Proveedor, no se ajustan a la normativa en materia de protección de datos que resulte de aplicación, las Partes deberán analizar dicho resultado y, en relación a dicho incumplimiento, el Proveedor deberá adoptar de inmediato todas las acciones rectificativas necesarias para su cumplimiento según lo estipulado con el Operador. En caso de no proceder a las subsanaciones necesarias, el Operador podrá resolver la relación contractual que mantiene con el Proveedor por incumplimiento de éste.

f) Que tendrá designado un delegado de protección de datos o un responsable de la llevanza de esta área y cumplimiento de la legislación de protección de datos, y comunicará su identidad y datos de contacto del Operador. En caso de que el Proveedor no tenga la obligación de designar a un delegado de protección de datos, éste deberá comunicar este hecho al Operador mediante declaración responsable.

g) Que garantizará 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 les informará convenientemente. Para ello, el

Proveedor mantendrá a disposición del Operador la documentación acreditativa del cumplimiento de la obligación establecida en este párrafo.

h) Que garantizará la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales bajo su cargo.

i) Que dará apoyo al Operador en la realización de las evaluaciones de impacto relativas a los datos de carácter personal a los que tenga acceso, cuando proceda y así lo solicite el Operador.

j) Que dará apoyo al Operador en la realización de las consultas previas a la autoridad de control, cuando proceda.

k) Que, en caso de que el Proveedor considere que el cumplimiento de una determinada instrucción del Operador pudiese comportar un incumplimiento del RGPD o de cualesquiera otras normas aplicables que lo modifiquen o complementen, el Proveedor deberá comunicarlo inmediatamente al Operador y solicitar a ésta que retire, enmiende o confirme la instrucción pertinente. El Proveedor podrá suspender la aplicación de la instrucción pertinente a la espera de la decisión del Operador que corresponda respecto a la retirada, enmienda o confirmación de la instrucción correspondiente.

l) Que aportará al Operador, como muy tarde en la fecha de firma de este Contrato, un certificado emitido por una empresa externa que acredite la adecuación de los procesos, sistemas y medidas de seguridad aplicadas por el Proveedor en el marco del tratamiento de datos a que se refiere el presente Contrato, a lo dispuesto en el RGPD y en cualesquiera otras normas aplicables que lo modifiquen o complementen; y aportará periódicamente al Operador durante la vigencia del presente Contrato, al menos una vez cada dos años, un certificado emitido por un auditor externo que acredite las circunstancias expresadas en esta cláusula.

m) Que, al finalizar la prestación de los Servicios, y a solicitud del Operador, destruirá o devolverá con carácter inmediato al Operador, según el Operador lo indique, los datos de carácter personal a los que haya tenido acceso, así como los documentos o soportes en que cualquiera de estos datos conste. En especial, el Proveedor se obliga a devolver o destruir: (i) los datos incluidos en ficheros responsabilidad del Operador, que ésta hubiera puesto a disposición del Proveedor como consecuencia de la prestación de los Servicios; (ii) aquellos que, en su caso, hubiesen sido generados a raíz del tratamiento por parte del Proveedor de los datos responsabilidad del Operador; y (iii) todos los soportes o documentos en que cualquiera de estos datos consten. No procederá la destrucción de los datos cuando exista una obligación legal de conservación, en cuyo caso el Proveedor devolverá al Operador, según esta le indique, los datos, debiendo garantizar este último dicha conservación.

n) Que implantará los mecanismos para: (i) garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; (ii) restaurar la disponibilidad y el acceso a los datos de forma rápida, en caso de incidente físico o técnico; (iii) verificar, evaluar y valorar, de forma regular, la eficacia de las medidas

técnicas y organizativas implantadas para garantizar la seguridad del tratamiento; y (iv) seudonimizar y cifrar los datos, en su caso.

o) Que el Proveedor notificará, como encargado del tratamiento, al Operador, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24 horas, y a través de correo electrónico, cualquier incidente, sospechado o confirmado, relativo a la protección de los datos, cualquier tratamiento de datos que pueda considerarse ilícito o no autorizado, cualquier pérdida, destrucción o daño de datos -de carácter personal dentro del área de responsabilidad del Proveedor (causada por el Proveedor, su personal, agentes o subcontratistas) y cualquier incidente que pueda ser considerado una vulneración de seguridad de los datos, junto con toda la información relevante para la documentación y comunicación de la incidencia a las autoridades o a los interesados afectados. En este sentido, 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, 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;
- 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; y
- Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Adicionalmente, el Proveedor iniciará de inmediato una investigación completa de las circunstancias relacionadas con dicho incidente y presentará al Operador su informe u observaciones sobre la misma, colaborando plenamente con la investigación que pudiera realizar el Operador y prestándole la asistencia requerida para la investigación de dicho incidente. Asimismo, asistirá al Operador, en caso de producirse una violación de la seguridad de los datos personales, de manera que se garantice el cumplimiento de las obligaciones de notificación de una violación de la seguridad de los datos personales de acuerdo con el RGPD (en particular, arts. 33 y 34 del RGPD) y de cualesquiera otras normas aplicables que lo modifiquen, complementen o que en el futuro puedan promulgarse.

p) Que asistirá al Operador cuando ésta le requiera, mediante simple solicitud, proporcionándole cualquier clase de información y/o documentación que ésta precise para la adecuada respuesta al ejercicio de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento y/o portabilidad de datos que pudiera recibir de los interesados, todo ello en plazos razonables y, en cualquier caso, con antelación suficiente para que el Operador pueda cumplir con aquellos plazos que legalmente resulten de aplicación para la atención de los citados derechos.

q) Que, en aquellos supuestos en los que el Proveedor recibiera directamente una solicitud de acceso, rectificación, supresión, oposición, limitación del tratamiento y/o portabilidad por el afectado, titular de los datos objeto de tratamiento, se compromete a dar traslado de dicha solicitud al Operador inmediatamente, al objeto de que ésta pueda atenderla en los plazos legalmente establecidos.

r) Subcontratación **(elegir 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 **[*]**, 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 **[*]**.

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 subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

s) Que mantendrá por escrito un registro de todas las categorías de actividades de tratamiento efectuadas en virtud del Contrato, de acuerdo con el art. 30.2 del RGPD, y que contenga:

- El nombre y los datos de contacto del Proveedor y, en su caso, del Operador o del Proveedor y del delegado de protección de datos;
- Las categorías de tratamientos efectuados en virtud del Contrato; y
- En caso de realizarse transferencias internacionales (que deberán estar, en todo caso, regularizadas o autorizadas por el Operador), la identificación del tercer país de destino de los datos responsabilidad del Operador y la documentación de garantías adecuadas.

t) Que no llevará a cabo transferencias internacionales de los datos de carácter personal responsabilidad del Operador a los que tenga acceso, salvo que cuente con la autorización previa y por escrito del Operador o se encuentren debidamente regularizadas.

u) Que el Proveedor dispondrá de una descripción general de las medidas técnicas y organizativas de seguridad relativas a: (i) la seudonimización y el cifrado de datos personales, en su caso; (ii) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; (iii) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico; y (iv) el proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Asimismo, el Proveedor se compromete a implementar todas aquellas medidas técnicas y organizativas en materia de seguridad que resulten aplicables de conformidad con lo previsto en el RGPD (en particular y con carácter no limitativo, las previstas en su artículo 32) y en cualesquiera otras normas aplicables que lo modifiquen, complementen o sustituyan. En el contexto particular de esta relación, tras la realización del análisis de riesgo pertinente, ambas partes han convenido que las medidas de seguridad concretas que el Proveedor debe implementar en relación con los datos tratados en virtud de este Contrato son las indicadas en el Apéndice I.

Dichas medidas de seguridad, y cualesquiera otras que deban implementarse podrán ser modificadas a instancias del Operador al objeto de acomodarlas a cambios normativos o a variaciones en la tipología de datos de carácter personal a los que el Proveedor vaya a tener acceso.

Si con posterioridad a la formalización del Contrato, el Operador exigiera al Proveedor la adopción o mantenimiento de medidas de seguridad distintas de las pactadas en esta cláusula y especificadas en el Apéndice I, o bien fuera obligatorio adoptarlas por cualquier norma que en el futuro pudiera promulgarse, y ello afectase de forma relevante a los costes de realización de los Servicios contratados, el Proveedor y el Operador acordarán las medidas oportunas para solventar dicha situación. Para mayor claridad, se deja constancia de que la adopción de las medidas de seguridad que resulten exigibles por razón de los requerimientos dimanantes del RGPD o de las normas estatales que lo complementen no

se considerará motivo para justificar una modificación de los precios de los Servicios que se puedan ver afectados por la adopción de dichas medidas.

Cuarta.- Prohibición de otros usos

De conformidad con lo establecido en la legislación de protección de datos, el Proveedor será considerado responsable del tratamiento en el caso de que destine los datos a otras finalidades, los comunique o los utilice incumpliendo las estipulaciones del presente Contrato, respondiendo de las infracciones en que hubiera incurrido personalmente.

Quinta.- Cláusula de responsabilidad

El Proveedor reembolsará al Operador el importe de las sanciones que eventualmente pudiera imponerle la Agencia Española de Protección de Datos o cualquier otra instancia competente por el incumplimiento o cumplimiento defectuoso de la normativa aplicable respecto de los cuales se determinase que el Proveedor o el subencargado al que hubiera contratado, fuese responsable, por derivarse de incumplimientos por su parte de las obligaciones asumidas por el Proveedor en materia de protección de datos, en virtud del presente Contrato. El Operador comunicará inmediatamente al Proveedor los procedimientos sancionadores eventualmente iniciados por la Agencia Española de Protección de Datos o cualquier otra instancia competente contra el Operador por tales incumplimientos o cumplimientos defectuosos, para que el Proveedor pueda asumir a su cargo la defensa legal, debiendo el Proveedor actuar, en todo momento, de forma coordinada con el Operador y preservando la imagen del Espacio de Datos.

El Proveedor mantendrá indemne al Operador frente a las reclamaciones, indemnizaciones, acciones y gastos derivados de reclamaciones de las personas afectadas que el Operador venga obligada a satisfacer por sentencia firme o laudo dictados por un tribunal competente, o bien en virtud de un acuerdo alcanzado por el Operador con los terceros reclamantes, que se deriven del incumplimiento o cumplimiento defectuoso de la normativa aplicable respecto de las cuales se determinase que el Proveedor o el subencargado al que hubiera contratado, fuese responsable por derivarse de incumplimientos imputables al Proveedor de las obligaciones asumidas por los mismos en materia de protección de datos de carácter personal en virtud del presente Contrato. A estos efectos, las Partes acuerdan que (i) el Operador deberá notificar por escrito al Proveedor las reclamaciones o acciones de los terceros reclamantes y los hechos que hubiesen dado lugar a las mismas; (ii) la defensa será dirigida por el Operador, coordinadamente con el Proveedor; (iii) el Operador podrá alcanzar con los terceros reclamantes los acuerdos extrajudiciales que estime convenientes, viniendo el Proveedor obligado a reembolsar Al Operador el importe de la indemnización y, en su caso, los gastos de asistencia letrada, procuradores o cualquier otro gasto al que el Operador haya tenido que hacer frente con causa en reclamaciones o acciones de terceros que se tratan en el presente párrafo.

Sexta.- Información en materia de protección de datos

6.1. Información a los firmantes

Las Partes tratarán los datos personales de los firmantes de este Contrato y representantes de la otra Parte con la finalidad de poder llevarlo a cabo, sobre la base de legitimación del interés legítimo de cada Parte en poder desarrollar y mantener la presente relación contractual. Los datos podrán ser conservados después del término de este Contrato (debidamente bloqueados, en caso de ser aplicable) por el plazo de prescripción de las acciones legales que pudieran derivarse del tratamiento. Los interesados podrán ejercitar, en cualquier momento, sus derechos de acceso, rectificación, supresión, limitación del tratamiento y oposición contactando directamente con la Parte correspondiente en la dirección señalada en el encabezamiento del Contrato. Adicionalmente, los interesados tienen derecho a poner una reclamación ante la Agencia Española de Protección de Datos (www.aepd.es) si consideran que sus derechos no han sido atendidos de acuerdo con su solicitud.

Salvo en los casos incluidos en la siguiente tabla, las Partes informan a los firmantes y representantes de que sus datos personales no serán comunicados o cedidos a terceras partes, y que sus datos no serán objeto de transferencias internacionales fuera del Espacio Económico Europeo.

	EL ESPACIO DE DATOS:	EL PROVEEDOR:
Delegado de Protección de Datos (DPO)[2]	**[*]**	**[*]**
Cesiones de datos	**[*]**	**[*]**
Transferencias Internacionales[3]	**[*]**	**[*]**
Encargados del Tratamiento[4]	**[*]**	**[*]**

6.2. Información a datos de contacto y empleados del Proveedor

Las Partes se comprometen y obligan a facilitar la información contenida en la presente cláusula a todos los empleados, representantes o personas de contacto de su organización cuyos datos personales vayan a ser facilitados a la otra Parte en el marco de este Contrato.

Y en prueba de conformidad, las partes firman el presente Contrato por duplicado y a un solo efecto en el lugar y fecha indicados en el encabezamiento.

EL OPERADOR **EL PROVEEDOR**

[2] En caso de no tener un DPO, por favor, deben incluirse los datos de contacto del responsable de privacidad o contacto encargado para cuestiones de privacidad en el Espacio de Datos.

[3] Destino de los datos transferidos y garantías utilizadas.

[4] Proveedores de servicios que podrán tener acceso a los datos personales de los firmantes bajo las instrucciones de cada Parte, con indicación al menos del sector (p.ej.: proveedores de tecnología, conservación de datos, servicios administrativos, asesoramiento legal etc.).

D./Dña. _____ D./Dña. _____

APÉNDICE I

Medidas de seguridad a implementar por el encargado del tratamiento respecto de los datos tratados en virtud del presente Contrato

Las medidas de seguridad que deberá implementar el Proveedor deberán cumplir, al menos, las garantías señaladas a continuación. En todo caso, el Proveedor facilitará al Operador un listado exhaustivo de las medidas de seguridad que tiene implementadas. El DPO del Espacio podrá formular recomendaciones de mejora:

- Funciones y obligaciones del personal: Serán definidas y asignadas todas las responsabilidades de la seguridad de la información.

- Registro de incidencias: Se registrará toda incidencia que afecte a los datos de carácter personal. En la incidencia se registrará el tipo de incidencia, momento en que se ha producido, persona que la notifica, persona a la que se comunica y efectos derivados tal como indica el procedimiento.

- Control de accesos: Los usuarios accederán únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones. Se mantendrá elaborada una relación actualizada de los usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos, así como establecidos los mecanismos necesarios para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados. Exclusivamente el personal autorizado para ello podrá conceder, alterar o anular el acceso autorizado sobre los datos y recursos.

- Proceso formal para el control y gestión de las autorizaciones respecto a los sistemas de información y siguientes dispositivos:

- Se mantendrá un control en la entrada y utilización de instalaciones, tanto habituales como alternativas.
- Se mantendrá un control en la entrada de equipos en producción, en particular, equipos que involucren criptografía.
- Se mantendrá un control en la entrada de aplicaciones en producción.
- Se mantendrá un control en el establecimiento de enlaces de comunicaciones con otros sistemas.
- Se mantendrá un control en la utilización de medios de comunicación (tanto habituales como alternativos).
- Se mantendrá un control en la utilización de soportes de información.
- Se mantendrá un control en la utilización de equipos móviles.

- Gestión de soportes y documentos: Los soportes y documentos que contengan datos de carácter personal permitirán identificar el tipo de información que contienen, ser inventariados y solo serán accesibles por el personal autorizado. Se garantizará la correcta conservación, localización y consulta de los documentos y posibilitar el ejercicio de derechos. Se protegerán adecuadamente los soportes que abandonen las instalaciones de la organización y todo soporte que salga de las

instalaciones se mantendrá cifrado. Siempre que se vaya a desechar cualquier documento o soporte que contenga datos de carácter personal se procederá a su destrucción o borrado, mediante la adopción de las medidas necesarias para evitar el acceso a la información contenida en el mismo o su recuperación posterior. Los dispositivos de almacenamiento que contengan datos de carácter personal especialmente sensibles dispondrán de mecanismos que obstaculicen su apertura, o en su defecto, medidas que impidan el acceso de personas no autorizadas.

- Identificación y autenticación: Se garantizará la correcta identificación y autenticación de los usuarios con acceso a datos de carácter personal. Se establecerán mecanismos que permitan la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información donde se encuentren los datos de carácter personal y la verificación de que está autorizado. Si el mecanismo de autenticación se basa en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad. Las contraseñas se cambiarán con una periodicidad que en ningún caso será superior a un año, y mientras estén vigentes se almacenarán de forma ininteligible.

- Copias de respaldo y recuperación: Se verificará la definición y correcta aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos. Se realizarán copias de respaldo, al menos semanalmente, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

- Los procedimientos establecidos para la realización de copias de respaldo y para la recuperación de los datos garantizarán en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. En caso de que la pérdida o destrucción afectase a tratamientos parcialmente automatizados, se procederá a grabar manualmente los datos quedando constancia documentada de este hecho. Se verificará cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos de carácter personal.

- Seguridad en los accesos a datos a través de redes de comunicaciones: Se garantizarán las medidas de seguridad exigibles a los accesos a través de redes de comunicaciones manteniendo un nivel de seguridad equivalente a los accesos en modo local anteriormente mencionados. Se realizarán mediante protocolos de comunicación seguros (SSH, SFTP, Editran, SSL, IPSec VPN, etc.).

- El desarrollo de software: El desarrollo de software se realizará sobre la base de las mejores prácticas de la industria, velando en todo el ciclo de desarrollo del software (diseño, desarrollo y prueba) por la seguridad de la información. El desarrollo de las aplicaciones web se basarán en directrices de codificación enfocando la seguridad de aplicaciones informáticas desarrolladas en todas sus dimensiones: personas, procesos y tecnologías. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado. Si está previsto realizar pruebas con datos reales, previamente se realizará una copia de seguridad.

Anexo 2: Definición de roles en la gobernanza del Espacio de datos

Contenido

1. Introducción

El propósito inicial de este documento será el de establecer un sistema de Gobernanza basado en roles, bajo los cuales se erigirán los principales órganos que llevarán a cabo la toma de decisiones dentro del espacio de datos. Estos roles han sido extraídos de los principales cuerpos normativos, documentos publicados por las principales autoridades de control, así como modelos reconocidos y disertaciones publicadas en la materia.

Finalmente, presentaremos los resultados extraídos del estudio de aplicabilidad inicial realizado para el proyecto, centrándonos en su aplicabilidad particularizada que los ámbitos normativos de Gobernanza, Seguridad, Privacidad y Legislación Sectorial podrán tener para el proyecto.

1.1. Definiciones y Acrónimos

1.1.1. Definiciones

No se estima necesaria la inclusión de definiciones específicas para la comprensión de los contenidos del presente documento.

1.1.2. Acrónimos

Acrónimo	Concepto
AEPD	Agencia Española de Protección de Datos
DGA	Data Governance Act
DA	Data Act
DSA	Digital Services Act
ENS	Esquema Nacional de Seguridad
EHDSR	European Health Data Space Regulation
ENS	Esquema Nacional de Seguridad
IDSA	International Data Spaces Association
LDC	Ley de defensa de la competencia
LGPDGDD	Ley de Protección de Datos y Garantías de Derechos Digitales
LGC	Ley General sobre condiciones generales de la contratación
LGT	Ley General de Telecomunicaciones
LSSICE	Ley de servicios de la sociedad de la información y de comercio electrónico
RGPD	Reglamento General de Protección de Datos
RDLSRSI	Real Decreto-Ley de seguridad de las redes y sistemas de información
RDDSRSI	Real Decreto de Desarrollo de seguridad de las redes y sistemas de información
UPM	Universidad Politécnica de Madrid

2. Modelo de Roles

En el contexto del Proyecto INESDATA, específicamente en sus Espacios de Datos, el marco de gobernanza jugará un papel crucial en la gestión diaria y en la toma de decisiones llevadas a cabo por sus órganos de gobierno. Es por ello que una clara definición de roles, aun en las fases iniciales del proyecto, se articula como uno de los primeros pasos a dar para alcanzar una correcta asignación de responsabilidades dentro de la plataforma y una nomenclatura común.

Después de realizar una lectura analítica de diversas fuentes, tanto normativas como documentales, hemos extraído una clasificación aproximada de cuáles serán los roles esenciales, así como un acercamiento a aquellas figuras complementarias que podrían materializarse en los demostradores. A continuación, se detallan a alto nivel las características de cada uno de estos roles.

2.1. Roles Esenciales para el funcionamiento de la plataforma

En general podemos identificar los siguientes roles esenciales, sin los cuales no podría plantear un verdadero marco mínimo de gobernanza en un espacio destinado a la intermediación de datos:

2.1.1. Titular de los Datos

Primera figura esencial desde la que se inicia el proceso de puesta a disposición de datos en una plataforma. En el Reglamento de Gobernanza de Datos se define al titular de datos como "*toda persona jurídica […] o persona física que no sea el interesado con respecto a los datos específicos en cuestión, que, de conformidad con el Derecho de la Unión o nacional aplicable, tenga derecho a conceder acceso a determinados datos personales o no personales o a compartirlos*"[1], de manera ligeramente más extensa el Reglamento de datos entiende como titular "*una persona física o jurídica que tiene el derecho o la obligación […] de utilizar y poner a disposición datos, incluidos, cuando se haya pactado contractualmente, los datos del producto o los datos de servicios relacionados que haya extraído o generado durante la prestación de un servicio relacionado*"[2]. Aprovechando este estudio, se ha considerado relevante consultar la propuesta de Reglamento sobre el Espacio Europeo de Datos Sanitarios, a pesar de encontrarse actualmente en proceso de aprobación y que su contenido se centra en una tipología de datos especifica, definiendo al titular de los datos como "*toda persona física o jurídica […] que tengan el derecho o la obligación, de conformidad con el presente Reglamento, con el Derecho de la Unión aplicable o con la legislación nacional por la que se aplique el Derecho de la Unión, o, en el caso de los datos no personales, mediante el control del diseño técnico de un producto y de los servicios conexos, de*

[1] Artículo 2.8 del DGA

[2] Artículo 2.10 del DA

poner a disposición, así como de registrar o entregar determinados datos, restringir el acceso a ellos o intercambiarlos"[3].

Continuando con definiciones distintas a las presentes en cuerpos normativos, encontramos que desde la Asociación Internacional de Espacios de Datos se define el titular como "una entidad que posee la autoridad suficiente para decidir como terceros pueden usar sus datos"[4]de forma similar pero más concisa esta figura aparece en un artículo monográfico titulado "*Elementos de un espacio de Datos*" de la Asociación profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información como "*aquel titular de los derechos de acceso y utilización de los datos*"[5] . Por otro lado, cabe puntualizar que la Agencia Española de Protección de Datos, al trasponer la definición establecida en el Reglamento de Gobernanza, hace una aclaración pertinente para el rol de titular, indicando que "*en marcos generales de Espacios de Datos se puede encontrar esta figura etiquetada como el "dueño de los datos" o "custodio de los datos". Esta denominación es engañosa cuando se refiere a datos personales, porque un responsable de tratamiento no posee los datos de los Interesados o Sujetos de los Datos, sino que dispone de una base jurídica que lo legitima para su tratamiento*"[6], alineándose con la definición aportada en el caso del Reglamento sobre el Espacio Europeo de Datos Sanitarios y atribuyendo, como veremos en el punto siguiente, la propiedad de los datos a los sujetos en caso de que los datos a disponer sean de carácter personal.

En síntesis, todas las definiciones aportadas coinciden en un elemento común, la capacidad de disponer de derechos de acceso sobre los datos para ser otorgados a posibles terceros. Esta figura, como veremos a continuación, difiere en ciertos aspectos rol de proveedor de datos, puesto que no tienen que ser directamente los titulares de los datos los que proporcionen los datos al espacio o plataforma, pudiendo hacer uso de intermediarios que lleven a cabo negociaciones por cuenta de varios titulares simultáneamente.

2.1.2. Proveedor de los Datos

La figura del proveedor de datos es algo particular, ya que no se encuentra explícitamente definida ni en el Reglamento de Gobernanza de Datos, ni en el Reglamento de Datos, ni en ninguna otra normativa europea de gobernanza; esto se debe a que se trata de una figura de carácter funcional. La asociación internacional de espacios de datos lo ha definido como "*Toda entidad responsable de recoger y preprocesar datos, así como ponerlos a disposición de terceros por cuenta del Titular de los datos*"[7]. De manera similar, la Asociación profesional de Cuerpos Superiores de Sistemas y Tecnologías de la

[3] Artículo 2.2.y) del EDSR

[4] Apartado 2.4.2 del documento "Design Principles for Data Spaces (IDSA)[Abril 2021]

[5] Página 2 del documento "*Elementos de un espacio de Datos"* (Francisco Javier Esteve Pradera)[Junio 2022]

[6] Apartado IV.A.2 del documento "*Aproximación a los Espacios de Datos desde la perspectiva del RGPD*" (AEPD) [Mayo 2023]

[7] Apartado 2.4.2 del documento "Design Principles for Data Spaces (IDSA)[Abril 2021]

Información ofrece una descripción en la misma línea "*Un proveedor de datos recoge datos y los ofrecen en el espacio de datos por medio del catálogo de datos*"[8].

La clave de la descripción de esta figura que la diferencia del rol de titular es la negociación, el contacto y la puesta a disposición directa del catálogo de los datos a posibles terceros interesados. Esta figura se despliega habitualmente sobre la misma entidad que la del titular, sin embargo, esta no es una condición sine qua non, puesto que existen diversos modelos de gobernanza mediante los que un proveedor actúa por cuenta de un conjunto plural de varios titulares, vinculado a ellos contractualmente, con el fin de poner a disposición de una plataforma concreta diversos catálogos de datos bajo una temática común.

2.1.2.1. Principales responsabilidades del proveedor de datos extraídas de la normativa

Los principales deberes indicados expresamente dentro del bloque normativo de gobernanza que, bajo el proyecto INESDATA, pueden asociarse a la figura del proveedor de datos son:

Obligaciones legales	
Reglamento (UE) 2022/868 de gobernanza de datos	Velar por la firma de contratos que no constituyan derechos exclusivos sobre los datos, para su reutilización por entidades distintas de las partes en tales acuerdos o prácticas. Excepto en aquellos casos que prevalga el interés general.
	Establecer condiciones de reutilización trasparentes, proporcionadas y no discriminatorias. Ajustándose estrechamente a las categorías y naturaleza de datos reutilizados.
	Velar por preservar la naturaleza protegida de los datos, concediendo acceso para su reutilización únicamente cuando el proveedor haya garantizado un método efectivo de control de divulgación de la información comercial de carácter confidencial y provea de un entorno de tratamiento seguro controlado por el proveedor.
	Reservarse el derecho a prohibir la utilización de aquellos resultados que contengan información que ponga en peligro los derechos e intereses de terceros. Llegando a prohibir en su caso la utilización de los resultados al reutilizador de forma comprensible y trasparente.
	Asistir a los reutilizadores potenciales en la obtención del consentimiento de los interesados o del permiso de los titulares de datos cuyos derechos e intereses puedan verse afectados por la reutilización, siempre que ello sea factible sin acarrear cargas desproporcionadas para el organismo del sector público.
	Velar por que los datos confidenciales no se divulguen como consecuencia de permitir la reutilización.
	Proporcionar orientación y asistencia a los reutilizadores para que cumplan con sus obligaciones.
	Valorar la posibilidad de cobrar una tasa trasparente, no discriminatoria y proporcionada por permitir la reutilización. El pago de estas tasas podrá efectuarse en línea, a través de servicios transfronterizos de pago de uso

[8] Página 2 del documento "*Elementos de un espacio de Datos"* (Francisco Javier Esteve Pradera)[Junio 2022]

	generalizado, y se calcularán en función de los costes relacionados con la tramitación de las solicitudes de reutilización.
	Ofrecer los contenidos del conjunto de datos proporcionados, las restricciones de utilización, las licencias, la metodología de recopilación de datos y la calidad e incertidumbre de los datos descritos en un formato de lectura mecánica.
Reglamento (UE) 2023/2854 de Datos	Los proveedores de datos constituidos como personas jurídicas, distintos de organismos del sector público, proporcionarán a organismos del sector público los datos que obren en su poder sobre los que se demuestre una necesidad excepcional.
	Cuando el titular de datos o proveedor reciba una solicitud de puesta a disposición de datos de un organismo del sector público, la Comisión, el Banco Central Europeo o un organismo de la Unión que demuestre una necesidad excepcional, pondrá los datos a disposición del organismo del sector público solicitante sin demora indebida, teniendo en cuenta las medidas técnicas, organizativas y jurídicas necesarias.
	El titular o proveedor de datos tendrá derecho a una compensación justa por poner a disposición datos en cumplimiento de una solicitud presentada por un organismo público. Tal compensación cubrirá los costes técnicos y organizativos soportados para dar cumplimiento a la solicitud, incluidos, en su caso, los costes de anonimización, seudonimización, agregación y de adaptación técnica, más un margen razonable.
Reglamento (UE) 2018/1807 para la libre circulación de datos no personales en la Unión Europea	El proveedor de datos no impondrá entre las condiciones de uso de los datos que proporcione al espacio requisitos de localización específicos, salvo que estén justificados por razones de seguridad pública de conformidad con el principio de proporcionalidad.
Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.	Velar porque los documentos en posesión del proveedor de datos público puedan ser reutilizados para fines comerciales o no comerciales, sin estar sujetos a condiciones específicas a menos que estas sean objetivas, proporcionadas, no discriminatorias y estén justificadas por un objetivo de interés público.
	En caso de existir condiciones de utilización fijar las mismas en licencias-tipo, las cuales podrán estar disponibles en formato digital y ser procesadas electrónicamente.
	Promover que la puesta a disposición de los datos para su reutilización, así como que la tramitación de solicitudes de reutilización se realice por medios electrónicos.
	Proporcionar en formato abierto, accesible, legible por máquina, y conjuntamente con sus metadatos. Su formato y los metadatos, en la medida de lo posible, deberán cumplir estándares y normas formales abiertas.
	En caso de proporcionar datos dinámicos para su reutilización estos se inmediatamente después de su recopilación, a través de interfaces de programación de aplicaciones (API) adecuadas. En caso de no poder proporcionar los datos dinámicos inmediatamente después de su recopilación, se proporcionarán en un plazo determinado o con

	restricciones técnicas temporales que no perjudiquen indebidamente su potencial económico y social.
	Esta puesta a disposición de los datos para su reutilización por medios electrónicos deberá realizarse en los términos establecidos por las normas reguladoras de la Administración electrónica, la interoperabilidad y los datos abiertos.
	Velar por la firma de contratos que no otorguen derechos exclusivos, y mantener una reutilización abierta a todos los agentes potenciales del mercado, incluso en aquellos casos en los que varios agentes exploten ya productos con valor añadido basados en estos documentos. Solo será admisible la suscripción de acuerdos exclusivos cuando sean necesarios para la prestación de un servicio de interés público, y por un plazo inferior a 10 años por regla general.
	Poner a disposición del público las condiciones finales de los acuerdos que, sin conceder expresamente un derecho exclusivo, conlleven una disponibilidad limitada a terceros para la reutilización de la información.
	El proveedor podrá aplicar, en aquellos supuestos no excluidos en la legislación, una tarifa por el suministro de datos para su reutilización limitada a los costes marginales en que se incurra para su reproducción, puesta a disposición, difusión, y protección. Pudiendo ser incrementado por un margen de beneficio razonable de la inversión.
	Sin perjuicio de lo anterior, se fomentará el uso de licencias abiertas con las mínimas restricciones posibles sobre la reutilización de la información. Reflejando la misma, al menos, información relativa a la finalidad concreta para la que se concede la reutilización, indicando igualmente si la misma podrá ser comercial o no comercial, o la duración de la licencia.
	El proveedor deberá nombrar o determinar la unidad responsable dentro de su organización de garantizar la puesta a disposición de su información.

2.1.3. Supervisor de Solicitudes

El supervisor de solicitudes es definido por la Agencia Española de Protección de datos como "aquellas entidades encargadas de evaluar las solicitudes presentadas por parte de un Usuario de Datos para el tratamiento de datos […], la concesión de la solicitud puede estar sujeta a distintas normativas y principios éticos"[9].

La figura del supervisor de solicitudes no es muy habitual en la mayoría de las modelos de roles presentes en el estudio realizado y, de la misma forma que el proveedor, no se encuentra formalmente

[9] Apartado IV.A.6 del documento "*Aproximación a los Espacios de Datos desde la perspectiva del RGPD*" (AEPD)[Mayo 2023

regulado por la normativa europea. Con una excepción, y es la mención indirecta y puntual establecida en un considerando del Reglamento de Gobernanza de datos, que establece que "*es preciso que los Estados miembros designen, establezcan o faciliten la creación de organismos competentes para respaldar las actividades de los organismos del sector público que se ocupen de autorizar la reutilización de determinadas categorías de datos protegidos*" [10]. Aunque este considerando esté enfocado exclusivamente al establecimiento de organismos del sector público por parte de los estados miembros, los mismos principios se aplicarían al establecimiento de un órgano controlador en una plataforma, que ejerciera ciertas funciones de control y gobernanza basadas en protocolos y principios éticos predefinidos, y determine la idoneidad de un conjunto de datos para ser incluidos en los catálogos del espacio. Esta visión es apoyada desde el punto de vista de la Agencia Española de Protección de Datos concretando que "*El Supervisor podría ser parte de la entidad de un Mediador del Espacio de Datos y ejercer ciertas funciones de Habilitador […]. Por ejemplo, pudiera darse ese caso con los Organismos Competentes definidos en la DGA cuando así lo exija la normativa sectorial de la Unión o nacional*"[11].

Por todo ello, entendemos que esta figura podrá definirse como aquella entidad con potestad y autonomía suficientes para ejercer ciertas funciones de control y concesión de solicitudes de acceso a los datos a usuarios dentro de la plataforma. A su vez no sería descabellado plantear una extensión de estas funciones, abarcando a su vez capacidad suficiente como para emitir informes consultivos sobre la idoneidad de determinados proveedores de datos, además de la revisión de determinados data sets para su alineamiento e inclusión en el catálogo.

2.1.3.1. Principales responsabilidades del supervisor de solicitudes

Principales responsabilidades	
	Supervisar la recepción y registro de las solicitudes.
	Evaluar la prioridad de las solicitudes.
	Acompañar el progreso de las solicitudes.
	Asegurar que las solicitudes cumplen con el marco contractual y organizacional del Espacio de Datos.
	Evaluar los posibles riesgos asociados a la inclusión del conjunto de datos en el catálogo del Espacio.
	Aprobar o rechazar las solicitudes.
	Garantizar que los usuarios tratan el conjunto de datos de acuerdo con la política de seguridad y de privacidad establecidas.
	Participar en auditorías internas y externas.

2.1.4. Mediador / Operador de la Plataforma

Entramos a clarificar una de las figuras protagonistas en todo modelo de roles dentro de una plataforma de datos. El rol de mediador u operador se define por la asociación internacional de espacios de datos como *"toda entidad que proporciona distintos tipos de infraestructura […]*

[10] Considerando 26 DGA

[11] Apartado IV.A.6 del documento "*Aproximación a los Espacios de Datos desde la perspectiva del RGPD*" (AEPD)[Mayo 2023]

siendo a su vez responsable de la gobernanza de la plataforma, proviniendo servicios de apoyo, definiendo los términos y condiciones […] sobre la admisión y retirada de conjuntos de datos o participantes. […] Los operadores del mercado de datos deben establecer mecanismos que garanticen el cumplimiento de las políticas de uso de datos"[12]. La Asociación profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información por su parte lo asocia a "*todos los participantes que se encarguen de la operación del espacio […] siendo los encargados de certificar tanto a los participantes, como sus conectores, y el resto de los componentes software del espacio. Para todos ellos, deben emitir acreditaciones para su identificación y autenticación. También ejercen la gobernanza del espacio de datos y definen el roadmap de funcionalidades"*[13]. Finalmente, la Agencia Española de Protección de Datos define al mediador como "*las entidades que establecen las relaciones en el Espacio de Datos entre los Sujetos de los Datos y/o Titulares de los Datos, por una parte, y los Usuarios de los Datos, por otra. Son aquellos que implementan los medios técnicos, jurídicos, organizativos, o de otro tipo que permiten la operación del espacio de datos entre múltiples titulares y múltiples usuarios de datos*"[14].

Sin embargo, a pesar de ser una figura central, esta figura no se encuentra directamente regulada en la legislación, ya que como acertadamente nos indica la Agencia Española de Protección de datos *"Dependiendo del contexto en el que opere el Mediador podrá tender una definición jurídica distinta como, por ejemplo, "servicio de intermediación de datos", "organismo competente", "organizaciones de gestión de datos con fines altruistas", "cooperativas de datos", etc."*[15]. Es por ello que en la legislación si encontramos definiciones de alguna de estas figuras en las que se encuadraría jurídicamente el operador, como es el caso del "*proveedor de servicios de intermediación de datos"* en el DGA comprendiendo "*todo servicio cuyo objeto sea establecer relaciones comerciales para el intercambio de datos entre un número indeterminado de interesados y titulares de datos, por una parte, y usuarios de datos, por otra, a través de medios técnicos, jurídicos o de otro tipo, incluidos los servicios destinados al ejercicio de los derechos de los interesados en relación con los datos personales*"[16].

A su vez, debemos entender que no todos los servicios regulados en la legislación en materias de gobernanza se ajustan a las relaciones existentes en un espacio de datos como el que se pretende

[12] Apartado 2.4.2 del documento "Design Principles for Data Spaces (IDSA)[Abril 2021]

[13] Página 2 del documento "*Elementos de un espacio de Datos"* (Francisco Javier Esteve Pradera)[Junio 2022]

[14] Apartado IV.A.4 del documento "Aproximación a los Espacios de Datos desde la perspectiva del RGPD" (AEPD)[Mayo 2023]

[15] Apartado IV.A.4 del documento "Aproximación a los Espacios de Datos desde la perspectiva del RGPD" (AEPD)[Mayo 2023]

[16] Artículo 2.11 del DGA

con el proyecto INESDATA, este es el ejemplo de la provisión de servicio de tratamiento de datos regulado en el Reglamento de datos y definido como todo "*servicio digital que se presta a un cliente y que permite un acceso de red ubicuo y bajo demanda a un conjunto compartido de recursos informáticos configurables, modulables y elásticos de carácter centralizado, distribuido o muy distribuido, que puede movilizarse y liberarse rápidamente con un mínimo esfuerzo de gestión o interacción con el proveedor de servicios*" [17]. En el contexto de un servicio de intermediación de datos como el que se pretende con INESDATA, los miembros de un espacio de datos compartidos no se consideran clientes del servicio de intermediación de datos en el sentido tradicional de la relación comercial entre un proveedor y un cliente. En este caso, el operador actúa como intermediario para facilitar las relaciones entre los miembros del espacio de datos compartidos, pero no necesariamente se establece una relación de cliente-proveedor en términos comerciales. Por su parte, el operador tendrá la función de facilitar la compartición de datos entre los miembros del espacio, asegurando el cumplimiento de las políticas, y las condiciones de seguridad y privacidad establecidas. Por lo tanto, podemos concluir que los miembros del espacio de datos y la entidad coordinadora tienen roles específicos dentro de este entorno, pero no se consideran clientes en el sentido convencional.

Finalmente, consideramos que la definición más ajustada para la naturaleza del proyecto de INESDATA sería la de aquella entidad responsable de implementar y gestionar los medios técnicos, jurídicos, organizativos, o de otro tipo, que permiten la operación del Espacio de Datos. Y la figura jurídica que ostentará la entidad que ocupe este rol será necesariamente la de proveedor de un servicio de intermediación de datos, teniendo que cumplir las condiciones para la prestación de servicios de intermediación de datos recogidas en el Reglamento de Gobernanza de Datos una vez dicha plataforma esté operativa.

2.1.4.1. Principales responsabilidades extraídas de la normativa:

Los principales deberes indicados expresamente dentro del bloque normativo de gobernanza que, bajo el proyecto INESDATA, pueden asociarse a la figura del operador de datos son:

Obligaciones legales	
Reglamento (UE) 2022/868 de gobernanza de datos	Prevenir la divulgación de cualquier información que ponga en peligro los derechos e intereses de terceros, que el reutilizador pueda haber adquirido a pesar de las garantías establecidas.
	Prohibir la reidentificación de cualquier interesado al que se refieran los datos, adoptando las medidas técnicas y operativas destinadas a evitar dicha reidentificación y notificar al proveedor de datos cualquier violación de la seguridad de los datos que dé lugar a una posible reidentificación de los interesados.

[17] Artículo 2.8 del DA

	En caso de reutilización no autorizada de datos no personales, el operador informará sin demora y, en su caso, con la ayuda del proveedor, a las personas jurídicas cuyos derechos e intereses puedan verse afectados.
	Permitir únicamente la reutilización de datos con la condición de respetar los derechos de propiedad intelectual existentes sobre los datos, en favor del proveedor.
	En caso de trasferir a un tercer país datos no personales protegidos por motivos de confidencialidad o por derechos de propiedad intelectual de terceros, el operador informará al proveedor de datos de su intención de transferirlos y de la finalidad de la transferencia en el momento de solicitar y acordar la reutilización de dichos datos.
	En aquellos terceros países no cubiertos por actos de ejecución de la comisión europea, a los que el operador pretenda trasferir datos no personales confidenciales o protegidos por derechos de propiedad intelectual, el operador deberá obligarse contractualmente a cumplir y respetar los derechos de propiedad intelectual, las medidas de prevención a la divulgación de datos, y aceptar la competencia de los organismos jurisdiccionales del Estado miembro del proveedor; absteniéndose de realizar cualquier trasferencia de datos en caso contrario.
	Aplicar las tasas de reutilización establecidas en las condiciones de uso de los datos acotadas por los proveedores.
	En caso de solicitar a un proveedor de datos la reutilización de un conjunto especifico de datos, y haber recibido una negativa del organismo competente de su decisión, se reconoce el derecho efectivo de recurso ante un órgano imparcial.
	Antes de entrar en funcionamiento la plataforma el operador deberá presentar una notificación a la autoridad competente en materia de servicios de intermediación de datos. Tras haber remitido una notificación de conformidad por parte del organismo competente, el proveedor de servicios de intermediación de datos podrá iniciar su actividad con arreglo a las condiciones establecidas en la normativa.
	El operador deberá designar un representante legal en cada uno de los Estados miembros en los que ponga a disposición sus servicios de intermediación de datos.
	Una vez recibida la notificación de conformidad, el operador podrá usar, en sus comunicaciones orales y escritas, la denominación «proveedor de servicios de intermediación de datos reconocido en la Unión», así como un logotipo común.
	En caso de cesar en sus actividades el operador deberá informar diligentemente a la autoridad competente en materia de servicios de intermediación de datos.
	El operador deberá designar un representante legal en cada uno de los Estados miembros en los que ponga a disposición sus servicios de intermediación de datos.
	Durante la prestación de servicios de intermediación provista por el operador de datos, no podrán utilizarse los datos provistos por los proveedores para fines distintos a los especificados durante su puesta a disposición.

	El operador de datos deberá ofrecer los servicios de intermediación a través de una persona jurídica distinta.
	Las condiciones contractuales comerciales propuestas por el operador, incluidas las relativas a los precios, para la prestación de servicios de intermediación de datos a un proveedor, un titular o a un usuario de datos no podrán depender de que el proveedor, un titular o el usuario de datos utilice otros servicios prestados por el operador o por una entidad relacionada con él. A si mismo, de utilizarlos no podrán depender de en qué grado el titular de datos o el usuario de datos utilice dichos servicios.
	Los datos recogidos sobre cualquier actividad de una persona física o jurídica, a efectos de la prestación de un servicio de intermediación de datos por el operador de la plataforma, solo se utilizarán para el desarrollo de ese servicio, lo que puede implicar la utilización de datos para la detección de fraudes o para fines de ciberseguridad. (Fecha, hora de conexión, duración de la actividad, conexiones que el usuario del servicio de intermediación de datos establezca con otras personas físicas o jurídicas…).
	El operador podrá incluir la oferta de herramientas y servicios específicos adicionales a los proveedores, titulares o a los interesados con el objetivo específico de facilitar el intercambio de los datos.
	El operador velará por que el procedimiento de acceso a sus servicios, incluidos los precios y las condiciones de servicio, sea equitativo, transparente y no discriminatorio, tanto para los interesados como para los titulares de datos y los usuarios de datos.
	El operador dispondrá de procedimientos para impedir prácticas fraudulentas o abusivas de las partes que deseen obtener acceso a través de sus servicios de intermediación de datos.
	El operador se asegurará en caso de insolvencia, de la continuidad razonable de la prestación de sus servicios de intermediación de datos. Y, cuando esos servicios de intermediación de datos incluyan el almacenamiento de datos, dispondrán de los mecanismos de garantía necesarios para que los titulares de datos y los usuarios de datos puedan acceder a sus datos, transferirlos o recuperarlos.
	El operador adoptará las medidas adecuadas para garantizar la interoperabilidad con otros servicios de intermediación de datos, entre otros, mediante normas abiertas de uso común en el sector.
	El operador informará sin demora a los titulares de datos en caso de transferencia, acceso o utilización no autorizados de los datos no personales que haya compartido.
	El operador actuará en el mejor interés de los titulares y proveedores, informándolos y, cuando corresponda, asesorándolos de manera concisa, transparente, e inteligible sobre los usos previstos de los datos por los usuarios de datos y las condiciones generales aplicables a dichos usos.
	El operador conservará un registro de la actividad de intermediación de datos.
Reglamento (UE) 2023/2854 de Datos	Establecer acuerdos y condiciones sobre el acceso a los datos, y su utilización, libres de cláusulas abusivas, alineándose con estándares de buenas prácticas comerciales según la normativa aplicable.
	Cuando el operador reciba una solicitud de puesta a disposición de datos de un organismo del sector público, la Comisión, el Banco Central Europeo

	o un organismo de la Unión que demuestre una necesidad excepcional, el operador informará a dicho organismo del sector público solicitante de la titularidad de los datos sin demora indebida, para que remita dicha solicitud al titular o proveedor original.
	El operador adoptará las medidas técnicas y organizativas previstas en la norma para permitir a los clientes cambiar a un servicio de tratamiento de datos que cubra el mismo tipo de servicio, que sea prestado por un proveedor diferente de servicios de tratamiento de datos o a una infraestructura de TIC local. Estas medidas alcanzarán únicamente solo a los servicios, contratos o prácticas comerciales prestados por el proveedor de servicios de tratamiento de datos de origen.
	Los derechos de los proveedores y usuarios de la plataforma, y las obligaciones del operador en relación con el cambio de proveedor de los servicios de intermediación o, en su caso, el cambio a una infraestructura de TIC local se establecerá con claridad en un acuerdo escrito. El proveedor de servicios de tratamiento de datos pondrá dicho acuerdo a disposición del cliente antes de su firma, de un modo que permita al cliente conservar y reproducir el contrato.
	Cuando el período transitorio de cambio obligatorio máximo establecido en los acuerdos, sea técnicamente inviable, el operador notificará la inviabilidad técnica al cliente dentro de un plazo de catorce días hábiles desde que se haya presentado la solicitud de cambio, y justificará debidamente dicha inviabilidad e indicará un período transitorio alternativo, que no excederá de siete meses.
	El operador proporcionará a los usuarios de la plataforma información sobre los procedimientos disponibles para el cambio, incluida la información sobre los métodos y formatos de cambio y de transferencia disponibles, así como las restricciones y limitaciones técnicas conocidas por el proveedor de servicios de tratamiento de datos. A su vez el operador podrá a disposición de los usuarios una referencia a un registro en línea actualizado alojado por el operador, con detalles de todas las estructuras y formatos de datos, así como de las normas pertinentes y las especificaciones de interoperabilidad abiertas.
	El operador pondrá en sus sitios web, y a disposición de los usuarios, la jurisdicción a la que está sujeta la infraestructura de TIC desplegada, así como una descripción general de las medidas técnicas, organizativas y contractuales adoptadas por el operador para impedir el acceso o transferencia internacionales por parte de las administraciones públicas de datos no personales que se encuentren en la Unión, cuando dicho acceso o transferencia pueda entrar en conflicto con el Derecho de la Unión o con el Derecho nacional.
	A partir del 12 de enero de 2027, el operador no impondrá a los usuarios ningún coste por el proceso de cambio de proveedor de servicio. Sin embargo, Del 11 de enero de 2024 hasta el 12 de enero de 2027, el operador podrá imponer al cliente costes por cambio reducidos por el proceso de cambio de proveedor de servicio.
	El operador deberá poner a disposición de los usuarios información clara sobre los costes estándar del servicio y las sanciones por resolución anticipada que podrían imponerse, o los servicios impliquen un cambio muy complejo o costoso, para los que sea imposible cambiar de proveedor sin interferencias significativas en los datos, los activos digitales o la arquitectura del servicio.

Reglamento (UE) 2018/1807 para la libre circulación de datos no personales en la Unión Europea	El operador de la plataforma no podrá denegar a las autoridades competentes acceso a los datos alegando concretamente que están siendo objeto de tratamiento en otro estado miembro. Si no que le remitirá a dicha autoridad el contacto del titular o proveedor de los datos para dar salida a la solicitud de acceso a los datos para el desempeño de sus funciones oficiales.
Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.	El operador no podrá atribuir contractualmente a los titulares o proveedores de datos la responsabilidad derivada del uso que de su información hagan los usuarios de la plataforma, ni tampoco de los daños sufridos o pérdidas económicas que, de forma directa o indirecta, produzcan o puedan producir perjuicios económicos, materiales o sobre datos, provocados por el uso de la información reutilizada.
	Los datos proporcionados por proveedores de datos pertenecientes a la administración pública, en la medida de lo posible, se pondrán a disposición de los usuarios conforme al principio de documentos abiertos desde el diseño y por defecto.
	El operador de la plataforma no podrá exigirse a los proveedores de datos pertenecientes a la administración pública que mantengan la producción y el almacenamiento de un determinado tipo de dato con vistas a su reutilización.
	La reutilización de la información proporcionada por proveedores de datos pertenecientes a la administración pública podrá estar sometida, entre otras, a ciertas condiciones generales: como la prohibición de alteración del contenido de la información, que no se desnaturalice el sentido de la información, que se citen las fuentes utilizadas, o que se mencione la última fecha de actualización entre otras.
	En caso de que el operador quiera solicitar la reutilización de información administrativa en poder de proveedores de datos pertenecientes a la administración pública deberá emitir una solicitud de reutilización al órgano competente, entendiendo por tal aquel en cuyo poder obren los documentos cuya reutilización se solicita. El órgano competente resolverá las solicitudes de reutilización en el plazo máximo de veinte días desde la recepción de la solicitud.
	El operador se verá sometido al régimen sancionador recogido en la legislación en caso de incumplimiento de alguno de sus preceptos.

2.1.5. Proveedor Tecnológico

En este caso, el rol del proveedor tecnológico se erige de una manera aparentemente simple, encontrándose ausente de toda normativa legal y documento técnico a excepción del articulo elaborado por La Asociación profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información, que lo delimita como " aquel rol que ejercen aquellos participantes que proporcionan componentes para el

funcionamiento del espacio de datos que no son servicios de intermediación, ni aplicaciones, sino que permiten que se ofrezca un ecosistema de intercambio de datos con seguridad y confianza"[18].

A estos efectos, es poco descabellado deducir que esta figura la asumirá toda entidad, o entidades, que proporcionen la infraestructura física necesaria para albergar los componentes que permitan el funcionamiento de la plataforma. En el caso de INESDATA este rol está siendo actualmente asumido en su totalidad por la Universidad Politécnica de Madrid.

2.1.5.1. Principales responsabilidades extraídas de la normativa:

Los principales deberes indicados expresamente dentro del bloque normativo de gobernanza que, bajo el proyecto INESDATA, pueden asociarse a la figura del proveedor tecnológico es:

Obligaciones legales	
Reglamento (UE) 2023/2854 Data Act	Debe adoptar todas las medidas razonables a su alcance para facilitar que el usuario, tras cambiar a un servicio que cubra el mismo tipo de servicio, logre la equivalencia funcional en el uso del servicio de tratamiento de datos de destino.
	El proveedor tecnológico de origen facilitará el proceso de cambio proporcionando capacidades, información adecuada, documentación, apoyo técnico y, cuando proceda, las herramientas necesarias.
	Debe poner gratuitamente interfaces abiertas a disposición de todos los usuarios y de los proveedores tecnológicos de destino afectados, de igual manera, para facilitar el proceso de cambio. Estas interfaces incluirán información suficiente sobre el servicio de que se trate para permitir el desarrollo de programas informáticos para comunicarse con los servicios, a efectos de la portabilidad de los datos y la interoperabilidad.
	En el caso de servicios de tratamiento de datos distintos, el proveedor tecnológico garantizará la compatibilidad con las especificaciones comunes basadas en especificaciones de interoperabilidad abiertas o normas armonizadas de interoperabilidad al menos doce meses después de la publicación de las referencias a dichas especificaciones comunes de interoperabilidad o normas armonizadas de interoperabilidad de los servicios de tratamiento de datos en el repositorio central de la Unión de normas para la interoperabilidad de los servicios de tratamiento de datos tras la publicación de los actos de ejecución correspondientes en el Diario Oficial de la Unión Europea.
	Deben actualizar el registro en línea de conformidad con sus obligaciones.
	En caso de cambio entre servicios del mismo tipo de servicio, para los que no se hayan publicado las especificaciones comunes o las normas armonizadas de interoperabilidad en el repositorio central de la Unión de normas para la interoperabilidad de los servicios de tratamiento de datos, el proveedor tecnológico deberá exportar, a petición del usuario, todos los datos exportables en un formato estructurado, de utilización habitual y de lectura mecánica.
	El proveedor tecnológico no estará obligado a desarrollar nuevas tecnologías o servicios, ni a revelar o transferir activos digitales protegidos por derechos de propiedad intelectual o que constituyan un secreto

[18] Página 2 del documento "*Elementos de un espacio de Datos"* (Francisco Javier Esteve Pradera)[Junio 2022]

	comercial, a un usuario o a un proveedor diferente de servicios de tratamiento de datos, ni a comprometer la seguridad y la integridad del servicio del usuario o del proveedor.
	Para facilitar la interoperabilidad, el proveedor tecnológico debe desarrollar las estructuras de datos, los formatos de datos, los vocabularios, los sistemas de clasificación, las taxonomías y las listas de códigos, cuanto estén disponibles, se describirán de manera que sean de acceso público y coherentes.
	Debe desarrollar los medios técnicos para acceder a los datos, tales como las interfaces de programación de aplicaciones, así como sus condiciones de uso y su calidad de servicio, se describirán en una medida suficiente para permitir el acceso automático a los datos y su transmisión automática entre las partes, incluido de forma continua, en descarga masiva o en tiempo real, en un formato de lectura mecánica cuando sea técnicamente viable y no impida el buen funcionamiento del producto conectado.

2.1.6. Consumidor Final / Usuario de Datos

Otro de los elementos esenciales para el funcionamiento completo del modelo, esta vez en la vertiente de salida del flujo de datos, es el papel ostentado por el consumidor final de los datos. Para la definición de esta figura debemos acudir a las definiciones establecidas por el Reglamento de Gobernanza de Datos, el cual entiende como usuario de datos a "toda persona física o jurídica que tenga acceso legítimo a determinados datos personales o no personales y el derecho, incluido el que le otorga el Reglamento (UE) 2016/679en el caso de los datos personales, a usarlos con fines comerciales o no comerciales"[19], de manera similar se define esta figura particularizada al ámbito sanitario en la propuesta de Reglamento sobre el Espacio Europeo de Datos Sanitarios "una persona física o jurídica que tiene acceso legítimo a determinados datos sanitarios electrónicos personales o no personales y está autorizada a usarlos con fines comerciales o no comerciales"[20]. Encontramos también una definición aplicable, pero algo más delimitada, en el Reglamento de Datos bajo la denominación de "*destinatario de datos*" entendiéndose como tal a "*una persona física o jurídica que actúa con un propósito relacionado con su actividad comercial, empresa, oficio o profesión, distinta del usuario de un producto conectado o servicio relacionado, a disposición de la cual el titular de datos pone los datos, incluso un tercero previa solicitud del usuario al titular de datos o de conformidad con una obligación legal*"[21]; la cual no debe confundirse con la definición de este mismo termino por la propuesta de Reglamento sobre el Espacio Europeo de Datos Sanitarios, que lo presenta en sus definiciones como "*una persona física o jurídica que recibe datos de otro responsable del tratamiento en el contexto del uso primario de datos sanitarios electrónicos*"[22].

En síntesis, y atendiendo a las particularidades del proyecto INESDATA, se entiende como usuario de datos al consumidor final de la plataforma, siendo este una persona física o jurídica que teniendo acceso legítimo a determinados datos puede utilizarlos con fines comerciales derivados de su actividad o no.

[19] Artículo 2.9 del DGA

[20] Artículo 2.2.z) del EDSR

[21] Artículo 2.14 del DA

[22] Artículo 2.2.k) del EDSR

2.1.6.1. Principales responsabilidades extraídas de la normativa:

Los principales deberes indicados expresamente dentro del bloque normativo de gobernanza que, bajo el proyecto INESDATA, pueden asociarse a la figura del usuario de datos es:

Obligaciones legales	
Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.	La utilización de los conjuntos de datos se realizará por parte de los usuarios de datos bajo su responsabilidad y riesgo, correspondiéndoles en exclusiva a ellos responder frente a terceros por daños que pudieran derivarse de ella.
	El usuario de datos no podrá atribuir contractualmente a los proveedores de datos pertenecientes a la administración pública la responsabilidad derivada del uso que de su información hagan los usuarios de la plataforma, ni tampoco de los daños sufridos o pérdidas económicas que, de forma directa o indirecta, produzcan o puedan producir perjuicios económicos, materiales o sobre datos, provocados por el uso de la información reutilizada.
	Los usuarios de datos no podrán indicar de ningún modo, que los proveedores de datos pertenecientes a la administración pública titulares de la información reutilizada participan, patrocinan o apoyan la reutilización que se lleve a cabo de ella.

2.1.7. Entidades Supervisoras

El rol de entidad supervisora de la plataforma, aunque pueda parecer evidente merece cierta concreción conceptual para poder delimitar que se entiende por dichas entidades en el contexto del proyecto. Con este fin, y a pesar de focalizarse en materia de protección de datos, la Agencia Española de Protección de Datos determina que "en materia de protección de datos, las autoridades competentes serán las indicadas en el RGPD, que en el caso de España será la AEPD, o las Autoridades Autonómicas de acuerdo con su competencia. Cuando otras autoridades actúen como autoridades competentes, por ejemplo, con arreglo a la DGA, lo deben hacer sin perjuicio de las facultades y competencias de supervisión de otras autoridades responsables"[23]. Por su parte, el Reglamento de Gobernanza de Datos establece que "*cada Estado miembro designará a una o varias autoridades competentes para desempeñar las funciones relacionadas con el procedimiento de notificación en materia de servicios de intermediación de datos*"[24] definiendo sus funciones y concretando que "*las autoridades competentes en materia de servicios de intermediación de datos controlarán y supervisarán el cumplimiento de los requisitos del presente capítulo por los proveedores de servicios de intermediación de datos*"[25].

De esta manera, podemos apreciar claramente como la existencia de una sola entidad que ostente el rol de entidad supervisora de la plataforma es un escenario altamente improbable, y que habrá que identificar y tener en cuenta todas las autoridades que supervisen las materias de cumplimiento a las que se vea sometida la plataforma.

[23] Apartado IV.A.7 del documento "Aproximación a los Espacios de Datos desde la perspectiva del RGPD" (AEPD)[Mayo 2023]

[24] Artículo 13.1 del DGA

[25] Artículo 14.1 del DGA

2.1.7.1. Principales responsabilidades extraídas de la normativa:

Los principales deberes indicados expresamente dentro del bloque normativo de gobernanza que, bajo el proyecto INESDATA, pueden asociarse a la figura de la entidad supervisora es:

Obligaciones legales	
Reglamento (UE) 2022/868 (Data Governance Act)	Las entidades supervisoras tendrán en cuenta el régimen de sanciones establecido por los Estados miembros, que será aplicable a cualquier infracción de las obligaciones relativas a las transferencias de datos no personales a terceros países. Tales sanciones serán efectivas, proporcionadas y disuasorias.
	Para la imposición de sanciones se deberá tener en cuenta la naturaleza, gravedad, magnitud y duración de la infracción; cualquier medida adoptada por el proveedor de servicios de intermediación de datos o la organización reconocida de gestión de datos con fines altruistas para mitigar o reparar el daño causado por la infracción; cualquier infracción anterior del proveedor de servicios de intermediación de datos o de la organización reconocida de gestión de datos con fines altruistas; los beneficios financieros obtenidos o las pérdidas evitadas por el proveedor de servicios de intermediación de datos o la organización reconocida de gestión de datos con fines altruistas debido a la infracción, en la medida en que dichos beneficios o pérdidas puedan determinarse de forma fiable;
	Recibir por parte de los organismos públicos las impugnaciones negativas o de solicitud de los titulares de datos.

2.2. Roles Complementarios para el funcionamiento de la plataforma

Una vez identificados los roles esenciales, podemos proceder a definir entidades más particulares que, si bien son de frecuente inclusión en los modelos prácticos más difundidos, no podríamos considerarlos desde el inicio y por defecto como esenciales en la concepción de todo espacio de datos:

2.2.1. Sujeto de los Datos

La existencia de este rol dentro de esta categoría se debe a que su presencia devendrá supeditada a la inclusión, o no, de datos personales dentro de la plataforma, con su consecuente tratamiento. A estos efectos la Agencia Española de Protección de Datos determina que "*en marcos generales de espacios de datos, el Interesado o Sujeto de los Datos, es decir, la persona física identificada o identificable cuyos datos personales son los que se plantea tratar, podría asociarse a la definición de "productor de los datos" utilizada en algunos esquemas de Espacios de Datos. Cuando se asocia la figura de "productor de los datos" a sistemas o servicios que recogen o generan datos personales de personas físicas*"[26].

Atendiendo a esta particularidad en el seno del proyecto de INESDATA, y específicamente para en aquellos demostradores que conlleven un tratamiento de datos personales, podremos entender a un sujeto de datos como cualquier persona física, identificada o identificable, que genera datos voluntaria o involuntariamente.

[26] Apartado IV.A.1 del documento "Aproximación a los Espacios de Datos desde la perspectiva del RGPD" (AEPD)[Mayo 2023]

2.2.2. Productor de los Datos

La presencia del productor de datos en un ecosistema, al igual que ocurría con los sujetos de datos, se supedita a la existencia de una casuística o condición particular, esta vez en el proceso de creación de los datos. Y es que, de manera similar a como un sujeto de datos requiere que se lleve a cabo un tratamiento de datos personales dentro de una plataforma para materializarse, lo mismo ocurre con un productor de datos, cuya condición es que no se configure como propietario de los datos en el proceso de su creación como bien indica la Asociación profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información en su artículo monográfico, entendiendo como productor toda persona física o jurídica que "*genere datos sin ser necesariamente los dueños de los mismos, ni los proveedores"*[27]. De esta definición extraemos, en su vertiente negativa, la confirmación de que los datos potencialmente generados por un productor de datos que se constituya en una persona física tendrán que ser necesariamente datos no personales, puesto que de generarse datos personales por parte de los sujetos interesados su protección, y por extensión su propiedad, se encuentran reconocidas constitucionalmente como un derecho fundamental y, por lo tanto, estas facultades serían indisponibles. Por otra parte, podemos inferir de la definición aportada que, al no ser los productores de los datos propietarios de los mismos, esta facultad recaería necesariamente en los titulares de los datos en cuyo ámbito de control se hubieran generado, creándose así una separación conceptual entre las dos figuras.

En lo que pudiera afectar al proyecto INESDATA, entendemos de todo ello que este rol de productor de los datos únicamente podría desplegarse en caso de que los datos incorporados a la plataforma no tuvieran la tipología de datos personales, entendiéndose estos como "*toda información sobre una persona física identificada o identificable*"[28], y encontrándose los mismos a disposición de proveedores que pudieran legítimamente disponer de los mismos teniendo simultáneamente la titularidad de los datos, o actuando por cuenta de los titulares bajo cuyo ámbito de control se hubieran generado estos datos, y que son en última instancia sus propietarios.

2.2.3. Habilitador

El rol de habilitador hace las veces de cajón de sastre, en lo que a roles de apoyo dentro de la plataforma se refiere. Se encuentran particularmente presentes dentro de modelos funcionales y trabajos de disertación, mas que delimitados por una normativa concreta. Podemos hallar una definición aproximada de sus características a través de la guía de la Agencia Española de Protección de Datos, "*los Habilitadores en el entorno de un Espacio de Datos serían aquellos que darán apoyo a todos los intervinientes anteriormente descritos para poder garantizar que la implementación se realiza un proceso eficiente, coherente, implementando los mecanismos de gobernanza y gestión entre múltiples intervinientes, evitando duplicidades y repeticiones de tareas, facilitando los trámites y solicitudes*"[29]. Por otro lado, y bajo la denominación de intermediarios, dentro del articulo monográfico de la Asociación profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información se les define como entidades que ofrecen "*servicios que no añaden directamente valor a los datos pero que se requieren para la publicación y búsqueda de recursos para el registro de transacciones*"[30].

---

[27] Página 2 del documento "*Elementos de un espacio de Datos"* (Francisco Javier Esteve Pradera)[Junio 2022]

[28] Articulo 4.1 del RGPD

[29] Apartado IV.A.5 del documento "Aproximación a los Espacios de Datos desde la perspectiva del RGPD" (AEPD)[Mayo 2023]

[30] Página 2 del documento "*Elementos de un espacio de Datos"* (Francisco Javier Esteve Pradera)[Junio 2022]

Bajo nuestra perspectiva, y centrándonos en los límites del proyecto INESDATA, concebimos al habilitador como toda entidad que de apoyo y provea de componentes para el acceso, la intermediación, o la gestión del espacio de datos; así como otras funciones puntuales que no añaden directamente valor a los datos (Proveedor de vocabularios, Proveedor de Identidades (FNMT)…), siendo esta última cualidad objeto de análisis en el siguiente apartado.

2.2.4. Proveedores de Servicios y Aplicaciones

Los roles de proveedores, tanto el de servicios como el de aplicaciones, se tratan de roles ciertamente similares cuya distinción no es otra que el objeto de la provisión que ofrecen. La figura de proveedor, en su dimensión especifica de gobernanza en plataformas como INESDATA, se encuentra ausente de regulación particular, puesto que el único servicio de provisión formalmente regulado es la provisión de servicios de intermediación de datos. A pesar de ello, existen menciones indirectas en esta materia en normativas como el Reglamento de Gobernanza de Datos que arroja algo de luz a esta distinción indicando que "*los servicios de almacenamiento en la nube, de análisis, el software de intercambio de datos, los navegadores, los complementos para navegadores o los servicios de correo electrónico no deben considerarse servicios de intermediación de datos en el sentido de lo dispuesto en el presente Reglamento, siempre que dichos servicios solo suministren herramientas técnicas para que los interesados o los titulares de datos intercambien datos con terceros, pero el suministro de dichas herramientas no se use con el objeto de establecer una relación comercial entre titulares de datos y usuarios de datos, […] Esto excluiría los servicios que obtienen datos de titulares de datos y que los agregan, enriquecen o transforman con el fin de añadirles un valor sustancial*"[31]. Por ello entendemos que la provisión de servicios de intermediación difiere, en esencia, de la provisión de servicios y aplicaciones a un ecosistema de intercambio de datos, llegando a prohibirse específicamente desde la normativa que ambos roles recaigan sobre la misma persona jurídica como el Reglamento de Gobernanza de datos que "exige una separación estructural entre el servicio de intermediación de datos y cualquier otro servicio prestado, a fin de evitar conflictos de intereses. Esto supone que los servicios de intermediación de datos deben prestarse a través de una entidad jurídica que sea independiente de las demás actividades del proveedor de dichos servicios"[32].

También debemos poner especial atención en su distinción con otros roles involucrados en la provisión de servicios dentro de la plataforma, como es el caso de los habilitadores. Esta distinción es reforzada gracias a ciertas definiciones como la propuesta por la Asociación profesional de Cuerpos Superiores de Sistemas y Tecnologías de la Información, que define al proveedor de aplicaciones como aquel que "*provee aplicaciones que añaden valor a los datos, como pueden ser modelos de machine learning, procesos de limpieza, visualización, transformación, aplicaciones*

[31] Considerando 28 del DGA

[32] Considerando 33 del DGA

de anonimización, etc..”[33]. Poniendo el foco en la creación de valor sobre los datos nos permite ver con claridad la distinción formal que existe entre estos dos roles, diferenciando rápidamente un tipo de proveedor u otro atendiendo a su impacto sobre el valor de los datos o la ausencia del mismo.

2.2.4.1. Principales responsabilidades del proveedor de servicios y aplicaciones

Principales responsabilidades contractuales	
Contrato firmado entre el Operador y el Proveedor	Asegurar que los datos son precisos, completos y actualizados.
	Implementar procesos de limpieza y validación de datos.
	Integrar datos de múltiples fuentes para crear conjuntos de datos más completos y de valor añadido.
	Añadir metadatos, etiquetas y estructurar los datos de manera que sean más accesibles y útiles para los usuarios.
	Desarrollar aplicaciones que proporcionen análisis avanzados para facilitar la interpretación de los datos.
	Asesorar al usuario al identificar áreas de mejora y de oportunidad para añadir valor adicional a los conjuntos de datos.

[33] Página 2 del documento “*Elementos de un espacio de Datos”* (Francisco Javier Esteve Pradera)[Junio 2022]

3. Análisis de Aplicabilidad Normativa

Una vez se ha procedido a la definición de los roles que conformarán el espacio de datos pretendido a través del proyecto INESDATA, es preceptivo realizar un análisis de aplicabilidad que cubra las principales normativas en las materias de mayor incidencia inicial y que merecerán una mayor atención desde las primeras fases del desarrollo del marco normativo. Estas normativas se han clasificado en cuatro grupos: Gobernanza, Seguridad, Privacidad y Legislación Sectorial.

3.1. Gobernanza

Debido a los recientes esfuerzos legislativos europeos fruto del avance la Estrategia Europea de Datos planteada en 2020, se han publicado diversos cuerpos normativos de alcance europeo que tendrán potenciales implicaciones en el diseño del marco de gobernanza dentro del proyecto INESDATA. A continuación, realizaremos un breve estudio preliminar en base al objeto de cada norma, su ámbito de aplicabilidad, y la forma en que el proyecto INESADATA se encuentra o no bajo el mismo.

3.1.1. Reglamento (UE) 2022/868 (Reglamento de Gobernanza de Datos)

Los objetivos del presente reglamento abarcan la reutilización, dentro de la Unión, de determinadas categorías de datos que obren en poder de organismos del sector público, así como el establecimiento de un marco de notificación y supervisión para la prestación de los servicios de intermediación de datos, para finalmente regular un marco para la inscripción voluntaria en un registro de las entidades que cedan datos con fines altruistas.

En este sentido, y analizando concretamente la implicación del reglamento sobre el proyecto INESDATA, solo existirían ramificaciones en los casos en que el operador sea considerado como proveedor de un servicio de intermediación de datos de dentro de la plataforma, así como en aquellas aportaciones de datos motivadas por una reutilización de determinadas categorías de datos protegidos, cuyos titulares fueran organismos del sector público.

En este contexto, hemos de indicar nuevamente las particularidades que el reglamento atribuye al concepto de servicio de intermediación de datos entendiendo como tal "*todo servicio cuyo objeto sea establecer relaciones comerciales para el intercambio de datos entre un número indeterminado de interesados y titulares de datos, por una parte, y usuarios de datos, por otra, a través de medios técnicos, jurídicos o de otro tipo, incluidos los servicios destinados al ejercicio de los derechos de los interesados en relación con los datos personales*"[34]. A esta definición se le añaden dos excepciones:

- Los servicios que conlleven un enriquecimiento de datos obtenidos de titulares y concedan licencias a usuarios sin establecer una relación comercial.

[34] Artículo 2.11 del DGA

- Los servicios de intermediación cuyo objeto sean datos de contenido protegido por derechos de autor.
- Los servicios utilizados exclusivamente por un único titular, un grupo cerrado de titulares, de los datos que obren en su poder, y en particular los obtenidos mediante funcionalidades de objetos y dispositivos conectados al internet de las cosas.
- Los servicios ofrecidos por organismos del sector público sin la intención establecer relaciones comerciales.

De considerarse el operador como un proveedor de servicios de intermediación de datos, un elemento de peso en la definición de este tipo de provisión de servicio es la existencia de una pretensión dirigida a establecer relaciones comerciales como base necesaria para entender aplicable este reglamento a la plataforma. Podemos entender las relaciones comerciales por ser aquellas en las que se realizan transacciones entre empresarios o profesionales en el ámbito de sus actividades comerciales o empresariales. Por lo que sería asumible que en el punto en el que se encuentra actualmente el proyecto INESDATA, entendamos que el operador de los datos, como coordinador principal de todo el espacio, actuará en condición de proveedor de servicio de intermediación de datos, en tanto se prevé que formalice relaciones comerciales tanto con proveedores de datos como con usuarios finales. Por lo que entraría dentro del ámbito de aplicación de este reglamento, y en especial se vería afectado por su régimen sancionador.

3.1.2. Reglamento (UE) 2023/2854 (Reglamento de Datos)

El reglamento de datos se publica con objeto de armonizar ciertas materias en cuanto a la asignación del valor de los datos entre los agentes de la economía de los datos, fomentando el acceso equitativo a los mismos y su utilización para contribuir al establecimiento de un verdadero mercado interior de datos. En concreto, de todos los ámbitos que componen el objeto de la norma, en lo que compete al proyecto INESDATA destacan las normas armonizadas[35] en materia de:

- Puesta a disposición de datos por parte de los titulares de datos en favor de los destinatarios de datos;
- La puesta a disposición de datos por parte de los titulares de datos en favor de los organismos del sector público, la Comisión, el Banco Central Europeo y los organismos de la Unión, cuando exista una necesidad excepcional de disponer de dichos datos para el desempeño de alguna tarea específica realizada en interés público;
- La introducción de salvaguardias contra el acceso ilícito de terceros a los datos no personales;
- El desarrollo de normas de interoperabilidad para el acceso, la transferencia y la utilización de datos.

Simultáneamente, entre las entidades que componen su ámbito de aplicación[36] podemos encontrar roles de cierta familiaridad para el proyecto como son:

[35] Artículo 1.1 del DA

[36] Artículo 1.3 del DA

- Titulares de datos, con independencia de su lugar de establecimiento, que pongan datos a disposición de los destinatarios de datos de la Unión.
- Destinatarios de datos de la Unión a cuya disposición se ponen datos
- Participantes en espacios de datos y proveedores de aplicaciones que utilicen contratos inteligentes y personas cuya actividad comercial, empresarial o profesional implique el despliegue de contratos inteligentes para terceros en el contexto de la ejecución de un acuerdo.

Por todo ello, al tratarse INESDATA de un proyecto de desarrollo de instalación y mantenimiento de un cloud privado para espacios de datos donde será previsible la participación de estos roles, podemos determinar que será de aplicación este reglamento, y deberán ser respetadas en sus distintas vertientes las normas armonizadas desplegadas sobre las materias anteriormente mencionadas dentro del proyecto INESDATA.

3.1.3. Reglamento (UE) 2018/1807 (Reglamento de datos no Personales)

Este breve reglamento tiene por objeto "*garantizar la libre circulación en la Unión de datos que no tengan carácter personal mediante el establecimiento de normas relativas a los requisitos de localización de datos, la disponibilidad de los datos para las autoridades competentes y la portabilidad de datos para los usuarios profesionales*"[37]. En su ámbito de aplicación se encuentra todo tratamiento de datos no personales que "*se preste como un servicio a usuarios que residan o tengan un establecimiento en la Unión, independientemente de si el proveedor de servicios está establecido o no en la Unión*"[38].

Debido a la generalidad de su ámbito de aplicación, este reglamento abarcaría los servicios previstos para el proyecto INESDATA. Sin embargo, habrá que poner especial atención en ciertas materias, como el cambio de proveedor de transferencias de datos, las cuales quedan subordinadas a exigencias normativas más especificas como se indica en el Reglamento de Datos, "*el presente Reglamento complementa el enfoque de autorregulación del Reglamento (UE) 2018/1807 mediante la introducción de obligaciones de aplicabilidad general sobre el cambio de nube*"[39].

3.1.4. Ley 37/2007, sobre reutilización de la información del sector público

Transposición nacional de la Directiva (UE) 2019/1024 relativa a los datos abiertos y la reutilización de la información del sector público cuyo objeto se centra en establecer una regulación básica aplicable a la reutilización de documento elaborados y custodiados por entidades públicas. Concretamente, los contenidos de la presente ley son aplicable a:

- La Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local.

[37] Artículo 1 del NPDR

[38] Artículo 2.1.b) del NPDR

[39] Artículo 1.7 del DA

- Los organismos y entidades del sector público institucional creados para satisfacer necesidades de interés general, que no tengan carácter industrial o mercantil
- Las sociedades mercantiles pertenecientes al sector público institucional

En este sentido, la aplicabilidad de esta norma en el proyecto de INESDATA vendrá determinada si alguno de los proveedores de datos es una entidad del sector público recogido dentro de su ámbito de aplicación.

De la misma manera existe un real decreto complementario de desarrollo de esta ley, el Real Decreto 1495/2011 sobre reutilización de la información del sector público, para el ámbito del sector público estatal, cuyo objeto profundiza concretamente en "*lo relativo al régimen jurídico de la reutilización, las obligaciones del sector público estatal, las modalidades de reutilización de los documentos reutilizables y el régimen aplicable a documentos reutilizables sujetos a derechos de propiedad intelectual o que contengan datos personales*"[40]. Este Real decreto devendrá obligatorio para aquellas entidades del sector público estatal que aspiren a reutilizar información y proporcionarla a la plataforma

3.2. Seguridad

Con objeto de alcanzar un nivel de seguridad adecuado en la plataforma, y simultáneamente cumplir con los requisitos complementarios de seguridad derivados de normativas aplicables al proyecto como el Reglamento de Gobernanza de datos y el Reglamento General de Protección de Datos Personales, se ha procedido a valorar la aplicabilidad del estándar nacional reconocido para alcanzar un nivel de seguridad adecuado en las administraciones públicas, el Esquema Nacional de Seguridad.

3.2.1. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

La Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión tenía por objeto coordinar el esfuerzo legislativo europeo con el objetivo de garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (Directiva NIS), entre sus preceptos más relevantes se encontraban ciertos requisitos a implementar por los países miembros: como la elaboración de "*una estrategia nacional de seguridad de las redes y sistemas de información*"[41] o el establecimientos de "*requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales*"[42]. la Directiva NIS se ha traspuesto a través del Real Decreto-ley 12/2018, de seguridad de las redes y sistemas de información, cuyo objeto se centra en mejorar los mecanismos de protección frente a amenazas

[40] Artículo 1.1 del Real Decreto 1495/2011

[41] Artículo 1.2.a) de la NIS

[42] Articulo 1.2.d) de la NIS

que afecten a las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establecer un sistema de notificación de incidentes. Erigiéndose como la primera norma en España en regular la seguridad lógica de redes y sistemas de información vinculadas a los servicios esenciales.

Dentro de su articulado, encontramos que en su definición de "servicio digital" nos remite a la definición contenida en la Ley 32/2002, que si bien la analizaremos en un apartado posterior podemos avanzar que define estos servicios como "*Todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario. El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios"* [43].Por tanto entenderíamos aplicable esta normativa para todos aquellos apartados referentes a la protección frente a amenazas de sistemas de información aplicables al proyecto.

Sin embargo, de cara a los requisitos tangibles a implementar este real decreto ley en su artículo 16 realiza una delegación normativa, indicando que "*el desarrollo reglamentario de este real decreto-ley preverá las medidas necesarias para el cumplimiento de lo preceptuado en el apartado anterior por parte de los operadores de servicios esenciales*."[44] Por lo que, deberemos recurrir a su desarrollo reglamentario para encontrar las ramificaciones que más pueden afectar al proyecto INESDATA, sin olvidar que será en este real decreto donde se contienen apartados no delegados como: el régimen sancionador, o el proceso establecido para la notificación de incidentes de seguridad.

3.2.1.1. Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

Este real decreto de desarrollo, en lo que nos respecta, tiene por objeto "*la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y la gestión de incidentes de seguridad*"[45] extendiéndose bajo el mismo ámbito de aplicación que el Real Decreto Ley al que acompaña concretando que "Este Real decreto se aplicará a la prestación de: Los servicios digitales que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube."[46]

En cuanto al establecimiento de medidas concretas de aplicación por los proveedores de servicios digitales, aunque en su artículo 6 comienza estableciendo algunas obligaciones concretas como la necesidad de aprobar una política de seguridad, llegando a establecer sus contenidos mínimos, lo

[43] Anexo "Definiciones" de la LSSICE

[44] Artículo 16.2 del RDLSRSI

[45] Artículo 1 del RDDSRSI

[46] Artículo 2.1.b) RDDSRSI

cierto es que a la hora de la verdad este real decreto vuelve a referenciar a otra normativa específica como extensión de sus contenidos, indicándonos "*Las medidas a las que se refieren los apartados anteriores tomarán como referencia las recogidas en el anexo II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, en la medida en que sean aplicables, y se basarán, cuando sea posible, en otros esquemas nacionales de seguridad existentes."*[47]Por lo que, a pesar de no perder de vista los preceptos contenido en este real decreto en materia de medidas para el cumplimiento o gestión de incidentes de seguridad, debemos acudir al Esquema Nacional de Seguridad si queremos encontrar un desarrollo concreto de medidas técnicas aplicables al proyecto INESDATA.

3.2.2. Real Decreto 311/2022, (ENS) de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

El Esquema Nacional de Seguridad tiene la consideración de norma jurídica con rango de ley, cuyo contenido recoge *los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación"* [48] ,poniendo un elevado énfasis en preservar sus 5 dimensiones de seguridad reconocidas: la confidencialidad, la integridad, la trazabilidad, la autenticidad, y la disponibilidad de los datos, la información y los servicios utilizados por medios electrónicos que gestionen la entidades comprendidas dentro de su ámbito de aplicación. Las entidades que se encuentran obligadas al cumplimiento del esquema se recogen en tres subgrupos:

- Todo el Sector Público en los términos que recoge la Ley de Régimen Jurídico del Sector Público[49]
- Los sistemas que tratan información clasificada
- Los sistemas de información de las entidades del sector privado que en virtud de una relación contractual preste servicios o provean soluciones a las entidades del sector público

Por lo que respecta a INESDATA, podemos entender sin lugar a dudas que el Esquema Nacional de Seguridad incidiría directamente sobre el proyecto. Bien debido a que el operador de la plataforma sea considerado como entidad pública, en tal caso su aplicación devendría obligatoria debido a la naturaleza jurídica de la entidad responsable. Bien debido a que se proporcione un servicio de intermediación a entidades del sector público en el ejercicio de sus competencias y potestades administrativas, en tal caso sería obligatoria su aplicación debido a la posición de proveedor de la administración pública por parte de la entidad responsable. O finalmente encontrándose en la obligación, como veníamos indicando en apartados anteriores, derivado de la proporción de un servicio digital, incluido bajo los ámbitos de aplicación sucesivamente referenciados en: La Directiva NIS, Real Decreto-Ley de seguridad de las redes y sistemas de

[47] Articulo 6.5 del RDDSRSI

[48] Artículo 1.2 del ENS

[49] Articulo 2 y 156.2 de la Ley 40/2015

información, y Real Decreto de Desarrollo de seguridad de las redes y sistemas de información. Entendiendo su aplicabilidad fuera de toda duda

3.3. Privacidad

Atendiendo a la naturaleza del proyecto, las obligaciones en materia de privacidad y protección de datos se erigen como deberes ineludibles para cualquier aplicación práctica de la plataforma. Ya sea debido al tratamiento de datos personales de los usuarios de la plataforma, o del tratamiento mucho más delicado de datos personales contenidos en los data-sets proporcionados por los proveedores de datos. Teniendo clara esta realidad, entraremos aun así a valorar detenidamente la aplicabilidad de cada uno de los cuerpos normativos que regulan estas obligaciones en nuestro país.

3.3.1. Reglamento (UE) 2016/679 (Reglamento general de datos Personales)

El Reglamento general de protección de datos establece un marco de protección aplicable a todo tipo de tratamientos de datos personales, y la circulación de los mismos, pertenecientes a personas físicas. Teniendo en cuenta la amplitud de su objeto su ámbito de aplicación es correlativamente amplio, aplicándose a todo tipo de tratamiento "*total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero*"[50].

Si estimamos que los casos de uso de la plataforma INESDATA albergarán indistintamente datos personales, ya sea a través del tratamiento de datos de usuarios o mediante la inclusión de data-sets conformados por datos personales que permitan la identificación o identificabilidad de posibles interesados, entendemos que serán exigibles todos aquellos requerimientos derivados de esta normativa.

No se debe perder de vista las particularidades incluidas en la legislación nacional, que complementa al reglamento europeo, siendo esta la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales. La cual se entiende directamente aplicable en todo aquello que no contradiga al reglamento europeo al que acompaña. Entre sus obligaciones se encuentra una remisión expresa al esquema nacional de seguridad en cuanto a medidas de seguridad aplicables, concretando que se "*deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad*"[51].

[50] Artículo 2.1 del RGPD

[51] Disposición adicional primera de la LOPDGDD

3.4. Legislación Sectorial

En este apartado se recogen actualmente todas las normativas aplicables que, si bien complementan especialmente a una norma o conjunto de normas ya analizadas en los subgrupos anteriores, contienen implicaciones normativas que desbordan o exceden dichos preceptos compatibles.

3.4.1. Reglamento (UE) 2022/2065 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales)

Este reglamento europeo establece un marco que asegure el "*correcto funcionamiento del mercado interior de servicios intermediarios estableciendo normas armonizadas para crear un entorno en línea seguro, predecible y fiable que facilite la innovación y en el que se protejan efectivamente los derechos fundamentales*" [52]. A estos efectos este reglamento entiende como "servicio intermediario"[53]:

- Los servicios de mera trasmisión, en el que se traslade en una red de comunicaciones, información facilitada por el destinatario del servicio, o se facilite el acceso a una red de comunicaciones con este fin.
- Todo servicio de memoria cache que trasmita información a través de una red de comunicaciones y la almacene automática y temporalmente para facilitar su transmisión a otros usuarios que la soliciten posteriormente, con el fin de mejorar la eficiencia de la transmisión.
- Todo servicio de «alojamiento de datos», consistente en almacenar datos facilitados por el destinatario del servicio y a petición de este.

Como podemos apreciar, todos estos servicios intermediarios han sido planteados y serán cubiertos por funcionalidades del espacio de datos propuesto en INESDATA. Con lo que se puede determinar acertadamente que los preceptos contenidos en esta normativa serán de aplicación para el proyecto y deberán consecuentemente satisfacerse durante el desarrollo.

3.4.2. Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio electrónico

Algo adyacente pero aun aplicable encontramos la Ley de servicios de la sociedad de la información y de comercio electrónico, que tiene por objeto principal la trasposición de la Directiva 2000/31/CE en nuestro ordenamiento, y asienta un marco de regulación que delimita "*las obligaciones de los prestadores de servicios incluidos los que actúan como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable*

[52] Artículo 1.1 del DSA

[53] Articulo 2.g) del DSA

a los prestadores de servicios de la sociedad de la información"[54]. A efectos de aplicabilidad, esta regulación abarca todo prestador de servicios establecido en España; entendiendo este establecimiento como toda entidad cuya "*residencia o domicilio social se encuentren en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios. En otro caso, se atenderá al lugar en que se realice dicha gestión o dirección*"[55].

Teniendo en cuenta su objeto y alcance, es evidente que esta normativa aplica de manera directa al proyecto de INESDATA, particularmente en la dimensión de proveedor de servicios de intermediación que ostentará el operador de la plataforma, lo que consecuentemente le atribuye el rol de prestador de servicios e intermediario en cuanto a los procesos provistos para la trasmisión de datos, comunicaciones comerciales, y celebración de contratos electrónicos. Sin embargo, hemos de puntualizar que esta normativa aplica de manera directa pero complementaria al proyecto de INESDATA, debiendo priorizarse regulaciones más específicas al objeto del proyecto como las previstas en normativas como el Reglamento de Servicios Digitales en lo que se refiere a servicios de intermediación, o el Reglamento General de Protección de datos en lo que respecta a tratamientos de datos personales. Tomando un segundo plano particularmente las implicaciones recogidas en su régimen sancionador.

3.4.3. Ley 7/1998, sobre condiciones generales de la contratación.

Dentro de los objetivos del proyecto de INESDATA, particularmente en lo que respecta a las aplicaciones tangibles del repositorio de datos, se plantea la perspectiva de brindar un servicio a potenciales consumidores finales que justifique la extracción de valor deseada de los datos proporcionados por los proveedores. La legitimidad y transparencia de esta prestación de servicios requiere imperativamente la creación de una documentación contractual exhaustiva que norme y regule esta relación entre diversas entidades jurídicas, facultando la provisión de los medios y recursos necesarios para la consecución de un objetivo común previamente acordado.

Debido a que estos contratos poseerán condiciones generales de contratación, así como *"cláusulas predispuestas cuya incorporación al contrato sea impuesta por una de las partes"*[56], y serán proporcionados por el operador de la plataforma actuando "*dentro del marco de su actividad profesional o empresarial, ya sea pública o privada*"[57], estos contratos deberán atender en todas aquellas condiciones generales a los preceptos aplicables contenidos en esta ley.

[54] Artículo 1.1 de la LSSICE

[55] Articulo 2.1 de la LSSICE

[56] Articulo 1.1 de la LGC

[57] Artículo 2.2 de la LGC

3.4.4. Ley 15/2007, de Defensa de la Competencia.

Puesto que se encuentra dentro del alcance del proyecto la provisión de un servicio a un numero indeterminado de clientes finales, y la participación activa en el mercado de servicios, se deberán atender los preceptos recogidos en la ley de defensa de competencia destinada a "reforzar los mecanismos existentes en el mercado y dotarlo de los instrumentos para proteger la competencia efectiva en el mismo"[58]. En concreto, y de cara al proyecto, se deberá prestar especial atención a los contenidos del Título I, referentes a las cuestiones sustantivas reguladas por la legislación; y al Título V, referente al régimen sancionador aplicable en caso de incumplimiento.

[58] Preámbulo I de la LDC

ANEXO A. BIBLIOGRAFÍA

Marco normativo:

- REGLAMENTO (UE) 2023/2854 del parlamento europeo y del consejo de 13 de diciembre de 2023 sobre normas armonizadas para un acceso justo a los datos y su utilización, y por el que se modifican el Reglamento (UE) 2017/2394 y la Directiva (UE) 2020/1828 (Reglamento de Datos)
- REGLAMENTO (UE) 2022/2065 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales)
- REGLAMENTO (UE) 2022/868 del parlamento europeo y del consejo de 30 de mayo de 2022 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos)
- REGLAMENTO (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea
- REGLAMENTO (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios. [03/05/2022]
- Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

Otras publicaciones:

- "*Aproximación a los Espacios de Datos desde la perspectiva del RGPD*" - Agencia Española de Protección de Datos [Mayo 2023]
- "*Design Principles for Data Spaces*" - International Data Spaces Association [Abril 2021]
- "*Elementos de un espacio de Datos*" - Francisco Javier Esteve Pradera [Junio 2022]

ANEXO B. TABLA REFERENCIAL

Roles Referenciados

Titular de los Datos	*"toda persona jurídica […] o persona física que no sea el interesado con respecto a los datos específicos en cuestión, que, de conformidad con el Derecho de la Unión o nacional aplicable, tenga derecho a conceder acceso a determinados datos personales o no personales o a compartirlos"*	REGLAMENTO (UE) 2022/868 relativo a la gobernanza europea de datos (Reglamento de Gobernanza de Datos)
	"una persona física o jurídica que tiene el derecho o la obligación […] de utilizar y poner a disposición datos, incluidos, cuando se haya pactado contractualmente, los datos del producto o los datos de servicios relacionados que haya extraído o generado durante la prestación de un servicio relacionado"	REGLAMENTO (UE) 2023/2854 sobre normas armonizadas para un acceso justo a los datos y su utilización (Reglamento de Datos)
	"toda persona física o jurídica […] que tengan el derecho o la obligación, de conformidad con el presente Reglamento, con el Derecho de la Unión aplicable o con la legislación nacional por la que se aplique el Derecho de la Unión, o, en el caso de los datos no personales, mediante el control del diseño técnico de un producto y de los servicios conexos, de poner a disposición, así como de registrar o entregar determinados datos, restringir el acceso a ellos o intercambiarlos"	Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios.
	"una entidad que posee la autoridad suficiente para decidir como terceros pueden usar sus datos"	"*Design Principles for Data Spaces*" - International Data Spaces Association
	"aquel titular de los derechos de acceso y utilización de los datos"	*"Elementos de un espacio de Datos*" - Francisco Javier Esteve Pradera
	"en marcos generales de Espacios de Datos se puede encontrar esta figura etiquetada como el "dueño de los datos" o "custodio de los datos". Esta denominación es engañosa cuando se refiere a datos personales, porque un responsable de tratamiento no posee los datos de los Interesados o Sujetos de los Datos, sino que dispone de una base jurídica que lo legitima para su tratamiento"	"*Aproximación a los Espacios de Datos desde la perspectiva del RGPD*" - Agencia Española de Protección de Datos

Proveedor de los Datos	*"Toda entidad responsable de recoger y preprocesar datos, así como ponerlos a disposición de terceros por cuenta del Titular de los datos"*	*"Design Principles for Data Spaces"* - International Data Spaces Association
	"Un proveedor de datos recoge datos y los ofrecen en el espacio de datos por medio del catálogo de datos"	*"Elementos de un espacio de Datos"* - Francisco Javier Esteve Pradera
Supervisor de Solicitudes	*"aquellas entidades encargadas de evaluar las solicitudes presentadas por parte de un Usuario de Datos para el tratamiento de datos […], la concesión de la solicitud puede estar sujeta a distintas normativas y principios éticos"*	*"Aproximación a los Espacios de Datos desde la perspectiva del RGPD"* - Agencia Española de Protección de Datos
	"es preciso que los Estados miembros designen, establezcan o faciliten la creación de organismos competentes para respaldar las actividades de los organismos del sector público que se ocupen de autorizar la reutilización de determinadas categorías de datos protegidos"	REGLAMENTO (UE) 2022/868 relativo a la gobernanza europea de datos (Reglamento de Gobernanza de Datos)
Operador de la Plataforma	*"toda entidad que proporciona distintos tipos de infraestructura […] siendo a su vez responsable de la gobernanza de la plataforma, proviniendo servicios de apoyo, definiendo los términos y condiciones […] sobre la admisión y retirada de conjuntos de datos o participantes. […] Los operadores del mercado de datos deben establecer mecanismos que garanticen el cumplimiento de las políticas de uso de datos"*	*"Design Principles for Data Spaces"* - International Data Spaces Association
	"todos los participantes que se encarguen de la operación del espacio […] siendo los encargados de certificar tanto a los participantes, como sus conectores, y el resto de los componentes software del espacio. Para todos ellos, deben emitir acreditaciones para su identificación y autenticación. También ejercen la gobernanza del espacio de datos y definen el roadmap de funcionalidades"	*"Elementos de un espacio de Datos"* - Francisco Javier Esteve Pradera
	"las entidades que establecen las relaciones en el Espacio de Datos entre los Sujetos de los Datos y/o Titulares de los Datos, por una parte, y los Usuarios de los Datos, por otra. Son aquellos que implementan los medios técnicos, jurídicos, organizativos, o de otro tipo	*"Aproximación a los Espacios de Datos desde la perspectiva del RGPD"* - Agencia Española de Protección de Datos

	que permiten la operación del espacio de datos entre múltiples titulares y múltiples usuarios de datos"	
Proveedor Tecnológico	"aquel rol que ejercen aquellos participantes que proporcionan componentes para el funcionamiento del espacio de datos que no son servicios de intermediación, ni aplicaciones, sino que permiten que se ofrezca un ecosistema de intercambio de datos con seguridad y confianza"	*"Elementos de un espacio de Datos"* - Francisco Javier Esteve Pradera
Usuario de Datos	"toda persona física o jurídica que tenga acceso legítimo a determinados datos personales o no personales y el derecho, incluido el que le otorga el Reglamento (UE) 2016/679 en el caso de los datos personales, a usarlos con fines comerciales o no comerciales"	REGLAMENTO (UE) 2022/868 relativo a la gobernanza europea de datos (Reglamento de Gobernanza de Datos)
	"una persona física o jurídica que tiene acceso legítimo a determinados datos sanitarios electrónicos personales o no personales y está autorizada a usarlos con fines comerciales o no comerciales"	Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios.
	"una persona física o jurídica que actúa con un propósito relacionado con su actividad comercial, empresa, oficio o profesión, distinta del usuario de un producto conectado o servicio relacionado, a disposición de la cual el titular de datos pone los datos, incluso un tercero previa solicitud del usuario al titular de datos o de conformidad con una obligación legal"	REGLAMENTO (UE) 2023/2854 sobre normas armonizadas para un acceso justo a los datos y su utilización (Reglamento de Datos)
Entidades Supervisoras	"en materia de protección de datos, las autoridades competentes serán las indicadas en el RGPD, que en el caso de España será la AEPD, o las Autoridades Autonómicas de acuerdo con su competencia. Cuando otras autoridades actúen como autoridades competentes, por ejemplo, con arreglo a la DGA, lo deben hacer sin perjuicio de las facultades y competencias de supervisión de otras autoridades responsables"	"*Aproximación a los Espacios de Datos desde la perspectiva del RGPD*" - Agencia Española de Protección de Datos
Sujeto de los Datos	*"en marcos generales de espacios de datos, el Interesado o Sujeto de los Datos, es decir, la persona física identificada o identificable cuyos datos personales son los que se plantea tratar, podría asociarse a la definición de "productor de los datos" utilizada en algunos esquemas de Espacios de Datos.*	"*Aproximación a los Espacios de Datos desde la perspectiva del RGPD*" - Agencia Española de Protección de Datos

Productor de los Datos	*Cuando se asocia la figura de "productor de los datos" a sistemas o servicios que recogen o generan datos personales de personas físicas"*	
	toda persona física o jurídica que "*genere datos sin ser necesariamente los dueños de los mismos, ni los proveedores"*	*"Elementos de un espacio de Datos"* - Francisco Javier Esteve Pradera
Habilitador	*"los Habilitadores en el entorno de un Espacio de Datos serían aquellos que darán apoyo a todos los intervinientes anteriormente descritos para poder garantizar que la implementación se realiza un proceso eficiente, coherente, implementando los mecanismos de gobernanza y gestión entre múltiples intervinientes, evitando duplicidades y repeticiones de tareas, facilitando los trámites y solicitudes"*	*"Aproximación a los Espacios de Datos desde la perspectiva del RGPD"* - Agencia Española de Protección de Datos
	"servicios que no añaden directamente valor a los datos pero que se requieren para la publicación y búsqueda de recursos para el registro de transacciones"	*"Elementos de un espacio de Datos"* - Francisco Javier Esteve Pradera
Proveedores de Servicios y Aplicaciones	*"los servicios de almacenamiento en la nube, de análisis, el software de intercambio de datos, los navegadores, los complementos para navegadores o los servicios de correo electrónico no deben considerarse servicios de intermediación de datos en el sentido de lo dispuesto en el presente Reglamento, siempre que dichos servicios solo suministren herramientas técnicas para que los interesados o los titulares de datos intercambien datos con terceros, pero el suministro de dichas herramientas no se use con el objeto de establecer una relación comercial entre titulares de datos y usuarios de datos, […] Esto excluiría los servicios que obtienen datos de titulares de datos y que los agregan, enriquecen o transforman con el fin de añadirles un valor sustancial"*	REGLAMENTO (UE) 2022/868 relativo a la gobernanza europea de datos (Reglamento de Gobernanza de Datos)
	"provee aplicaciones que añaden valor a los datos, como pueden ser modelos de machine learning, procesos de limpieza, visualización, transformación, aplicaciones de anonimización, etc.."	*"Elementos de un espacio de Datos"* - Francisco Javier Esteve Pradera

Anexo 3: Modelos contractuales tipo definidos bajo el marco de gobernanza

Contenido

1. Introducción

1.1. Propósito

La redacción de este documento de Modelos Contractuales para el Espacio de Datos Federado, objeto del proyecto de INESData, tiene como objetivo establecer un marco jurídico y operativo que regule las relaciones entre los diferentes actores que participan en el acceso, intercambio y uso de datos. Este marco abarca varios documentos clave que definen las condiciones generales de participación, las responsabilidades de las partes, los derechos sobre los datos y las normas de gobernanza del Espacio.

El primer documento, Acuerdo de Adhesión al Espacio de Datos Inesdata, tiene como finalidad formalizar la incorporación de nuevas partes al Espacio de Datos, proporcionando la información necesaria sobre cada parte adherente, así como estableciendo los términos bajo los cuales se lleva a cabo su adhesión. Tras el Acuerdo de Adhesión, las partes acuerdan suscribirse al Convenio Constitutivo del Espacio de Datos, mediante el cual se establecen las bases para la creación y funcionamiento del Espacio de Datos.

Las Condiciones generales establecen los términos y condiciones bajo los cuales las partes pueden participar y operar dentro del Espacio. En ellas se reflejan diversas responsabilidades y aspectos críticos relacionados con el uso y gestión de los datos. Además, definen las normas de confidencialidad, seguridad y cumplimiento normativo.

El Modelo de gobernanza regula el marco organizativo que define cómo se toman las decisiones, cómo se gestionan los cambios y cómo se resuelven los conflictos dentro del Espacio. Este modelo asegura que todas las partes involucradas operen bajo un conjunto claro de reglas, promoviendo la transparencia, la equidad y la eficiencia en la gestión del Espacio de Datos.

Por último, las Condiciones Específicas de Uso del Conjunto de Datos abarcan las normas particulares que se aplican al tratamiento de los datos dentro del Espacio, según el tipo de información y las necesidades del proyecto. Estas condiciones incluyen aspectos relacionados con la licencia de uso de los datos, la protección de la privacidad y la seguridad, las limitaciones de uso y las responsabilidades en caso de incumplimiento.

1.2. Acrónimos

Acrónimo	Concepto
EEE	Espacio Económico Europeo.
LOPDGDD	Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales.
RGPD	Reglamento General de Protección de Datos.
UE	Unión Europea.

2. Acuerdo de Adhesión al Espacio de Datos Inesdata

2.1. Partes interesadas

PARTE ADHERENTE

Por una parte, _____ con CIF _____ en adelante denominado como "PARTE ADHERENTE", con domicilio social en _____, representado en este acto por D./Dña._____ DNI _____ , en su calidad de _____, con poderes suficientes para obligar al mismo.

OPERADOR DEL ESPACIO DE DATOS

Y por otra parte, _____ con CIF _____ en adelante denominado como "OPERADOR", con domicilio social en _____, representado en este acto por D./Dña._____ DNI _____ , en su calidad de _____, con poderes suficientes para obligar al mismo.

2.2. Manifiestan

Que PARTE ADHERENTE manifiesta la voluntad de adherirse de un Espacio de Datos, denominado INESDATA – **[Incluir Referencia del Demostrador]**, el cual estará sujeto a las cláusulas que se pacten en el presente acuerdo y la normativa aplicable en el territorio español y el espacio europeo.

Las dos partes se reconocen expresa y recíprocamente capacidad legal suficiente para constituir el presente Acuerdo, y por ello acuerdan las siguientes clausulas.

2.3. Clausulas

2.3.1. Antecedentes

1. La PARTE ADHERENTE ha manifestado su interés en adherirse al Convenio Constitutivo del Espacio de Datos INESDATA – **[Incluir Referencia del Demostrador]** destinada a la compartición voluntaria, soberana y segura de **[Añadir tipología especifica de datos**

tratados por el demostrador] en base a una infraestructura descentralizada, firmado en fecha **[Incluir fecha de firma de Convenio Constitutivo]**.

2. El Espacio de Datos opera como un repositorio de **[Añadir especificidades de los datos tratados por el demostrador]** con el propósito de facilitar el intercambio, almacenamiento y acceso a la información entre proveedores y consumidores finales de datos del espacio.

3. Con el fin de regular las relaciones entre el Operador del Espacio de Datos y los nuevos adherentes, se establece el presente Acuerdo de Adhesión.

4. La ratificación y subsecuente adhesión al Acuerdo Constitutivo permitirá a la PARTE ADHERENTE acceder a todas las funcionalidades dispuestas en el Espacio de Datos INESDATA **[Añadir especificidades de los datos tratados por el demostrador].** Siempre que su pretensión y condición sea validada previamente por el supervisor de solicitudes acorde a la normativa interna del Espacio de Datos.

2.3.2. Adhesión al acuerdo

5. La Parte Adherente ha manifestado su interés expreso en adherirse al Convenio Constitutivo del Espacio de Datos INESDATA – **[Incluir Referencia del Demostrador]**. La adhesión a dicho acuerdo permitirá a la PARTE ADHERENTE asumir el rol de usuario de datos, con todos los derechos y responsabilidades derivados del mismo.

6. Cualquier modificación o enmienda a este contrato deberá ser acordada por escrito y firmada por ambas partes. El Comité Directivo se reserva el derecho de realizar modificaciones al Convenio Constitutivo, las cuales entrarán en vigor de manera automática para todos los adherentes del Espacio de Datos.

7. El Adherente manifiesta su plena conformidad y aceptación con los términos y condiciones establecidos en el Convenio Constitutivo del Espacio de Datos, comprometiéndose a cumplirlos en su totalidad.

2.3.3. Entrada en Vigor y Aplicación

8. El presente Acuerdo de Adhesión entrará en vigor a partir de su ejecución por la PARTE ADHERENTE y después de que haya sido debidamente aprobado por el Comité Directivo de INESDATA, previo informe positivo del supervisor de solicitudes.

9. El presente acuerdo tendrá una duración indefinida. A la terminación por cualquier circunstancia de la condición de usuario de datos, la PARTE ADHERENTE perderá automáticamente todos sus beneficios y derechos de acceso al Espacio de Datos.

10. El Comité Directivo INESDATA **[Añadir especificidades de los datos tratados por el demostrador]** se reserva el derecho de revocar definitivamente la condición de usuario de datos en caso de incumplimiento del Convenio Constitutivo, los Términos y Condiciones Generales, las Condiciones de Uso de los Conjuntos de Datos, o el correspondiente Código de Conducta.

11. La terminación de este contrato podrá ser llevada a cabo por la PARTE ADHERENTE o por el Comité Directivo mediante notificación por escrito a la otra parte con al menos un mes de anticipación. En caso de terminación, ambas partes deberán cumplir con todas las obligaciones pendientes hasta la fecha de terminación.

12. El Adherente reconoce que su adhesión al Convenio Constitutivo del Espacio de Datos implica la aplicación plena de este acuerdo y sus consideraciones desde el momento de su firma.

2.3.4. Legislación Aplicable y Resolución de Conflictos

13. El presente Acuerdo se regirá e interpretará de conformidad con la legislación española, teniendo en cuenta los principios de derecho internacional privado, y la legislación europea aplicable.

14. Cualquier disputa, controversia o reclamación que surja de o en relación con los Datos compartidos en virtud del presente acuerdo o que guarde relación con él, incluida cualquier cuestión relativa a su existencia, validez, interpretación, cumplimiento o terminación, será resuelta definitivamente mediante arbitraje administrado por la Corte de Arbitraje de la Cámara Oficial de Comercio, Industria y Servicios de Madrid, de acuerdo con su Reglamento de Arbitraje vigente a la fecha de presentación de la solicitud de arbitraje. El número de árbitros será un único designado, la sede del arbitraje será Madrid (España) y el idioma del arbitraje será el español.

2.3.5. Contrapartes

El presente Acuerdo de Adhesión se firma en dos ejemplares idénticos, uno para la PARTE ADHERENTE y uno para el Operador del Espacio de Datos.

En ___el_____20

_____	_____
Nombre:	Nombre:
Título:	Título:

3. Convenio Constitutivo del Espacio de Datos

3.1. Partes

[Miembro Fundador 1]

Por una parte, _____ con CIF _____ en adelante denominado como "MIEMBROS FUNDADORES", con domicilio social en _____, representado en este acto por D./Dña._____ DNI _____ , en su calidad de _____, con poderes suficientes para obligar al mismo.

[Miembro Fundador 2]

Por una parte, _____ con CIF _____ en adelante denominado como "MIEMBROS FUNDADORES", con domicilio social en _____, representado en este acto por D./Dña._____ DNI _____ , en su calidad de _____, con poderes suficientes para obligar al mismo.

[Miembro Fundador 3]

Por una parte, _____ con CIF _____ en adelante incluido dentro del término "MIEMBROS FUNDADORES", con domicilio social en _____, representado en este acto por D./Dña._____ DNI _____ , en su calidad de _____, con poderes suficientes para obligar al mismo.

[...]

3.2. Manifiestan

Que las partes manifiestan la voluntad de creación de un Espacio de Datos, denominado INESDATA – **[Incluir Referencia del Demostrador]**, el cual estará sujeto a las cláusulas que se pacten en el presente contrato y la normativa aplicable en el territorio español y el espacio europeo.

Todas las partes se reconocen expresa y recíprocamente capacidad legal suficiente para constituir el presente Acuerdo, y por ello acuerdan las siguientes clausulas.

3.3. Clausulas

3.3.1. Antecedentes y Objetivo

1. Los MIEMBROS FUNDADORES contemplan establecer un Espacio de Datos denominado INESDATA – **[Incluir Referencia del Demostrador]** que permita compartir y potenciar el valor de **[Añadir tipología especifica de datos tratados por el demostrador]** en posesión tanto de organismos de la administración pública, como de proveedores del sector privado.
2. El Espacio de Datos operará como un repositorio de **[Añadir especificidades de los datos tratados por el demostrador]** con el propósito de facilitar el intercambio, almacenamiento y acceso a la información entre proveedores y consumidores finales de datos del espacio.
3. Con el fin de regular la ratificación de los principales acuerdos que regularán el espacio, y el reconocimiento jurídico entre los MIEMBROS FUNDADORES, se establece el presente Acuerdo de Adhesión.

3.3.2. El Espacio de Datos

4. El Espacio de Datos es caracterizado por contemplar la reutilización de información provista por determinados proveedores, la cual será almacenada en una infraestructura desplegada en servidores propiedad del proveedor tecnológico. Sobre dichos servidores se desplegará una infraestructura capaz de provisionar servicios de almacenamiento, procesamiento y visualización de datos con capacidad de escalado, monitorización y garantías de continuidad de servicio.
5. Para obtener más información sobre la infraestructura de la red de datos utilizada, se proporcionará un análisis en profundidad en el **[Incluir referencia al Documento de Infraestructura].**
6. Los Miembros Fundadores acuerdan que podrán adherirse nuevos MIEMBROS FUNDADORES al Espacio de Datos con sujeción a las condiciones reflejadas en **[Incluir referencia al Código de Conducta], [Incluir referencia al Documento de Modelo de Gobernanza], [Incluir referencia a las Condiciones Generales].**
7. El Espacio de Datos está sujeta a las siguientes disposiciones:

NO EXCLUSIVIDAD

8. Ninguna disposición del presente Convenio impide ni restringirá la participación de los MIEMBROS FUNDADORES en otras redes de datos, plataformas, ecosistemas o cualquier otro tipo de cooperación, ni el uso de servicios prestados por terceros.
9. En caso de actuar eventualmente como proveedores de datos dentro de INESDATA – **[Incluir Referencia del Demostrador]** las condiciones recogidas en este acuerdo y en sus anexos no impedirá ni restringirá que dicho proveedor de datos respectivo comparta dichos datos con terceros a su propia discreción.

GOBERNANZA DE LA RED

10. El marco de gobernanza que se aplicará a INESDATA – **[Incluir Referencia del Demostrador]** se definirá en más detalle en el **[Incluir referencia al Documento de Modelo de Gobernanza]**.

11. Los MIEMBROS FUNDADORES acuerdan designar que los representantes están debidamente autorizados para representar a la parte correspondiente en los órganos rectores tal y como se encuentran recogidos en el **[Incluir referencia al Documento de Modelo de Gobernanza]**. Además, los MIEMBROS FUNDADORES reconocen que las decisiones adoptadas por los órganos rectores son jurídicamente vinculantes para los mismos en virtud del presente Convenio.

12. Teniendo en cuenta la representación y los poderes otorgados a los representantes aquí reunidos, las partes reconocen el nombramiento de **[Incluir referencia a la entidad que actuará en concepto de Operador del Espacio de Datos]** como "Operador" del Espacio de Datos conforme a los preceptos recogidos en **[Incluir referencia al Documento de Modelo de Gobernanza]** anexado a este convenio.

EXCEPCIONES A LAS CONDICIONES GENERALES

13. Los MIEMBROS FUNDADORES han acordado sustituir las siguientes cláusulas de Condiciones Generales del siguiente modo:

[En caso sea aplicable, mencionar las cláusulas]

TERMINACIÓN Y VALIDEZ

14. Este Convenio se celebra por un período indefinido desde su fecha de entrada en vigor, tras la cual permanecerá en vigor por un tiempo indefinido hasta su rescisión.

15. Una vez acordada la rescisión del contrato las Partes no tendrán derecho a seguir utilizando los servicios o recursos del Espacio de Datos, puesto que dejarán de estar disponibles en términos de negociación como se indica expresamente en **[Incluir referencia a Las condiciones generales del servicio]**.

AVISOS

16. Todas las notificaciones previstas en el presente convenio deberán presentarse por escrito a los Representantes que figuran en el Anexo **[Incluir referencia a un la Lista de miembros y datos de contacto anexada]**.

17. Cualquier cambio en las personas de contacto o en los datos pertinentes deberá comunicarlo inmediatamente el respectivo MIEMBRO FUNDADOR al Comité Directivo de INESDATA – **[Incluir Referencia del Demostrador]** conformado por representantes de todas las partes firmantes.

LIMITACIÓN DE RESPONSABILIDAD

18. La responsabilidad total anual de cualquiera de las Partes bajo este Convenio no excederá del mayor entre dos valores de referencia: la cantidad de **[Incluir una cantidad ponderada bajo el régimen sancionador acorde a los criterios de la normativa]**, o **[Incluir un porcentaje ponderado bajo el régimen sancionador acorde a los criterios de la normativa]**de las

tasas a la parte incumplidora según este Convenio en el periodo de **[Incluir un plazo determinado para el establecimiento de la cantidad]** meses anteriores a la causa de la acción que da lugar a la reclamación bajo esta cláusula.

19. Sin perjuicio de las limitaciones de responsabilidad, el artículo 82 del Reglamento General de Protección de Datos (RGPD) se aplica a los daños referidos a los datos personales. La limitación de responsabilidad mencionada no limita el derecho del responsable del tratamiento a reclamar a los demás implicados en el mismo tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños, según el artículo 82 del RGPD.

3.3.3. Otros Términos

[En su caso añadir cualquier otro termino pertinente]

3.3.4. Entrada en vigor y aplicación

20. El presente Convenio de Constitución de INESDATA **[Añadir especificidades de los datos tratados por el demostrador]** entrará en vigor a partir de su ejecución por los MIEMBROS FUNDADORES, debidamente representados en este convenio.

3.3.5. Legislación Aplicable y Resolución de Conflictos

21. Este Convenio se regirá e interpretará según la legislación española, considerando los principios de derecho internacional privado, y la legislación europea aplicable.

22. Cualquier disputa, controversia o reclamación que surja de o en relación con los Datos compartidos en virtud del presente Convenio o que guarde relación con él, incluida cualquier cuestión relativa a su existencia, validez, interpretación, cumplimiento o terminación, será resuelta definitivamente mediante arbitraje administrado por la Corte de Arbitraje de la Cámara Oficial de Comercio, Industria y Servicios de Madrid, de acuerdo con su Reglamento de Arbitraje vigente a la fecha de presentación de la solicitud de arbitraje. El número de árbitros será un único designado, la sede del arbitraje será Madrid (España) y el idioma del arbitraje será el español.

3.3.6. Contraparte

El presente Convenio ha sido firmado en **[Incluir referencia del número de copias emitidas]** ejemplares idénticos, uno para cada MIEMBRO FUNDADOR.

En _____ el _____ 20__

_____ _____

Nombre: Nombre:

Título:

Título:

Nombre:

Título:

Nombre:

Título:

4. Condiciones generales

4.1. Aplicabilidad, ámbito de aplicación y gobernanza

1. El Espacio de Datos se establecerá mediante la formalización del Convenio Constitutivo, cuya firma o adhesión será preceptiva para todos los Miembros del Espacio.

2. Las disposiciones de las presentes Condiciones Generales serán aplicables y jurídicamente vinculantes para los acuerdos de puesta en común de datos de los miembros integrantes del Espacio de Datos a partir de la ejecución del Convenio Constitutivo y de los Acuerdos de Adhesión.

3. En caso de discrepancia entre cualquiera de los términos y condiciones establecidos en el Convenio Constitutivo, los Acuerdos de Adhesión y las presentes Condiciones Generales, incluidos sus apéndices o anexos, dicha discrepancia se resolverá de acuerdo con el siguiente orden de prioridad:

   - Las cláusulas del Convenio Constitutivo;
   - Las cláusulas de cualquier Acuerdo o Acuerdos de Adhesión;
   - Condiciones del uso de los datos;
   - Las presentes Condiciones Generales;
   - Otros Apéndices del Convenio Constitutivo por orden numérico.

4. Cualquier modificación o derogación de las presentes Condiciones Generales deberá acordarse en el Convenio Constitutivo para que sea válida.

4.2. Responsabilidades en relación con el servicio

5. En el contexto del Espacio de Datos INESDATA, los roles definidos cuyas funciones se encuentran estrechamente ligadas con la provisión del servicio regulado bajo estas Condiciones Generales son: el Proveedor de los Datos, el Supervisor de Solicitudes, el Operador/Promotor del Espacio de Datos, el Proveedor Tecnológico, los Consumidores Finales/Usuarios de Datos, así como todo Proveedor de Servicios y Aplicaciones.

6. Una Parte puede ocupar simultáneamente varias funciones. En tal caso, la Parte en cuestión deberá cumplir todas las obligaciones aplicables relacionadas con cada función y los Datos pertinentes. Además, el rol de Usuario Final es una función reconocida en estas Condiciones Generales que se aplica a cualquier parte interesada que no sea Parte del Convenio Constitutivo, pero que reciba datos.

7. Es importante puntualizar que en el Convenio Constitutivo se podrá incluir cualquier determinación específica de las responsabilidades esenciales de cada función regulada bajo estas condiciones de acordarse por los miembros fundadores.

4.2.1. Proveedor de los datos

8. El Proveedor de Datos se constituirá como el responsable de recoger y preprocesar datos, así como ponerlos a disposición del espacio bien por cuenta de un Titular de Datos tercero, o actuando como tal en caso de ostentar esta condición. Además, este rol será el responsable de poner a disposición los conjuntos de datos objeto del servicio en el catálogo de datos del Espacio por medio de formatos estandarizados especificados con más precisión en el documento de arquitectura o su documentación de apoyo.

9. Sus responsabilidades específicas se centran en:

   a) Velar por la firma de las Condiciones de Uso del Conjunto de Datos para que cualquier Dato se ponga a disposición dentro del Espacio de Datos.

b) Garantizar un método efectivo de control de divulgación de la información comercial de carácter confidencial y proveer un entorno de tratamiento seguro controlado.

c) Prohibir la utilización de aquellos resultados que contengan información que ponga en peligro los derechos e intereses de terceros.

d) Asistir a los usuarios en la obtención del consentimiento de los interesados o del permiso de los titulares de datos cuyos derechos e intereses puedan verse afectados por la reutilización, siempre que ello sea factible sin acarrear cargas desproporcionadas para el organismo del sector público.

e) Velar por que los datos confidenciales no se divulguen como consecuencia de permitir la reutilización.

f) Proporcionar orientación y asistencia a los usuarios para que cumplan con sus obligaciones.

g) Valorar la posibilidad de cobrar una tasa trasparente, no discriminatoria y proporcionada por permitir la reutilización.

h) Ofrecer los contenidos del conjunto de datos proporcionados, las restricciones de utilización, las licencias, la metodología de recopilación de datos y la calidad e incertidumbre de los datos descritos en un formato de lectura mecánica.

i) Proporcionar información a organismos del sector público, la Comisión, el Banco Central Europeo o un organismo de la Unión los datos que obren en su poder sobre los que se demuestre una necesidad excepcional, sin demora indebida, teniendo en cuenta las medidas técnicas, organizativas y jurídicas necesarias. Por la puesta a disposición tendrá derecho a una compensación justa en cumplimiento de una solicitud presentada por un organismo público.

j) No imponer entre las condiciones de uso de los datos que proporcione al espacio requisitos de localización específicos, salvo que estén justificados por razones de seguridad pública de conformidad con el principio de proporcionalidad.

k) Velar porque los documentos que se encuentren en su posesión puedan ser reutilizados para fines comerciales o no comerciales, sin estar sujetos a condiciones específicas a menos que estas sean objetivas, proporcionadas, no discriminatorias y estén justificadas por un objetivo de interés público.

l) Fijar las condiciones de utilización en licencias-tipo, las cuales podrán estar disponibles en formato digital y ser procesadas electrónicamente.

m) Promover que la puesta a disposición de los datos para su reutilización, así como que la tramitación de solicitudes de reutilización se realice por medios electrónicos.

n) Proporcionar en formato abierto, accesible, legible por máquina, y conjuntamente con sus metadatos. Su formato y los metadatos, en la medida de lo posible, deberán cumplir estándares y normas formales abiertas.

o) Velar por la firma de contratos que no otorguen derechos exclusivos, y mantener una reutilización abierta a todos los agentes potenciales del mercado, incluso en aquellos casos en los que varios agentes exploten ya productos con valor añadido basados en estos documentos. Solo será admisible la suscripción de acuerdos exclusivos cuando sean necesarios para la prestación de un servicio de interés público, y por un plazo inferior a 10 años por regla general.

p) Poner a disposición del público las condiciones finales de los acuerdos que, sin conceder expresamente un derecho exclusivo, conlleven una disponibilidad limitada a terceros para la reutilización de la información.

q) Nombrar o determinar la unidad responsable dentro de su organización de garantizar la puesta a disposición de su información.

4.2.2. Supervisor de solicitudes

10. Las funciones de este órgano se centrarán ejercer ciertas funciones de control y concesión de solicitudes de acceso a los datos a usuarios dentro del Espacio de Datos, actuando como punto de contacto, y asistiendo en la gestión de diversos procesos de tramitación documental.

11. Sus responsabilidades específicas se centran en:

    a) Asistir en los procesos de adhesión de nuevos miembros al espacio, actuando como punto de contacto para la aportación de la documentación pertinente.

    b) Evaluar las solicitudes presentadas por parte de un miembro del Espacio de Datos para el acceso a un conjunto de datos bajo los que exista algún tipo de restricción, emitiendo a su vez un informe no vinculante de decisión previa.

    c) Supervisar la recepción y el registro de las solicitudes.

    d) Evaluar la prioridad de las solicitudes.

    e) En el marco de un proceso de adhesión, emitir un informe no vinculante de decisión previa, que podrá ser o no validado por el Operador del Espacio de Datos, tras evaluar el compromiso del solicitante con los valores del Espacio de Datos.

    f) Informar del progreso de las solicitudes presentadas.

    g) Asegurar que las solicitudes cumplen con el marco contractual y organizacional del Espacio de Datos.

    h) Evaluar los posibles riesgos asociados a la inclusión de un conjunto de datos en el catálogo del Espacio de Datos.

    i) Garantizar que los usuarios tratan el conjunto de datos de acuerdo con la política de seguridad y de privacidad establecidas.

    j) Actuar como punto de contacto en cuanto al recibimiento de posibles solicitudes y comunicaciones de proveedores de herramientas o servicios dentro del espacio.

    k) Asistir al operador en la definición de las condiciones aplicables a los proveedores de herramientas o servicios dentro del espacio, de cara a que se respeten los derechos e intereses de los proveedores y usuarios del espacio.

    l) Participar en auditorías internas y externas.

    m) Auxiliar al Operador del Espacio de Datos y el Comité Directivo en la toma de decisiones.

4.2.3. Operador/Promotor del Espacio de Datos

12. El Operador del Espacio de Datos se constituirá como el proveedor principal de servicios de intermediación de datos, es decir, será la figura que gestionará los recursos del espacio y será el responsable principal de la gobernanza del Espacio de Datos.

13. A su vez será el responsable de aportar en el Espacio todos aquellos servicios esenciales que permitan la operativa, como los servicios de apoyo, la autenticación, o la identificación y gestión de identidades. Garantizando en todo momento la seguridad de los datos o proporcionando soluciones técnicas para el Espacio.

14. El Operador del Espacio de Datos será igualmente responsable de certificar tanto a los participantes, como el resto de los componentes software. Debiendo implementar todos aquellos medios técnicos, jurídicos y organizativos que permitan la operativa del Espacio de Datos entre múltiples proveedores y múltiples usuarios de datos de manera segura y bajo las suficientes garantías.

15. Sus responsabilidades específicas se centran en:

a) Prevenir la divulgación de cualquier información que ponga en peligro los derechos e intereses de terceros, que el usuario pueda haber adquirido a pesar de las garantías establecidas.

b) Prohibir la reidentificación de cualquier interesado al que se refieran los datos, adoptando las medidas técnicas y organizativas adecuadas destinadas a evitar dicha reidentificación y notificar al proveedor de datos cualquier violación de la seguridad de los datos que dé lugar a una posible reidentificación de los interesados.

c) En caso de reutilización no autorizada de datos no personales, informar sin demora a las personas jurídicas cuyos derechos e intereses puedan verse afectados, en su caso, con la ayuda del proveedor de datos.

d) En caso de no cederse por parte del proveedor de datos la totalidad de los derechos de explotación presentes en los conjuntos de datos, permitir únicamente la reutilización de datos con la condición de respetar los derechos de propiedad intelectual mantenidos sobre los mismos, en favor del proveedor o titular.

e) En caso de trasferir a un tercer país datos no personales protegidos por motivos de confidencialidad o por derechos de propiedad intelectual de terceros, informar al proveedor de datos de su intención de transferirlos y de la finalidad de la transferencia en el momento de solicitar y acordar la reutilización de dichos datos.

f) Aplicar las tasas de reutilización establecidas en las condiciones de uso de los datos acotadas por los proveedores.

g) Presentar una notificación a la autoridad competente en materia de servicios de intermediación de datos antes de entrar en funcionamiento del Espacio de Datos.

h) Deberá designar un representante legal en cada uno de los Estados miembros en los que ponga a disposición sus servicios de intermediación de datos.

i) Impedir la puesta a disposición de los datos aportados por los proveedores para fines distintos a los especificados durante su inclusión al catálogo de datos del espacio.

j) Incluir la oferta de herramientas y servicios específicos adicionales a los proveedores, titulares o a los interesados con el objetivo específico de facilitar el intercambio de los datos.

k) Velar por que el procedimiento de acceso a sus servicios, incluidos los precios y las condiciones de servicio, sea equitativo, transparente y no discriminatorio, tanto para los interesados como para los titulares de datos y los usuarios de datos.

l) Disponer de procedimientos para impedir prácticas fraudulentas o abusivas de los usuarios que deseen obtener acceso a través de sus servicios de intermediación de datos.

m) Asegurar, en caso de insolvencia, la continuidad razonable de la prestación de sus servicios de intermediación de datos. Y, cuando esos servicios de intermediación de datos incluyan el almacenamiento de datos, disponer de los mecanismos de garantía necesarios para que los titulares o proveedores de datos y los usuarios puedan acceder debidamente a los mismos, transferirlos o recuperarlos.

n) Adoptar las medidas adecuadas para garantizar la interoperabilidad con otros servicios de intermediación de datos, entre otros, mediante normas abiertas de uso común en el sector. Así como informar sin demora a los titulares de datos en caso de transferencia, acceso o utilización no autorizados de los datos no personales que haya compartido.

o) Actuar en el mejor interés de los titulares y proveedores, informándolos y, cuando corresponda, asesóralos de manera concisa, transparente, e inteligible sobre los usos previstos de los datos por los usuarios de datos y las condiciones generales aplicables a dichos usos.

p) Conservar un registro completo y actualizado de la actividad de intermediación de datos, el cual deberá contener cuando sea posible: una descripción adecuada del conjunto de datos, el título del conjunto de datos, el dominio, la lista de los diccionarios de datos disponibles, lista de formatos disponibles, lista de los tipos de datos, lista de todas las políticas empleadas en la recopilación y preparación del conjunto de datos, historial de revisiones, transformaciones

preexistentes, la fecha en que se inició y la fecha de la última entrada del conjunto de datos y un resumen estadístico.

q) Definir adecuadamente las condiciones aplicables a los proveedores de herramientas o servicios dentro del espacio, de cara a que se respeten los derechos e intereses de los proveedores y usuarios del espacio.

r) Poner a disposición de los miembros del espacio información clara sobre los costes estándar del servicio y las sanciones por resolución anticipada que podrían imponerse, o los servicios impliquen un cambio muy complejo o costoso, para los que sea imposible cambiar de proveedor sin interferencias significativas en los datos, los activos digitales o la arquitectura del servicio.

s) Indicar claramente en los sitios web de su propiedad, y a disposición de los miembros del espacio, la jurisdicción a la que está sujeta la infraestructura de TIC desplegada, así como una descripción general de las medidas técnicas, organizativas y contractuales adoptadas por el operador para impedir el acceso o transferencia internacionales por parte de las administraciones públicas de datos no personales que se encuentren en la Unión, cuando dicho acceso o transferencia pueda entrar en conflicto con el Derecho de la Unión o con el Derecho nacional.

4.2.4. Proveedor Tecnológico

16. El Proveedor Tecnológico será responsable de proporcionar todos aquellos componentes técnicos que permitan el despliegue y el funcionamiento del Espacio de Datos. Esto implica el desarrollo, configuración y parametrización de la infraestructura.

17. Ofreciendo un ecosistema de intercambio de datos basado en la seguridad y la confianza. Proporcionando la asistencia técnica necesaria tanto a los usuarios, los proveedores, y todos aquellos órganos encargados de la gestión del Espacio de Datos.

18. Sus responsabilidades específicas se centran en:

a) Adoptar todas las medidas razonables a su alcance para facilitar que el usuario, tras cambiar a un servicio que cubra el mismo tipo de servicio, logre la equivalencia funcional en el uso del servicio de tratamiento de datos de destino.

b) Facilitar el proceso de cambio proporcionando capacidades, información adecuada, documentación, apoyo técnico y, cuando proceda, las herramientas necesarias.

c) Debe poner gratuitamente interfaces abiertas a disposición de todos los usuarios y de los proveedores tecnológicos de destino afectados, de igual manera, para facilitar el proceso de cambio. Estas interfaces incluirán información suficiente sobre el servicio de que se trate para permitir el desarrollo de programas informáticos para comunicarse con los servicios, a efectos de la portabilidad de los datos y la interoperabilidad.

d) En el caso de servicios de tratamiento de datos distintos, el proveedor tecnológico deberá garantizar en la medida de los posible la compatibilidad con las especificaciones comunes basadas en especificaciones de interoperabilidad abiertas o normas armonizadas de interoperabilidad publicadas en el Repositorio Central de la Unión de Normas para la Interoperabilidad de los Servicios de Tratamiento de Datos.

e) Actualizar el registro en línea del catálogo de datos.

f) En caso de cambio entre servicios del mismo tipo de servicio, para los que no se hayan publicado las especificaciones comunes o las normas armonizadas de interoperabilidad en el Repositorio Central de la Unión de Normas para la Interoperabilidad de los Servicios de Tratamiento de Datos, el proveedor tecnológico deberá exportar, a petición del usuario, todos los datos exportables en un formato estructurado, de utilización habitual y de lectura mecánica.

g) No revelar o transferir activos digitales protegidos por derechos de propiedad intelectual o que constituyan un secreto comercial, a un usuario o a un proveedor diferente de servicios de

tratamiento de datos, ni a comprometer la seguridad y la integridad del servicio del usuario o del proveedor.

h) Facilitando la interoperabilidad, el proveedor tecnológico deberá asistir en el desarrollo de estructuras adecuadas de datos, formatos, vocabularios, sistemas de clasificación, taxonomías y listas de códigos. Así como asistir en su descripción de manera que se encuentren a disposición del público y contengan un lenguaje coherente.

i) Desarrollar los medios técnicos para acceder a los datos, tales como las interfaces de programación de aplicaciones, sus condiciones de uso y su calidad de servicio. Se describirán en una medida suficiente para permitir el acceso automático a los datos y su transmisión automática a los miembros, siendo esta de forma continua, en descarga masiva o en tiempo real, empleando un formato de lectura mecánica cuando sea técnicamente viable y no impida el buen funcionamiento del del espacio.

4.2.5. Consumidor Final/Usuario de Datos

19. Todo miembro adherido al Espacio de Datos que tenga acceso efectivo, o la intención, de acceder a determinados conjuntos de datos, se constituirá como el Consumidor Final del Espacio de Datos, teniendo acceso legitimo a determinados datos para utilizarlos, o no, con fines comerciales derivados de su actividad.

20. Su responsabilidad principal se erige en torno al respeto y alineamiento con los principios de uso de datos recogidos el Convenio Constitutivo, estas condiciones generales, así como todas las condiciones específicas que sean dispuestas por los proveedores de datos en cuanto a un conjunto de datos especifico.

21. Sus deberes se centrarán en:

a) Utilizar los conjuntos de datos de forma responsable y asumiendo el riesgo derivado de su uso.

b) Responder frente a terceros por daños que pudieran derivarse del uso ilegitimo de dichos datos.

c) No utilizar los datos provistos por los proveedores para fines distintos a los especificados durante su puesta a disposición.

d) No atribuir a los proveedores de datos cualquier uso ilícito de los datos, aportados al espacio, que se lleve a cabo por los usuarios del Espacio de Datos.

e) No atribuir a los proveedores de datos cualquier daño o pérdida económica, material o sobre datos, sufrida de forma directa o indirecta debido a un mal uso de los datos pertenecientes al catálogo del espacio.

f) No indicar de ningún modo que los proveedores de datos pertenecientes a la administración pública titulares de la información reutilizada participan, patrocinan o apoyan la reutilización que se lleve a cabo de ella.

g) En caso de proceder a trabajos derivados a partir del conjunto de datos, se deberá atribuir la autoría de los conjuntos de datos originales al proveedor o titular proveedor de los mismos.

h) No perseguir prácticas anticompetitivas, como el bloqueo, la limitación o dificultar de cualquier modo el acceso de otros usuarios terceros a los datos.

4.2.6. Proveedores de Servicios y Aplicaciones

22. Los proveedores de Servicios y Aplicaciones tendrán como responsabilidad primordial añadir valor a los conjuntos de datos, mediante los servicios y aplicaciones implementados y ofrecidos a través del espacio.

23. El Proveedor deberá entregar o prestar los servicios y aplicaciones de acuerdo con las condiciones establecidas por los órganos encargados de la gestión del Espacio de Datos.

24. Sus responsabilidades específicas se centran en:

a) Respetar en todo momento las condiciones existentes sobre un conjunto de datos concreto.

b) Asegurar que los datos incluidos en los servicios son precisos, completos y actualizados.

c) Implementar procesos de limpieza y validación de datos cuando sea posible y pertinente.

d) Integrar, cuando estén disponibles, diversas fuentes de datos para crear conjuntos más completos aumentando así el valor añadido a los servicios o aplicaciones ofrecidos dentro del espacio.

e) Añadir metadatos, etiquetas y estructurar los datos de manera que sean más accesibles y útiles para los usuarios en relación con los servicios o aplicaciones ofrecidos dentro del espacio.

f) Proporcionar funcionalidades avanzadas para facilitar la interpretación de los datos, o todo rendimiento que se pudiera extraer de los mismos.

g) Asistir al usuario a identificar áreas de mejora y de oportunidad para añadir valor adicional a los conjuntos de datos mediante sus herramientas y soluciones.

h) Colaborar con el operador y el proveedor tecnológico del espacio para mejorar el rendimiento de la infraestructura desplegada. Y en concreto atender, en la medida de lo posible, a todos los requerimientos que estos soliciten a dichos proveedores.

4.3. Responsabilidades Generales

4.3.1. Seguridad, protección y gestión de datos

25. Cada Miembro deberá designar a un representante y persona de contacto para asuntos de seguridad de datos, que será responsable de los sistemas del Miembro pertinente que estén conectados al Espacio y de la aplicación de la política de seguridad que rija el espacio.

26. Cada uno de los miembros del Espacio de Datos deberá disponer de capacidades suficientes para acceder a los Datos de forma segura y de conformidad con las normas pertinentes de seguridad de los datos establecidas por el operador en colaboración con el proveedor tecnológico, así como de manera individualizada por determinados proveedores de datos. Estas normas y medidas de seguridad establecidas estarán alineadas con los preceptos aplicable contenidos en el Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad.

27. Todas aquellas tecnologías y medidas técnicas serán recogidas debidamente en el **[Insertar Referencia a Documento de Infraestructura]** del Espacio de Datos.

28. Los miembros deberán aplicar y mantener medidas técnicas, organizativas y físicas adecuadas que se ajusten a las buenas prácticas del mercado, teniendo en cuenta la naturaleza de los datos tratados. Cada una de las Partes deberá tener la capacidad de cumplir adecuadamente sus obligaciones en virtud del Convenio Constitutivo y las Condiciones de Uso aplicables y, en caso necesario, de cesar las actividades de procesamiento de datos, sin demora indebida, por cualquier motivo pertinente requerido por el operador, el comité directivo, o cualquier otro órgano con atribuciones suficientes.

29. Las capacidades mencionadas incluyen, por ejemplo, la capacidad de controlar los Datos y su tratamiento mediante el conocimiento del origen de los Datos (en concreto, si el origen es el propio miembro, otro miembro o un Tercero); la base para el tratamiento de datos ya sean personales o no personales; las posibles restricciones y limitaciones, especificadas por determinados proveedores, que se apliquen al tratamiento de los Datos; y los derechos y restricciones que se aplican a la redistribución o refinamiento de los Datos.

30. Los miembros deberán ser capaces de identificar los Datos, eliminarlos o devolverlos en el caso de que la base mediante la cual se fundamentaba el tratamiento de datos expire. La obligación de eliminar o devolver los Datos no es aplicable a los Materiales Derivados.

31. En caso de identificar una violación de la seguridad que pudiera afectar potencialmente a los datos esta deberá ser debidamente documentada, rectificada y comunicada a las Partes

afectadas sin demora injustificada. Todas las Partes implicadas tienen la responsabilidad mutua de contribuir razonablemente a la investigación de cualquier violación de la seguridad de los datos en el Espacio de Datos.

4.3.2. Subcontratacion

32. Los miembros del espacio tendrán derecho a subcontratar y emplear a terceros subcontratistas bajo los que exista un contrato de proporción de servicios, pudiendo darles acceso a los datos del Espacio con autorización previa.

33. Las Partes serán responsables de toda acción, tratamiento o acceso llevado a cabo por a terceros subcontratistas como de las suyas propias se tratase.

34. Los miembros del espacio que empleen a terceros subcontratistas se harán cargo de cualquier daño o pérdida económica, sufrida de forma directa o indirecta a causa de un mal uso de los datos pertenecientes al catálogo del espacio.

4.4. Redistribución de Datos

35. Los Miembros del espacio tendrán derecho a redistribuir datos contenidos en el catálogo del espacio a a Terceros Usuarios Finales o Terceras Partes, siempre que dicha redistribución haya sido específicamente autorizada o confirmada por el Proveedor de datos de manera expresa, o haya incluido dicha posibilidad dentro de las condiciones específicas aplicables a dicho conjunto de datos.

36. Si el Proveedor de Datos opta por permitir la redistribución de los Datos a Terceros Usuarios Finales, el Proveedor de Datos será responsable de determinar las Condiciones de Uso del Conjunto de Datos que se aplican a la redistribución. El Proveedor de Servicios deberá incluir dichas condiciones relativas a la redistribución de Datos en cualquier acuerdo o condición con Terceros Usuarios Finales.

37. No obstante, lo anterior, las Partes tendrán derecho a redistribuir los Datos a sus empresas afiliadas, a menos que las Condiciones de uso del Conjunto de Datos aplicables prohíban explícitamente dicha redistribución. Siempre que dicha redistribución se mantenga dentro del ámbito de control del miembro del espacio.

38. Los derechos sobre el Material Derivado pertenecerán al usuario final que genere dicho Material Derivado y las restricciones de uso establecidas para los Datos en estas Condiciones generales no cubrirán el Material Derivado. Cualquier restricción de uso o redistribución del Material Derivado se establecerán explícitamente pro el proveedor de datos en las Condiciones de Uso del Conjunto de Datos especifico, si las hubiere.

39. Los Miembros del espacio tienen derecho a redistribuir Materiales Derivados a otros Miembros y a cualquier Tercero, a menos que esté específicamente prohibido en las Condiciones de Uso del Conjunto de Datos aplicable.

40. La redistribución de cualquier Dato Personal o Material Derivado creado sobre la base de cualquier Dato Personal puede estar sujeta a requisitos y restricciones más detallados. Cada responsable del tratamiento de datos garantizará por su cuenta que toda redistribución y uso del material derivado que se realice de conformidad con la legislación aplicable en materia de protección de datos. Además, toda conducta entre Responsables del tratamiento y Encargados del tratamiento estará sujeta a los Acuerdos de encargados de tratamiento de datos aplicables.

4.5. Tasas y costes

41. El acceso al catálogo de datos del Espacio podrá estar asociado al abono de un coste o tasa de carácter justo, acorde al Data Governance Act, la Ley 8/1989 de Tasas y Precios Públicos, y en última instancia alineado con el criterio recogido en la normativa europea de compensación justa por poner a disposición datos, incrementado por un margen razonable de beneficio.

42. Tal compensación cubrirá los costes técnicos y organizativos soportados a raíz del suministro de datos para su reutilización y tratamiento, limitada a los costes marginales en que se incurra para su puesta a disposición, difusión, y protección. Esta compensación puede ser incrementada por un margen de beneficio razonable de la inversión, incluidos en su caso, los costes de anonimización, seudonimización, agregación y de adaptación técnica, más un margen razonable.

43. Cada Miembro asumirá sus propios costes relacionados con el acceso al Espacio y su funcionamiento como Miembro de este. Para evitar dudas, el mantenimiento y la administración de la Red no incluyen los costes derivados del acceso al servicio que deberán ser soportados por los miembros cuando proceda, y según se definan en estas Condiciones generales.

4.6. Confidencialidad

44. Las Partes deberán utilizar cualquier información confidencial que reciban en relación con el funcionamiento del Espacio de Datos únicamente para los fines para los que se haya facilitado dicha información confidencial. Las Partes se abstendrán de utilizar o divulgar ilícitamente a terceros cualquier información confidencial de la que hayan tenido conocimiento en el curso del funcionamiento del Espacio de Datos.

45. A la expiración o terminación del Convenio Constitutivo, las Partes deberán dejar de utilizar la Información Confidencial y, a petición de cualquiera de las Partes, devolver o destruir de forma verificable cualquier copia de la misma. No obstante, lo anterior, las Partes tienen derecho a seguir utilizando los Datos con sujeción a la cláusula 10. Además, las Partes podrán conservar copias de la Información Confidencial según lo exija la legislación aplicable o las autoridades competentes.

46. Si una Parte está obligada, en virtud de la legislación aplicable o de una orden emitida por una autoridad competente, a revelar Información Confidencial de otra Parte a las autoridades o a Terceros, la Parte obligada deberá notificar sin demora dicha revelación a la Parte afectada cuya Información Confidencial vaya a ser revelada, si así lo permite la legislación aplicable o la orden de la autoridad competente.

47. Las obligaciones de confidencialidad establecidas en las presentes Condiciones Generales subsistirán a la terminación del Convenio Constitutivo.

4.7. Derechos de propiedad intelectual

48. Los Derechos de Propiedad Intelectual de las Partes deberán ser respetados y protegidos en todo caso relación con el funcionamiento del Espacio de Datos. Especialmente y en todo caso deberán respetarse aquellos derechos morales existentes sobre los datos aportados al espacio.

49. La firma del Convenio Constitutivo y el intercambio de Datos dentro del Espacio permitirá de manera general la explotación del material derivado extraído de los datos que conforman el catálogo del espacio, excluyéndose la redistribución los datos a terceros.

50. Disposiciones más específicas en cuanto a la cesión de derechos de explotación existentes sobre los datos compartidos, o particularidades que afecten a los derechos de explotación del material derivado, se incluirán en las Condiciones de Uso específicas de los Conjuntos de Datos.

51. El Proveedor de Datos es responsable de garantizar que dispone de derechos suficientes para el suministro de Datos de conformidad con estas Condiciones Generales.

52. Las Partes tienen derecho a utilizar herramientas de software u otras formas de automatización de procesos, aprendizaje automático, o inteligencia artificial al procesar los Datos. De conformidad en su caso con las Condiciones específicas de Uso del Conjunto de Datos, las Partes tienen derecho a aprender de los Datos y a utilizar cualquier habilidad y experiencia profesional adquirida al procesar los Datos.

4.8. Protección de datos

53. Todos los datos personales tratados en el Espacio de Datos deberán ser tratados de conformidad con el RGPD y la LOPDGDD. A efectos del tratamiento de datos personales dentro del Espacio, cualquier Parte que revele o reciba datos se considerará, individualmente y por separado, responsable del tratamiento con arreglo a las disposiciones del RGPD.

54. Se delega la responsabilidad sobre el uso de datos personales para generar productos que se proporcionarán a través del Espacio de Datos al que desarrolle estos servicios.

55. También se supondrá que dichos proveedores/desarrolladores estarán tratando datos actuando como responsables del tratamiento, a menos que hayan celebrado un Contrato de Encargado de Tratamiento por escrito que establezca el objeto y la duración del tratamiento, la naturaleza y la finalidad del tratamiento, el tipo de Datos Personales y las categorías de interesados y las obligaciones y derechos del responsable y del encargado del tratamiento. Cuando dicho Contrato sea aplicable en general a determinados Conjuntos de Datos o servicios prestados en virtud del Convenio Constitutivo, deberá incluirse como Apéndice del Convenio Constitutivo.

56. Los órganos encargados de la gestión del espacio deberán impedir el tratamiento no autorizado e ilícito de Datos Personales mediante el empleo de medidas técnicas y organizativas apropiadas. Los Miembros del espacio deberán garantizar que las personas autorizadas a tratar Datos Personales se han comprometido a mantener la confidencialidad de dichos datos o están vinculadas por una obligación legal apropiada de confidencialidad.

57. Los Datos Personales que se compartan dentro del Espacio de Datos no podrán transferirse dentro de la Unión Europea y del Espacio Económico Europeo (EEE) sin que el proveedor de datos lo haya indicado expresamente en las Condiciones de Uso específicas de los Conjuntos de Datos. A su vez, este tipo de Datos Personales no podrán transferirse fuera de la UE y del EEE, sin autorización expresa del proveedor de datos, además de proporcionar las garantías suficientes de acuerdo con lo dispuesto en el Capítulo V del RGPD.

58. Los Miembros se comprometerán a prestar una asistencia razonable a otros Miembros cuando dicha asistencia sea necesaria para que la otra Parte cumpla sus obligaciones en virtud de la legislación aplicable en materia de protección de datos.

4.9. Terminación y Validez

59. El Convenio Constitutivo se celebrará por una duración indefinida indefinido y expirará cuando las Partes lo rescindan. Una vez rescindido dicho convenio los datos contenidos en el catálogo del espacio no podrán seguir siendo utilizados por los miembros y dejarán de estar disponibles en términos de negociación, salvo que se acuerde lo contrario por el Comité Directivo.

60. Una vez rescindido el Convenio Constitutivo se procederán a eliminar todos los accesos al Espacio de Datos invalidando los usuarios previamente otorgados a los miembros del espacio.

61. Cualquiera de las Partes podrá optar por rescindir el Convenio Constitutivo tal y como se define en el mismo. La rescisión deberá notificarse por escrito a todos los demás miembros. En caso de que haya más de dos objeciones por parte del conjunto de miembros, este convenio seguirá en vigor para los miembros objetores restantes tras la rescisión del mismo.

62. Cuando las Partes hayan acordado un proceso de modificación del Convenio Constitutivo distinto del consentimiento escrito de todos los Miembros, cualquier Miembro que se oponga por escrito a dicha modificación después de haber tenido conocimiento de la misma tendrá derecho a rescindir el Convenio Constitutivo notificándolo a las demás Partes. La rescisión se hará efectiva una vez que el Miembro objetante haya presentado la notificación mencionada a las demás Partes, tras lo cual la modificación entrará en vigor, a menos que los Miembros acordantes hayan convenido en una fecha posterior.

63. De producirse un de incumplimiento, de estas condiciones generales, o de llevarse a cabo un tratamiento ilícito de los datos, se procederá a restringir el acceso de dicho Miembro infractor al catálogo de datos del espacio.

64. En caso de que sólo haya dos Partes conformando el Convenio Constitutivo y una de ellas cometa un incumplimiento sustancial de las disposiciones del mismo o de estas Condiciones Generales, la otra Parte tendrá el derecho unilateral de rescindir el Convenio Constitutivo con efecto inmediato mediante notificación por escrito a la otra Parte.

65. En caso de que haya más de dos Partes en el Convenio Constitutivo y una de ellas cometa un incumplimiento grave de las disposiciones del mismo, el Comité Directivo tendrá derecho a rescindir el Convenio Constitutivo con la Parte infractora con efecto inmediato. La rescisión deberá notificarse por escrito a todas las Partes.

66. Si el incumplimiento puede subsanarse, la Parte o Partes no incumplidoras podrán decidir suspender el cumplimiento de sus obligaciones en virtud del Convenio Constitutivo hasta que la Parte incumplidora haya subsanado el incumplimiento.

67. De la misma forma, en caso de haber indicios suficientes de que una de las Partes ha cometido un incumplimiento grave, los miembros del espacio podrán tomar la decisión de retirarle el acceso al catálogo de datos del espacio preventivamente. De no alcanzarse un acuerdo entre las Partes, el Operador será quien tendrá la última palabra acerca de esta medida preventiva.

68. Cuando se ponga fin a la pertenencia de un Miembro al Espacio de Datos como consecuencia del incumplimiento material del Convenio Constitutivo por parte del Miembro, el derecho del Miembro infractor a utilizar los Datos finalizará en la fecha de la terminación. El Miembro infractor deberá dejar de utilizar los Datos y, a petición de cualquiera de las Partes, devolver o destruir de forma verificable los Datos y cualquier copia de Información Confidencial, incluidas sus copias. No obstante, el Miembro infractor tiene derecho a conservar los Datos según lo exija la legislación aplicable o las autoridades competentes, siempre que el Miembro infractor notifique al Proveedor de Datos dicha obligación de conservación de datos antes de la fecha de rescisión.

4.10. Responsabilidad

69. Las Partes solo serán responsables de los daños directos resultantes del incumplimiento de las disposiciones recogidas en el Convenio Constitutivo, tal y como se definen a continuación y, en su caso, en el mismo Convenio Constitutivo. Cualquier otra responsabilidad queda excluida, a menos que se defina específicamente lo contrario en el Convenio Constitutivo.

70. Las Partes no son responsables del lucro cesante ni de los daños debidos a una disminución o interrupción de la producción o del volumen de negocios, ni de otros daños indirectos o consecuentes.

71. Las Partes no serán responsables de las pérdidas, daños, costes, reclamaciones o gastos que se deriven de una avería mecánica o eléctrica o de un corte del suministro eléctrico o de cualquier otra causa ajena al control razonable de la Parte; y las Partes deberán compensar íntegramente cualquier daño resultante de un incumplimiento intencionado o por negligencia grave de las disposiciones establecidas en el Convenio Constitutivo.

72. Cada una de las Partes, por separado y no conjuntamente, será responsable de atender los derechos de los interesados en materia de indemnización, compensación y responsabilidad derivados de cualquier infracción de las obligaciones en materia de datos personales de conformidad con lo establecido en el artículo 82 del RGPD.

73. Específicamente, los miembros del Espacio, al utilizar la infraestructura tecnológica proporcionada por el Responsable Tecnológico, asume la responsabilidad conjunta en la implementación y mantenimiento de las medidas de seguridad requeridas para garantizar la protección de los datos y la integridad del sistema. El Responsable Tecnológico proporcionará un Espacio seguro conforme a los estándares establecidos, pero no será responsable por daños derivados de su uso inadecuado por parte de los miembros del Espacio. La responsabilidad por incidentes de seguridad será compartida según las acciones de cada parte.

4.11. Fuerza mayor

74. Ninguno de los Miembros será responsable de las lesiones o daños que se deriven de acontecimientos o circunstancias que no pudieran preverse razonablemente de antemano y que estén fuera de su control.

75. El Miembro que no pueda cumplir sus obligaciones debido a un acontecimiento de fuerza mayor deberá informar a las demás Partes de dicho impedimento sin demora injustificada. Estas causas de incumplimiento expirarán en el momento en que pase el acontecimiento de fuerza mayor. Esta cláusula está sujeta a una fecha límite prolongada: cuando se impida el cumplimiento durante un periodo continuado de ciento ochenta (180) días o más, las Partes tendrán derecho a resolver el Contrato Constitutivo según lo establecido en la cláusula 5.10.

4.12. Auditoría

76. Un Proveedor de Datos tendrá derecho a auditar a las Partes que procesen los datos puestos a disposición por el Proveedor de Datos, corriendo con los gastos, incluidos también los costes directos materiales y razonables de la parte auditada. El objetivo y el alcance de la auditoría se limitan a verificar el cumplimiento de los requisitos materiales del Convenio Constitutivo, de las condiciones de uso del conjunto de datos, y la legislación aplicable.

77. Las Partes son responsables de imponer a sus Miembros las mismas obligaciones de auditoría que se establecen en el presente documento y las Partes actuarán de buena fe para garantizar que los objetivos de los derechos de auditoría del Proveedor de Datos se materialicen con respecto a los subcontratistas de una Parte.

78. La Parte auditora deberá notificar la auditoría a la Parte auditada por escrito al menos treinta (30) días antes de la auditoría. La notificación escrita debe revelar el alcance y la duración de la auditoría e incluir una lista de los materiales solicitados y los derechos de acceso.

79. La Parte auditada tiene derecho a exigir que la auditoría sea realizada por un Tercero independiente mutuamente aceptable y/o certificado.

80. Las Partes están obligadas a conservar y facilitar a la Parte auditora y/o al Tercero auditor, a efectos de la auditoría, todos los registros y documentos, así como el acceso a todos los sistemas de datos y locales necesarios y a entrevistar al personal que sea de importancia significativa para la auditoría. Los registros y documentos así conservados deberán abarcar hasta la auditoría anterior o hasta la adhesión de la Parte auditada a la Red, si ésta fuera posterior.

81. La Parte auditora y/o el Tercero auditor sólo podrán solicitar los registros y documentos y el acceso a los sistemas de datos y a los locales, así como entrevistar al personal que sean de importancia significativa para la auditoría.

82. Todos los registros, documentos e información recopilados y revelados en el curso de la auditoría constituyen Información Confidencial. La Parte auditora y/o el Tercero auditor no podrán utilizar o revelar ilícitamente la Información Confidencial de la que hayan tenido conocimiento en el transcurso de la auditoría. La Parte auditada declara y garantiza que cualquier Tercero auditor, en su caso, cumple con las obligaciones de confidencialidad aplicables. La Parte auditada tiene derecho a exigir que la Parte auditora y/o el Tercero auditor o cualesquiera otras personas que participen en la auditoría firmen un acuerdo personal de confidencialidad, siempre que los términos y condiciones de dicho acuerdo de confidencialidad sean razonables.

83. Los resultados, conclusiones y recomendaciones de la auditoría deberán presentarse en un informe de auditoría. La Parte auditada tiene derecho a revisar el informe de auditoría de cualquier Tercero auditor por adelantado (y antes de que el Tercero auditor lo facilite al Proveedor o Proveedores de Datos pertinentes). La Parte auditada tiene derecho a exigir al Tercero auditor que introduzca en el informe de auditoría los cambios que considere razonables teniendo en cuenta la Información confidencial de la Parte auditada y los intereses comerciales del Proveedor de datos correspondiente en los Datos. La Parte auditada deberá responder al informe de

auditoría en un plazo de treinta (30) días. A falta de respuesta, se considerará que la Parte auditada ha aceptado el contenido del informe.

84. Si la Parte auditora considera justificadamente que la Parte auditada incumple sustancialmente las obligaciones que le impone el Convenio Constitutivo, podrá realizarse una auditoría adicional.

85. En caso de que la auditoría revele un incumplimiento material de las obligaciones impuestas en el Convenio Constitutivo o en las Condiciones de Uso del Conjunto de Datos aplicables, la Parte auditada será responsable de los gastos directos razonables y verificables en los que haya incurrido como resultado de la auditoría.

4.13. Legislación aplicable y resolución de litigios

86. Estas Condiciones Generales se regirá e interpretará según la legislación española, considerando los principios de derecho internacional privado, y la legislación europea aplicable.

87. Cualquier disputa, controversia o reclamación que surja de o en relación con los Datos compartidos en virtud de las presentes Condiciones Generales o que guarde relación con él, incluida cualquier cuestión relativa a su existencia, validez, interpretación, cumplimiento o terminación, será resuelta mediante arbitraje administrado por la Corte de Arbitraje de la Cámara Oficial de Comercio, Industria y Servicios de Madrid, de acuerdo con su Reglamento de Arbitraje vigente a la fecha de presentación de la solicitud de arbitraje. El número de árbitros será un único designado, la sede del arbitraje será Madrid (España) y el idioma del arbitraje será el español.

4.14. Otras disposiciones

88. Salvo acuerdo en contrario de las Partes, cualquier modificación del Convenio Constitutivo deberá hacerse por escrito y ser firmada por todas las Partes.

89. Ninguna Parte podrá ceder el Convenio Constitutivo, ni total ni parcialmente, sin el consentimiento por escrito de la otra Parte o Partes. No obstante, no será necesario el consentimiento cuando el Miembro sea una empresa que pertenezca al mismo grupo de empresas.

90. Si alguna disposición del Convenio Constitutivo o de las Condiciones de uso de data set aplicables es declarada inválida por un tribunal de justicia u otra autoridad competente, la invalidez de dicha disposición no afectará a la validez de las demás disposiciones establecidas en el Convenio constitutivo.

91. Cada una de las partes declara y garantiza que tiene existencia válida y goza reconocimiento jurídico conforme a las leyes aplicables del territorio de su constitución o registro. Asimismo, cada una de las Partes declara y garantiza que tiene todo el poder y la autoridad necesarios para ejecutar, entregar y cumplir sus obligaciones en virtud del Contrato Constitutivo y, en su caso, para obligar a sus filiales.

92. Las Partes tienen la intención de crear un Espacio de Datos sujeta a un único conjunto de condiciones contractuales, y nada de lo contenido en el Convenio Constitutivo podrá interpretarse en el sentido de que son Miembros o partes de una empresa conjunta o mandantes, agentes o empleados de las otras Partes. Ninguna de las Partes tendrá ningún derecho, poder o autoridad, expresa o implícita, para obligar a ninguna otra Parte.

93. Ningún retraso u omisión por cualquiera de las Partes en el ejercicio de cualquier derecho o facultad en virtud del presente documento menoscabará dicho derecho o facultad, ni podrá interpretarse como una renuncia al mismo. La renuncia por cualquiera de las Partes a cualquiera de los pactos que deben cumplir las otras Partes o cualquier incumplimiento de los mismos no podrá interpretarse como una renuncia a cualquier incumplimiento posterior de los mismos o de cualquier otro pacto.

4.15. Avisos

94. Todas las notificaciones relativas a las presentes Condiciones Generales y al Convenio Constitutivo deberán enviarse por escrito o en formato electrónico o entregarse en persona a la persona de contacto y/o dirección especificada por la Parte respectiva en el Convenio Constitutivo o en el Acuerdo de Adhesión aplicable.

95. Cada Parte será responsable de garantizar que sus datos de contacto estén actualizados.

96. Se considerará que las notificaciones han sido recibidas tres días después de su envío o salvo prueba en contrario.

4.16. Superviviencia

97. Las cláusulas contenidas en los siguientes apartados de estas condiciones generales 5.1, 5.2, 5.3, 5.4, 5.7, 5.8, 5.10, 5.13, 5.15 y 5.16 de estas Condiciones Generales sobrevivirán a la resolución del Convenio Constitutivo en su totalidad, junto con cualquier cláusula especifica que deba razonablemente sobrevivir a la resolución de acuerdo debido a sus ramificaciones.

98. Las cláusulas no previstas para su supervivencia serán las contenidas en los apartados 5.5, 5.9, 5.11 y 5.14.

99. Las cláusulas 5.12 y 5.6 de estas Condiciones Generales podrán subsistir acorde al periodo establecido en la normativa aplicable.

5. Modelo de gobernanza

5.1. Disposiciones generales

1. El Espacio de Datos se establecerá bajo un Convenio Constitutivo, del que partirán todas las demás normativas internas. Este convenio será debidamente aceptado y firmado por todos y cada uno de los miembros del espacio, ya sea durante su fundación o adhiriéndose con posterioridad.
2. El propósito de esta normativa será definir y documentar adecuadamente las obligaciones y responsabilidades esenciales que se asignarán a los órganos encargados de la gobernanza del Espacio de Datos. Al mismo tiempo, se expondrán debidamente los procedimientos y mandatos necesarios para gestionar el espacio, así como cualquier cambio en la gestión implementado durante el ciclo de vida del Espacio de Datos.
3. El Convenio Constitutivo incluirá una Lista de Miembros en la que figuren las Partes firmantes del Convenio Constitutivo y los datos de contacto de sus representantes. La Lista de Miembros deberá actualizarse en caso de adhesión de nuevas Partes y de cese de las Partes actuales, así como en caso de cualquier modificación de los datos de contacto.

5.2. Órganos y Comités designados

5.2.1. Comité directivo

4. El Comité Directivo es el órgano decisorio supremo del Espacio de Datos. La finalidad del Comité Directivo es facilitar la colaboración entre las Partes y organizar adecuadamente la administración del Espacio a nivel estratégico. El Comité Directivo también decide sobre asuntos que puedan tener un impacto financiero o de riesgo significativo para las Partes.

5.2.1.1. Funciones y Responsabilidades Principales de Gobernanza

5. El Comité Directivo será responsable de establecer la visión y misión estratégica del espacio de datos, siendo el responsable de que estas reflejen los intereses y necesidades de todos los miembros del espacio, así como cualquier parte interesada. Esta visión y misión serán recibirán revisiones periódicas para adaptarse a cambios en el entorno tecnológico y regulatorio.
6. El Comité Directivo será competente para revisar, modificar y aprobar toda política o procedimiento requerido para desplegar un adecuado marco de gobernanza destinado a regular el funcionamiento del Espacio de Datos. Esto incluirá toda política de seguridad, privacidad, acceso a datos y uso del Espacio de Datos, así como cualquiera que dentro del alcance se considere necesaria.
7. El Comité Directivo será el encargado de aprobar toda estrategia o plan de acción necesarios para perseguir las finalidades del espacio, supervisando su implementación y asegurándose de que se cumplan los plazos y se alcancen los objetivos establecidos en ellos. Esto incluirá la evaluación de informes periódicos y la realización de reuniones de seguimiento con los responsables de la implementación.
8. Se encuentra bajo responsabilidad del Comité Directivo la misión de coordinarse con otros subcomités y órganos encargados de la organización del espacio con objeto de asegurar una gestión integrada y coherente del Espacio de Datos. Esta coordinación incluirá la organización de reuniones conjuntas y la creación de grupos de trabajo interdisciplinares para abordar temas específicos cuando sea pertinente.
9. El Comité Directivo evaluará periódicamente el desempeño del Espacio de datos utilizando Indicadores clave de resultados (KPIs) y otros criterios de evaluación acordados y detallados previamente entre sus miembros. Los resultados de estas evaluaciones podrán ser empleadas, junto con una base justificada, para realizar ajustes en las estrategias y planes de acción

elaboradas por el comité, así como para informar a todos los miembros del Espacio de Datos sobre el progreso y los logros alcanzados.

5.2.1.2. Composición, Reuniones y Organización de Gobernanza

10. Cada miembro perteneciente del Espacio de Datos ostentará la obligación de nombrar a un representante para formar parte del Comité Directivo y defender sus tanto sus intereses como los del espacio en su conjunto. Los representantes que conformen el Comité Directivo serán seleccionados basándose en criterios de experiencia relevante y conocimientos técnicos.

11. Una vez conformado el Comité Directivo, sus miembros procederán a elegir un presidente y un secretario de entre sus miembros. Para el secretario le será incompatible ejercer simultáneamente las funciones atribuidas a su cargo justo a las inherentes al cargo de miembro del comité. El presidente podrá ejercer simultáneamente sus asignaciones como miembro del comité y las atribuidas al cargo de presidente.

12. En la selección de presidente y secretario se priorizará a aquellos candidatos que posean una trayectoria previa comprobada en proyectos de datos, innovación tecnológica y gobernanza. Además, se valorará la diversidad en términos de sector industrial, género y origen geográfico para asegurar una representación equitativa de todas las partes interesadas.

13. La elección de los cargos del Comité Directivo se realizará a través de un proceso transparente y participativo. Los candidatos serán nominados por los miembros del Espacio de Datos y evaluados por un comité de selección independiente, el cual revisará las nominaciones en base a los criterios preestablecidos. Posteriormente, se llevará a cabo una votación en la que cada miembro del Espacio de Datos tendrá derecho a un voto, debiendo obtener los candidatos una mayoría absoluta para ser elegidos, ostentando el representante del Operador del Espacio de Datos voto de calidad en la decisión.

14. Los cargos elegidos del Comité Directivo serán nombrados por un período inicial de tres años. Una vez concluido este periodo, se realizará una evaluación de su desempeño, que incluirá una revisión de sus contribuciones y logros durante su mandato. Los miembros podrán ser renovados por un período adicional de tres años mediante un proceso de votación similar al de su elección inicial.

15. Cada Representante debe esforzarse por estar presente o representado en todas las reuniones, pudiendo nombrar a un sustituto o apoderado para asistir con derecho a voto en cualquier sesión. Todos los representantes independientemente de su afiliación deberán participar en las reuniones demostrando espíritu de cooperación en la consecución de la misión del espacio.

16. El presidente tendrá la obligación de convocar una reunión ordinaria del Comité Directivo al menos una vez cada seis meses para evaluar la situación actual, así como convocar toda reunión extraordinaria en cualquier momento previa solicitud por escrito del secretario o de cualquier representante del Comité Directivo. Antes de programar una reunión extraordinaria, el presidente o el representante que haya solicitado la reunión extraordinaria deberá enviar un correo electrónico resumiendo el asunto prioritario en cuestión siempre que sea factible de cara al tiempo disponible.

17. Toda reunión del Comité Directivo podrá celebrarse o asistirse a través de videoconferencia o teleconferencia cuando el presidente lo considere necesario. El Comité Directivo deberá celebrar anualmente al menos dos reuniones presenciales coincidentes o no con las reuniones ordinarias anuales.

18. El secretario coordinará todos aquellos asuntos relacionados con las funciones del Comité Directivo. En particular, el secretario será directamente responsable de:

    a) Preparar las reuniones del Comité Directivo, proponiendo y ordenando los puntos del orden del día, redactar las actas de las reuniones y supervisar la aplicación de las decisiones tomadas por el Comité Directivo;

    b) Mantener actualizados y disponibles el Convenio constitutivo junto a todos sus apéndices y anexos;

c) Recopilar, presentar, revisar y verificar la coherencia de los documentos y las solicitudes necesarias en relación con las funciones del Comité Directivo;

d) Coordinar y administrar los asuntos cotidianos del Comité Directivo;

e) Transmitir con prontitud todo documento o notificación relacionada con el Espacio de Datos a cualquier Parte interesada en nombre del Comité Directivo;

f) Facilitar a las Partes que lo soliciten copias oficiales u originales de los documentos que obren en poder exclusivo del secretario, cuando dichas copias u originales sean necesarios para que las Partes puedan presentar sus reclamaciones o ejercitar sus derechos.

19. El secretario no está facultado para actuar o hacer declaraciones jurídicamente vinculantes en nombre de del Espacio de Datos o ninguno de sus miembros, a menos que se indique explícitamente lo contrario en el Acuerdo Constitutivo o que todas las Partes lo autoricen por escrito para una finalidad específica. El secretario no debe tratar de ampliar sus funciones más allá de las tareas especificadas en el presente Modelo de Gobernanza.

20. Una reunión se constituirá en quórum cuando estén presentes de manera presencial o telemática el presidente, o su vicepresidente, y al menos dos tercios de los representantes o sus apoderados. El Comité Directivo se esforzará por trabajar sobre una base común de consenso de manera general para la toma de decisiones durante las reuniones constituidas. Sin embargo, en caso necesario, el Comité Directivo votará las decisiones relativas al Espacio rigiéndose por mayoría absoluta. En caso de resultado similar de votos el presidente ostentará voto de calidad en las decisiones.

21. En caso de que el Comité Directivo no logre alcanzar un consenso claro de propuestas concretas, se adoptará como decisión del Comité Directivo una propuesta que cuente con el apoyo de al menos una mayoría de dos tercios de los Representantes presentes en la reunión.

22. Cualquier modificación del Convenio Constitutivo, o del Condiciones Generales o del presente Modelo de Gobernanza que tenga un impacto negativo material objetivo con respecto a cualquiera de los miembros del espacio deberá ser acordada por una mayoría de dos tercios de todos los representantes.

23. Las nuevas Partes pueden unirse al Espacio firmando un Acuerdo de Adhesión y su adhesión deberá ser aprobada por una mayoría simple del Comité Directivo.

24. Cuando la decisión del Comité Directivo de modificar el Convenio Constitutivo afecte materialmente a los derechos u obligaciones de una Parte que se oponga a dicha modificación, la Parte que se oponga tendrá derecho a rescindir el Convenio Constitutivo notificándolo por escrito al Comité Directivo dentro de los catorce días siguientes a la fecha en que la Parte que se oponga tenga conocimiento de la decisión del Comité Directivo. Esta rescisión se hará efectiva en un plazo de treinta días a partir de la fecha en que la Parte objetora haya presentado la notificación a las demás Partes.

5.2.2. Comités Técnicos y Funcionales

5.2.2.1. Funciones y Responsabilidades Principales

25. Los comités técnicos serán responsables de desarrollar y mantener estándares técnicos que aseguren la interoperabilidad y seguridad dentro del Espacio de Datos, más concretamente dentro de su infraestructura. Los estándares implementados serán revisados y actualizados periódicamente para adaptarse a los cambios producidos debido a nuevas tecnologías, modificaciones técnicas de la infraestructura y requisitos regulatorios durante el funcionamiento del Espacio de Datos.

26. Los comités revisarán y aprobarán las especificaciones técnicas necesarias para el funcionamiento del Espacio de Datos, asegurando que estas cumplan con los estándares establecidos como objetivo y las mejores prácticas de la industria.

27. Los comités serán responsables de evaluar y validar la interoperabilidad de los sistemas y tecnologías utilizadas en el Espacio de Datos, asegurando que todos los componentes se integren de manera eficiente y efectiva.

28. Los comités supervisarán la implementación en el Espacio de Datos de soluciones técnicas específicas aprobadas por el Comité Directivo, garantizando que estas se introduzcan en el espacio conforme a especificaciones concretas acordadas por dicho comité, y cumpliendo en todo caso con los requisitos de seguridad y desempeño necesarios para su adecuada inclusión en la infraestructura.

29. Los comités técnicos y funcionales se coordinarán estrechamente con el Comité Directivo y otros comités para asegurar una implementación coherente de políticas y soluciones técnicas. Esta coordinación incluirá su participación consultiva en reuniones del Comité Directivo, y la colaboración interdisciplinar en proyectos y planes específicos aprobados en el marco de los objetivos del espacio.

5.2.2.2. Composición, reuniones y organización

30. Los comités técnicos y funcionales estarán conformados necesariamente por cinco miembros: un representante del Comité Directivo, un representante del Operador del Espacio de Datos y dos miembros pertenecientes al proveedor tecnológico. Si el comité lo considera conveniente, podrá designar un número superior de miembros debido al alcance, la complejidad o la relevancia del proyecto que se asigne al comité técnico.

31. Los miembros serán formalmente designados por parte del Comité Directivo mediante un nombramiento expreso en base a su experiencia técnica, así como su conocimiento especializado en áreas determinadas como críticas para el Espacio de Datos, estándares de seguridad específicos, o tecnologías disruptivas.

32. Se priorizará a aquellos candidatos que posean una sólida formación académica y experiencia práctica en áreas como la interoperabilidad de sistemas, desarrollo de software, ciberseguridad y estándares tecnológicos relevantes para el espacio.

33. Los miembros del comité técnico podrán ser propuestos por los órganos a los que pertenezcan, y dichas propuestas deberán ser debidamente atendidas y evaluadas por el Comité Directivo. La designación final será aprobada por el Comité Directivo, basado en una evaluación exhaustiva de las cualificaciones y experiencia de los candidatos. Este proceso deberá basarse estrictamente en los principios de transparencia y equidad en la selección de miembros del comité.

34. Los miembros de los comités técnicos y funcionales serán nombrados por un período ajustado al proyecto asignado, con la posibilidad de renovación basada en el desempeño y las necesidades del espacio.

35. Se requerirá que los miembros posean una formación técnica avanzada, a determinar explícitamente caso por caso por parte del Comité Directivo. Tanto el Operador del Espacio de Datos como el proveedor tecnológico emitirán informes consultivos con recomendaciones en esta materia que deberán ser atendidos por el Comité Directivo.

5.2.3. Subcomités Especializados

5.2.3.1. Áreas de actuación

36. El Comité Directivo podrá proceder al nombramiento de diversos subcomités especializados cuando las necesidades del espacio así lo requieran, o para resolver cuestiones específicas. Los subcomités especializados abordarán áreas específicas de interés crítico para el Espacio de Datos, como la seguridad, la privacidad o la innovación. Cada subcomité tendrá asignadas sus propias áreas de enfoque basándose en las necesidades y prioridades del Espacio de Datos.

37. Cada subcomité definirá sus propios objetivos y tareas específicas en alineación con la visión y misión del Espacio de Datos, bajo la supervisión del Comité Directivo. Estos objetivos y tareas serán claros, medibles y alineados con las prioridades estratégicas del Espacio de Datos.

38. Los miembros y líderes de los subcomités serán seleccionados mediante un proceso de nominación y nombramiento similar al de los comités técnicos, careciendo de cualquier requerimiento mínimo de composición para favorecer de esta manera su flexibilidad. Los candidatos serán evaluados por sus conocimientos y experiencia en el área específica del subcomité. El nombramiento final será realizado en todo caso por el Comité Directivo.

39. Los miembros y líderes de los subcomités serán nombrados por un período ajustado a la persistencia de la necesidad de la constitución del propio subcomité comité, con la posibilidad de renovación basada en su desempeño y las necesidades del Espacio de Datos.

40. Los subcomités se coordinarán y comunicarán regularmente con otros comités, subcomités y órganos de gobernanza para asegurar la coherencia y efectividad en la implementación de sus mandatos. Esta coordinación incluirá la participación en reuniones conjuntas, la elaboración de informes periódicos y la colaboración en iniciativas transversales.

5.3. Procedimientos Específicos

5.3.1. Toma de Decisiones

5.3.1.1. Procedimientos de Votación

41. Los miembros de todos los comités y subcomités fomentarán la búsqueda de consenso en todas las decisiones alcanzadas dentro del cómputo de sus funciones. Cuando por diversos motivos no se alcance un consenso en la toma de decisiones, se procederá a una votación formal como último recurso. Se registrarán todos los intentos de consenso y los puntos de vista disidentes para mantener la transparencia en el proceso de toma de decisiones.

42. Los comités técnicos y subcomités adoptarán un proceso de votación estructurado para la toma de decisiones conflictivas en el desempeño de sus labores. Cada miembro tendrá derecho a un voto, y las decisiones se adoptarán por mayoría simple, a menos que se especifique lo contrario por parte del Comité Directivo durante su constitución. En casos de decisiones críticas o de alto impacto para el Espacio de Datos, será preceptiva la emisión de una consulta vinculante al Comité Directivo. Los procedimientos de votación serán documentados y registrados en las actas del comité técnico o subcomité.

43. Los desacuerdos se gestionarán mediante un proceso estructurado que incluirá la documentación de los puntos de vista de todas las partes, la programación de reuniones adicionales y, si es necesario, la intervención de un mediador neutral designado formalmente por el Operador del Espacio de Datos. Los votos disidentes se registrarán formalmente y se incluirán en las actas, asegurando su documentación y trazabilidad.

5.3.1.2. Documentación y Trasparencia

44. Todas las decisiones adoptadas por todos los comités serán debidamente documentadas de manera detallada en sus actas de reunión. Esto incluirá la descripción de la decisión alcanzada, el contexto en el que se alcanzó, los criterios utilizados para la toma de decisiones y el resultado de todas las votaciones llevadas a cabo. Las actas de las reuniones serán preparadas y distribuidas por el secretario a todos los miembros del comité para su adecuada revisión y aprobación.

45. Se implementarán mecanismos para garantizar la transparencia de todas las decisiones alcanzadas. Esto incluirá la publicación de actas y decisiones en una plataforma accesible a todos los miembros del Espacio de Datos, así como la creación de un repositorio centralizado de documentación clave para el espacio. Los miembros tendrán acceso a la información relevante y podrán solicitar aclaraciones o información adicional al Operador del Espacio de Datos cuando sea necesario.

46. Las decisiones serán comunicadas a todos los participantes de manera oportuna y clara. Se utilizarán canales de comunicación establecidos, como boletines informativos, correos

electrónicos oficiales y reuniones informativas. Además, se desarrollará un protocolo de comunicación que detalle los pasos y el cronograma para la divulgación de decisiones importantes.

5.3.2. Gestión de Cambios

5.3.2.1. Evaluación y Aprobación de Cambios dentro del Espacio

47. Cualquier miembro podrá motivar una propuesta de cambio sobre cualquier materia que afecte directa o indirectamente al Espacio de Datos. Las propuestas de cambio deberán ser debidamente presentadas por escrito y acompañadas de una justificación y motivación detalladas para su evaluación.

48. Estas propuestas de cambio serán revisadas inicialmente por el Operador del Espacio de Datos, que determinará su viabilidad, necesidad, proporcionalidad y alineamiento con los objetivos del Espacio de Datos mediante un informe preliminar comunicado al Comité Directivo, que será en última instancia el encargado de decidir sobre su implementación.

49. Todas las propuestas de cambio serán evaluadas en función de su impacto potencial, acorde a la información obtenida al tiempo de la presentación de la propuesta. Algunos de los criterios de evaluación tenidos en cuenta para determinar la viabilidad de una propuesta podrán ser: el alcance del cambio, los recursos necesarios, el tiempo de implementación, los riesgos asociados al cambio y los beneficios esperados para el espacio o sus miembros.

50. Un análisis de impacto especifico de la medida podrá ser realizado por el Operador del Espacio de Datos, incluyéndose este en su informe preliminar, asegurándose que todos los aspectos sean considerados debidamente antes de la aprobación.

51. Una vez analizadas, las propuestas de cambio serán sometidas a un proceso de aprobación individualizado que incluirá su evaluación final por parte del Comité Directivo. Los cambios clasificados como menores podrán ser aprobados por Comité Directivo mediante mayoría simple sin necesidad de haberse llevado a cabo análisis de impacto; siempre y cuando se cumplan los criterios de proporcionalidad y motivación preestablecidos. Por otro lado, los cambios calificados como significativos que pudieran afectar al espacio requerirán de una validación preliminar mediante informe y análisis de impacto positivo emitido por el Promotor del Espacio de Datos, seguido por una votación formal del Comité Directivo debiendo alcanzarse mayoría absoluta.

5.3.2.2. Implementación de Cambios

52. Una vez aprobada una propuesta de cambio, se procederá a nombres un subcomité encargado establecer un plan de implementación detallado y llevarlo a término dentro del espacio. Este plan incluirá entre otros contenidos: un cronograma de los plazos previstos para la implementación, los recursos asignados, los responsables de la implementación y los hitos clave. La comunicación del subcomité al Comité Directivo sobre el avance de los cambios será clara y concisa, asegurándose de que todos los miembros estén informados del avance de la implementación, los pasos a seguir o acciones a tomar de los que sean directamente responsables y el impacto esperado.

53. El subcomité encargado del cambio propondrá mecanismos de seguimiento para monitorear la implementación de los cambios. Esto podrá incluir, pero no estará limitado a, la revisión periódica del progreso, la identificación de obstáculos y la adopción de medidas correctivas cuando sea necesario. Al finalizar la implementación, el subcomité encargado del cambio será responsable de aportar una evaluación final para determinar el éxito del cambio y documentar las lecciones aprendidas, siendo asistido en esta tarea por el Operador del Espacio de Datos cuando sea necesario.

5.4. Resolución de Conflictos

5.4.1. Identificación y Reporte de Conflictos

54. Se implementarán mecanismos proactivos para la identificación temprana de conflictos dentro del Espacio de Datos. Estos mecanismos incluirán la realización de reuniones regulares de seguimiento, la llevanza de una documentación transparente, y la creación de canales de comunicación abiertos para que los miembros puedan expresar sus pretensiones de manera oportuna. Además, se promoverá una cultura ética y de colaboración para detectar y abordar posibles conflictos internos antes de su escalada.

55. Los miembros del Espacio de Datos deberán acudir a procedimientos protocolizados para el reporte formal de conflictos. Estos procedimientos incluirán la presentación de un informe detallado que recoja la naturaleza del conflicto, las partes involucradas y cualquier evidencia relevante para el proceso.

56. Posteriormente, el informe será sometido a un subcomité de revisión de conflictos, conformado por representantes designados por el Operador del Espacio de Datos y el Comité Directivo que no ostenten una incompatibilidad manifiesta por la que no puedan conocer del caso. Este subcomité evaluará la situación y determinará los pasos a seguir, garantizando la confidencialidad y la imparcialidad en la revisión de todos los conflictos investigados.

5.4.2. Procedimiento de Resolución de Conflictos

5.4.2.1. Mediación y Arbitraje

57. La mediación será el primer paso para la resolución de conflictos entre miembros del espacio. Se designará un mediador neutral por parte del Operador que deberá ser aceptado por todas las partes involucradas, para facilitar las discusiones y ayudar a alcanzar un acuerdo mutuo. El proceso de mediación incluirá sesiones de reunión, exploración de posibles soluciones y la redacción de un acuerdo de mediación si se alcanza un consenso. La mediación será voluntaria y no vinculante, buscando siempre resolver el conflicto de manera amistosa y colaborativa.

58. Si la mediación no resuelve el conflicto, se procederá al arbitraje. El arbitraje será conducido por un árbitro o panel de árbitros independientes, seleccionados conforme a los criterios de imparcialidad y competencia en la materia del conflicto. El proceso de arbitraje incluirá la presentación de pruebas, audiencias y la emisión de una decisión vinculante. Las decisiones del arbitraje serán finales y obligatorias para todas las partes involucradas.

5.4.2.2. Resolución Interna

59. Se establecerán procesos internos para la resolución de conflictos, entre los que se incluirán: la intervención de líderes de equipo o directivos, la utilización de métodos específicos de resolución de conflictos, o la creación de subcomités especializados destinados a resolver una causa de conflicto con relación a algún objetivo común del espacio. Estos métodos buscarán resolver los conflictos de manera rápida y efectiva, minimizando el impacto en la operación del Espacio de Datos.

60. Una vez alcanzada una solución, se seguirán protocolos específicos para su implementación. Estos protocolos incluirán la elaboración de planes de acción, así como la asignación de responsabilidades a las partes involucradas, la definición de plazos concretos y la monitorización del cumplimiento de las medidas acordadas mediante las distintas vías o procesos internos. Se asegurará que todas las partes involucradas comprendan y acepten las soluciones propuestas.

5.4.2.3. Documentación y Seguimiento

61. Todos los conflictos y sus resoluciones serán documentados de manera detallada y recopilados en el repositorio centralizado del Espacio de Datos, gestionado por el secretario del Comité Directivo. La documentación incluirá toda aquella documentación generada a lo largo del

proceso, como podrá ser: informes de conflicto, actas de sesiones, y acuerdos finales. Esta documentación será archivada y accesible para futuros análisis y referencias, asegurando la transparencia y la responsabilidad dentro del espacio y sus procesos.

62. Se implementarán mecanismos de seguimiento para asegurar que las resoluciones de los conflictos se cumplan efectivamente. Esto incluirá revisiones periódicas del estado de implementación de los planes de acción, y la evaluación del cumplimiento de los acuerdos alcanzados. Los resultados del seguimiento serán reportados al Comité Directivo y se tomarán las medidas correctivas relevantes de ser necesario.

5.5. Implementación y Evaluación del Espacio

5.5.1. Procedimientos de Incorporación de Nuevos Miembros

63. Los nuevos participantes deberán cumplir con criterios específicos para su incorporación al Espacio de Datos. Estos criterios incluirán la evaluación de sus aportes técnicos, su conformidad con las políticas de seguridad y privacidad, y su compromiso con los principios y objetivos del Espacio de Datos. Además, se requerirá que los nuevos participantes presenten referencias y demuestren su capacidad para contribuir positivamente al espacio, aportando está documentación al supervisor de solicitudes cuando sea necesario.

64. Las solicitudes de participación serán evaluadas mediante un proceso estructurado que incluirá la revisión de la documentación presentada por el potencial miembro, seguida por una entrevista con los solicitantes y la validación de sus capacidades técnicas y operativas. El Operador del Espacio de Datos, en colaboración con el supervisor de solicitudes, serán los responsables de llevar a cabo este proceso, y las decisiones reflejadas en los informes de admisión o denegación se tomarán basándose en criterios objetivos y transparentes. Las solicitudes independientemente de su resultado serán comunicadas formalmente a los nuevos participantes, y en caso de admisión también se comunicarán los próximos pasos requeridos para su incorporación.

65. El Operador desarrollará planes de incorporación y formación para los nuevos participantes, asegurando su integración efectiva en el Espacio de Datos. Estos planes incluirán sesiones de orientación sobre las políticas y procedimientos del Espacio de Datos, formación técnica sobre las herramientas y plataformas utilizadas, y la asignación de puntos de contacto para facilitar su adaptación al espacio. La formación continua será promovida para mantener a todos los participantes actualizados sobre las mejores prácticas, nuevos desarrollos y estándares implementados dentro del Espacio de Datos.

5.5.2. Revisión y Actualización del Modelo de Gobernanza

66. Se establecerán procedimientos para la revisión periódica de este modelo de gobernanza, asegurando que se mantenga relevante y efectivo. Estas revisiones se realizarán al menos cada dos años, o con mayor frecuencia si se producen cambios significativos en el entorno operativo o regulatorio. Un subcomité de revisión funcional será responsable de conducir estas revisiones y de proponer modificaciones necesarias.

67. Las actualizaciones aprobadas de este modelo de gobernanza se basarán en criterios claros y justificados, incluyendo la evaluación de su efectividad, la identificación de áreas de mejora que cubren o la incorporación de mejores prácticas emergentes. El proceso de actualización incluirá consultas de todos los miembros y partes involucradas, la redacción detallada de la propuesta de cambio, la emisión de un informe consultivo por parte del Operador de la y la aprobación final por parte del Comité Directivo de dicha propuesta. Se deberá garantizar por el secretario del Comité Directivo que todas las actualizaciones sean comunicadas claramente a los miembros y se implementen de manera ordenada.

68. Deberá fomentarse la participación activa de todos los interesados en el proceso de revisión y actualización del modelo de gobernanza. Esto incluirá la realización de encuestas, procesos consultivos y sesiones de retroalimentación para recoger opiniones y sugerencias en relación

con los cambios propuestos. La participación inclusiva asegurará que el modelo de gobernanza refleje las necesidades y expectativas de todos los miembros del Espacio de Datos, sin alejarse de su misión y principios rectores.

6. Condiciones Específicas de Uso del Conjunto de Datos

6.1. Partes

[Proveedor del Conjunto de Datos]

Por una parte, _____ con CIF _____ en adelante denominado como "PROVEEDOR DEL CONJUNTO DE DATOS", con domicilio social en _____, representado en este acto por D./Dña._____ DNI _____ , en su calidad de _____, con poderes suficientes para obligar al mismo.

[Parte Adherente]

Por una parte, _____ con CIF _____ en adelante denominado como "PARTE ADHERENTE", con domicilio social en _____, representado en este acto por D./Dña._____ DNI _____ , en su calidad de _____, con poderes suficientes para obligar al mismo.

[...]

6.2. Manifiestan

Que las partes manifiestan su voluntad de vincularse en el marco del presente Acuerdo al Espacio de Datos denominada INESDATA – **[Incluir Referencia del Demostrador]**, el cual estará sujeto a las cláusulas estipuladas en el presente contrato, así como a la normativa aplicable en el territorio español y el espacio europeo.

Asimismo, las partes aceptan que el objeto del presente acuerdo implica el acceso, uso y procesamiento de un conjunto de datos proporcionado por el Proveedor. Además, las partes se reconocen expresa y recíprocamente capacidad legal suficiente para constituir el presente Acuerdo, y por ello acuerdan las siguientes clausulas.

6.3. Clausulas

6.3.1. Descripción del conjunto de datos

69. El Dataset objeto de estas condiciones específicas, así como su ubicación y método de distribución, se describen como: **[Incluir descripción]**

70. El Proveedor de Datos se asegurará de que posee todos los derechos y autorizaciones necesarios para poner el Dataset objeto de estas condiciones específicas a disposición de las otras Partes para su uso de conformidad con los términos y condiciones aplicables.

6.3.2. Antecedentes

71. El propósito de estas Condiciones Específicas de Uso del Conjunto de Datos es definir los datos que el proveedor de datos pone a disposición a través del Espacio de Datos Federado y establecer los términos y condiciones específicas para el uso de dicho Dataset.

6.3.3. Aplicabilidad y ámbito de aplicación

72. Las presentes Condiciones Específicas de Uso del Conjunto de Datos se aplican al Conjunto o los Conjuntos de Datos proporcionados por el Proveedor de Datos en virtud del presente acuerdo.

73. Al utilizar dichos Datos, el Usuario se compromete a utilizarlos de conformidad con las presentes Condiciones Específicas de Uso del Conjunto de Datos.

6.3.4. Finalidad del uso de los datos

74. Con sujeción a las presentes Condiciones Específicas de Uso del Conjunto de Datos, el Proveedor de datos concede al Usuario un derecho no exclusivo a utilizar los Datos para los siguientes fines:

- **[Incluir finalidades]**
- **[*]**

75. **[Determinar si el usuario tiene derecho a aprender de los Datos y a utilizar cualquier habilidad y experiencia profesional adquirida al tratar los Datos]**

6.3.5. Restricciones al tratamiento y a la redistribución de datos

76. Los datos no pueden ser procesados en las siguientes situaciones:

- **[Describir cualquier restricción específica que se aplica al tratamiento o a la redistribución del Dataset objeto de estas condiciones específicas]**
- **[*]**

6.3.6. Cese del Suministro de datos

77. El Proveedor de Datos podrá dejar de suministrar los Datos notificándolo a las demás Partes del Espacio de Datos al menos **[*]** días antes de que finalice el suministro de los Datos en cuestión.

6.3.7. Material Derivado

78. No se considerará material derivado y seguirán aplicándose en su caso las normas relativas al uso de datos:

- Los Datos pueden ser fácilmente convertidos, revertidos o implícitos a partir del Material Derivado para recrear los Datos;
- El Material Derivado puede utilizarse como sustituto de los Datos;
- Los proveedores individuales de los datos pueden identificarse a partir del material derivado;
- El Material Derivado contenga cualquier Información Confidencial del Proveedor de Datos;
- **[*]**
- **[*]**
- **…**

79. No se considerará material derivado y permanecerá bajo las restricciones establecidas anteriormente para los datos en los casos en que un conjunto de datos se modifique sólo en aspectos menores y se utilice para sustituir al conjunto de datos original.

6.3.8. Restricciones de uso y redistribución del material derivado

80. El material derivado no puede utilizarse para:

- **[Incluir restricciones]**
- **[*]**

6.3.9. Tarifas y condiciones de pago

81. El uso del Dataset objeto de estas condiciones específicas está sujeto a las siguientes tasas: **[Incluir tasas aplicables]**, de carácter justo, acorde al Data Governance Act, la Ley 8/1989 de Tasas y Precios Públicos, y en última instancia alineado con el criterio recogido en la normativa europea de compensación justa por poner a disposición datos, incrementado por un margen razonable de beneficio.

82. Tal compensación cubrirá los costes técnicos y organizativos soportados a raíz del suministro de datos para su reutilización y tratamiento, limitada a los costes marginales en que se incurra para su puesta a disposición, difusión, y protección. Esta compensación puede ser incrementada por un margen de beneficio razonable de la inversión, incluidos en su caso, los costes de anonimización, seudonimización, agregación y de adaptación técnica, más un margen razonable.

6.3.10. Informes

83. El uso del Dataset objeto de estas condiciones específicas está sujeto a las siguientes obligaciones específicas de información:

- **[Describa aquí, cuando proceda, cualquier obligación específica de notificación que se aplique al uso del conjunto o conjuntos de datos]**
- **[*]**

6.3.11. Auditoría

84. El uso del Dataset objeto de estas condiciones específicas está sujeto a las siguientes obligaciones de auditoría:

- **[Incluir obligaciones y condiciones específicas de auditoría]**
- **[*]**

6.3.12. Seguridad de los datos

85. El uso del Dataset objeto de estas condiciones específicas está sujeto a la siguiente obligación específica de seguridad de datos:

- **[Describir cualquier requisito específico de seguridad de los datos para el Dataset objeto de estas condiciones específicas]**
- **[*]**

6.3.13. Información confidencial

86. Las Partes reconocen que el Conjunto de Datos incluye Información Confidencial y que su uso y procesamiento está sujeto a:

- **[Cuando el Dataset objeto de estas condiciones específicas incluyan información confidencial, se deben detallar los requisitos específicos que**

considere necesarios para que los datos estén disponibles en el Espacio de Datos]

6.3.14. Protección de datos

[Si el Dataset objeto de estas condiciones específicas, incluye datos de carácter personal, se debe considerar, como mínimo, la inclusión de las siguientes cláusulas de Protección de Datos. Sin embargo, el Proveedor de Datos tiene la posibilidad de definir las especificaciones que considere, siempre y cuando estén acorde a la normativa vigente]

87. Todos los datos personales tratados en el Espacio de Datos deberán ser tratados de conformidad con el RGPD y la LOPDGDD. A efectos del tratamiento de datos personales dentro del Espacio, cualquier Parte que revele o reciba datos se considerará, individualmente y por separado, responsable del tratamiento con arreglo a las disposiciones del RGPD.

88. Se delega la responsabilidad sobre el uso de datos personales para generar productos que se proporcionarán a través del Espacio de Datos al que desarrolle estos servicios.

89. También se supondrá que dichos proveedores/desarrolladores estarán tratando datos actuando como responsables del tratamiento, a menos que hayan celebrado un Contrato de Encargado de Tratamiento por escrito que establezca el objeto y la duración del tratamiento, la naturaleza y la finalidad del tratamiento, el tipo de Datos Personales y las categorías de interesados y las obligaciones y derechos del responsable y del encargado del tratamiento. Cuando dicho Contrato sea aplicable en general a determinados Conjuntos de Datos o servicios prestados, deberá incluirse como Apéndice de este Acuerdo.

90. Los órganos encargados de la gestión del espacio deberán impedir el tratamiento no autorizado e ilícito de Datos Personales mediante el empleo de medidas técnicas y organizativas apropiadas. Los Miembros del espacio deberán garantizar que las personas autorizadas a tratar Datos Personales se han comprometido a mantener la confidencialidad de dichos datos o están vinculadas por una obligación legal apropiada de confidencialidad.

91. Los Datos Personales que se compartan dentro del Espacio de Datos no podrán transferirse dentro de la Unión Europea y del Espacio Económico Europeo (EEE). A su vez, este tipo de Datos Personales no podrán transferirse fuera de la UE y del EEE, sin autorización expresa del proveedor de datos, además de proporcionar las garantías suficientes de acuerdo con lo dispuesto en el Capítulo V del RGPD.

92. Los Miembros se comprometerán a prestar una asistencia razonable a otros Miembros cuando dicha asistencia sea necesaria para que la otra Parte cumpla sus obligaciones en virtud de la legislación aplicable en materia de protección de datos.

6.3.15. Derechos de propiedad intelectual

[Cuando el Proveedor de Datos considere necesario establecer excepciones al enfoque por defecto de los Derechos de Propiedad Intelectual estipulados en las Condiciones Generales, deberán describirse en el presente Contrato las excepciones específicas del Conjunto de Datos. Sin embargo, para gestionar eficazmente los Derechos de Propiedad Intelectual, los Miembros deberían considerar si sería factible definir el enfoque por defecto de los Derechos de Propiedad Intelectual para el Espacio estableciendo una plantilla estándar para las Condiciones de Uso del Conjunto de Datos que se apliquen a la Red específica]

[Se incluirán en estas Condiciones de Uso específicas de los Conjuntos de Datos disposiciones más específicas en cuanto a la cesión de derechos de explotación existentes sobre los datos

compartidos, o particularidades que afecten a los derechos de explotación del material derivado]

93. Los Derechos de Propiedad Intelectual de las Partes deberán ser respetados y protegidos en todo caso relación con el funcionamiento del Espacio de Datos. Especialmente y en todo caso deberán respetarse aquellos derechos morales existentes sobre los datos aportados al espacio.

94. La firma del presente Acuerdo y el intercambio de Datos dentro del Espacio permitirá de manera general la explotación del material derivado extraído de los datos que conforman el catálogo del espacio, excluyéndose la redistribución los datos a terceros.

95. El Proveedor de Datos es responsable de garantizar que dispone de derechos suficientes para el suministro de Datos de conformidad con las Condiciones Generales.

96. Las Partes tienen derecho a utilizar herramientas de software u otras formas de automatización de procesos, aprendizaje automático, o inteligencia artificial al procesar los Datos.

97. Las Partes tienen derecho a aprender de los Datos y a utilizar cualquier habilidad y experiencia profesional adquirida al procesar los Datos.

6.3.16. Exención y limitación de responsabilidad

[Ejemplo: Salvo que se exprese lo contrario en las presentes Condiciones, el Proveedor de datos ofrece los datos "tal cual" y "según disponibilidad", sin garantía de ningún tipo. El riesgo inherente a la idoneidad de los datos para los fines del Usuario recae exclusivamente en éste. No obstante lo anterior, esto no limita la responsabilidad del Proveedor de Datos en virtud de las Condiciones Generales]

[Las Condiciones Generales establece las disposiciones aplicables a la limitación de responsabilidad. Cualquier derogación específica de Dataset en materia de responsabilidad deberá definirse en la misma. Tenga en cuenta, cuando proceda, que los Miembros pueden haber establecido excepciones a las cláusulas de responsabilidad de las Condiciones Generales, en cuyo caso deberá hacerse referencia a dichas cláusulas de responsabilidad en el presente documento para mayor claridad.]

6.3.17. Entrada en vigor y aplicación

98. Este derecho de uso de los Datos entrará en vigor una vez firmado el presente Acuerdo y cuando el usuario acceda a los Datos, y se aplicará hasta que el usuario deje de tratarlos. / **[Aplicar un plazo cuando proceda]**

6.3.18. Abstenerse de compartir datos y modificaciones

99. El Proveedor de Datos podrá abstenerse de compartir Datos dentro del Espacio y modificar los presentes términos y condiciones (incluidos, entre otros, el contenido o la calidad del Conjunto de Datos) en cualquier momento, notificando dicha modificación por escrito a todos los demás Miembros del Espacio. El suministro de Datos finalizará o los términos modificados entrarán en vigor en un plazo de **[*]** días después de que el Proveedor de Datos haya notificado a los demás Miembros la abstención de compartir o las modificaciones realizadas en estos términos y condiciones, pero las modificaciones no se aplicarán a ningún Dato recibido por los Usuarios antes de la entrada en vigor de las modificaciones.

6.3.19. Otros términos

100. Se reconoce que estas condiciones específicas no restringirán en modo alguno los derechos de los usuarios basados en la legislación obligatoria aplicable. En caso de discrepancia entre dicha legislación imperativa y las presentes condiciones, prevalecerá la legislación imperativa.

6.3.20. Legislación aplicable y resolución de litigios

101. Estas Condiciones Específicas se regirá e interpretará según la legislación española, considerando los principios de derecho internacional privado, y la legislación europea aplicable.

102. Cualquier disputa, controversia o reclamación que surja de o en relación con los Datos compartidos en virtud de las presentes Condiciones o que guarde relación con él, incluida cualquier cuestión relativa a su existencia, validez, interpretación, cumplimiento o terminación, será resuelta mediante arbitraje administrado por la Corte de Arbitraje de la Cámara Oficial de Comercio, Industria y Servicios de Madrid, de acuerdo con su Reglamento de Arbitraje vigente a la fecha de presentación de la solicitud de arbitraje. El número de árbitros será un único designado, la sede del arbitraje será Madrid (España) y el idioma del arbitraje será el español.