

**PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HA DE REGIR EN EL CONTRATO DE LOS SERVICIOS DE CONSULTORÍA Y ASISTENCIA TÉCNICA PARA LA TRANSFORMACIÓN GLOBAL DE LOS PROCESOS DE GESTIÓN PARA LA FUNDACIÓN PARA EL CONOCIMIENTO MADRIMASD A ADJUDICAR POR PROCEDIMIENTO ABIERTO SIMPLIFICADO CON PLURALIDAD DE CRITERIOS**

---

**EXPEDIENTE nº S\_2025\_017**

**1. OBJETO DEL CONTRATO.**

La Fundación para el Conocimiento Madrimasd (en adelante Fundación madri+d) es una organización sin ánimo de lucro perteneciente al sector público de la Comunidad de Madrid (sector público institucional).

La Fundación tiene carácter de organismo de investigación público de la Comunidad de Madrid y se rige por el ordenamiento civil, jurídico-administrativo y tributario que, por razones de especialidad y vigencia, le sea aplicable, en cada momento, por sus Estatutos y por normas y disposiciones que, en interpretación y desarrollo de los mismos establezca su Patronato.

La Fundación madri+d tiene, entre sus fines, contribuir al aprovechamiento social de la ciencia y la tecnología, el apoyo al desarrollo del conocimiento científico y tecnológico y a su gestión, en la nueva sociedad del conocimiento mediante el fomento y la promoción de la educación superior, la ciencia, la tecnología y la innovación.

El objeto del presente contrato es la provisión de una plataforma tecnológica en la nube y los servicios profesionales asociados para la modernización de la gestión documental, la unificación del dato y la explotación analítica avanzada de la Fundación madri+d.

Este proyecto se concibe como el pilar fundamental de una estrategia de transformación digital que busca superar las limitaciones de los actuales procesos manuales y silos de información. La finalidad es dotar a la Fundación de una capacidad tecnológica que permita la toma de decisiones basada en la evidencia, la automatización de tareas de bajo valor añadido y el cumplimiento proactivo de las normativas de seguridad y privacidad.

La gestión documental de la Fundación para el Conocimiento Madri+d debe evolucionar para ser un pilar fundamental en la eficiencia operativa, la toma de decisiones informada y la seguridad de la información de la Fundación.

**Objetivos:**

- Unificación.
- Digitalización Avanzada.
- Seguridad Proactiva.
- Escalabilidad.
- Optimización Continua.

#### **Beneficios esperados:**

- Impulso a la Eficiencia Operativa
- Mejora en la Toma de Decisiones Informadas: :
- Fortalecimiento de la Seguridad y el Cumplimiento
- Fomento de la Adaptación y Evolución Tecnológica
- Refuerzo de la Cultura de Calidad y Mejora Continua

#### **1.1. Alcance del Proyecto**

Dada la complejidad y criticidad de la transformación, el alcance técnico se estructura en una hoja de ruta progresiva. El presente pliego tiene como objetivo la ejecución de la **Fase I: Cimientos e Inteligencia Táctica**, que comprende:

- 1. Despliegue de Infraestructura Base Segura (Landing Zone):** Provisión y configuración de un entorno en la nube pública de hiperescala, diseñado bajo principios de "Seguridad por Diseño" y "Mínimo Privilegio". Deberá incluir la gestión centralizada de identidades, segmentación de redes y controles de cumplimiento automatizados.
- 2. Implementación de un Almacén de Datos Corporativo (Data Warehouse):** Construcción de un repositorio analítico centralizado capaz de ingerir, historificar y gobernar datos estructurados y no estructurados. Se requiere una metodología de modelado que garantice la **auditableidad histórica** del dato (separando el dato crudo inmutable de la lógica de negocio).
- 3. Solución de Inteligencia Artificial para Dominios Prioritarios:** Desarrollo de capacidades de búsqueda, extracción y explotación de información mediante IA Generativa para los departamentos de **Proyectos Europeos** y de **Administración y Financiero**. La solución deberá permitir la carga y procesamiento seguro de documentación administrativa y técnica para su consulta en lenguaje natural.
- 4. Modelo de Gobierno y Operación:** Definición de los roles, políticas y procedimientos necesarios para la gestión segura del ciclo de vida del dato y la infraestructura. Queda fuera del alcance de esta fase inicial la integración nativa bidireccional automatizada con sistemas de gestión documental corporativos (tipo SharePoint o similar) o ERPs, la cual se abordará en fases subsiguientes una vez consolidada la plataforma de datos.

#### **1.2. Justificación de la Necesidad**

La situación actual (*As-Is*) de la Fundación, caracterizada por la dispersión de la información en múltiples formatos y repositorios no integrados, plantea riesgos operativos y de seguridad que este contrato pretende mitigar:

- **Eficiencia:** Reducción de tiempos dedicados a la búsqueda y consolidación manual de información.
- **Seguridad:** Eliminación de riesgos asociados al almacenamiento local y falta de copias de seguridad unificadas.
- **Conocimiento:** Transformación de la documentación pasiva en activos de conocimiento activo mediante tecnologías semánticas.

## 2. CONTEXTO ESTRATÉGICO Y VISIÓN DE TRANSFORMACIÓN

### 2.1 Propósito del Documento

El presente documento tiene como propósito definir el marco técnico, funcional y operativo para la contratación de la **Fase I del Proyecto de Transformación Global** de la Fundación Madri+d.

Más allá de una simple especificación de requisitos, este pliego establece los **principios rectores** que guiarán la evolución tecnológica de la entidad durante los próximos años. Su objetivo es garantizar que las inversiones realizadas en esta fase inicial —centradas en la infraestructura base (Landing Zone), el gobierno del dato y los pilotos de Inteligencia Artificial— no sean soluciones aisladas, sino los cimientos de una plataforma institucional robusta, escalable y segura por diseño.

Se busca transicionar desde un modelo de seguridad perimetral tradicional, dependiente de barreras físicas de red, hacia un modelo de **Seguridad de Confianza Cero (Zero Trust)** nativo en la nube, donde la identidad y el contexto son los nuevos perímetros de control.

### 2.2 Visión Estratégica para la Gestión: Hacia un Sistema Nervioso Digital

La visión estratégica de la Fundación es evolucionar sus sistemas de gestión para que actúen como un verdadero "**Sistema Nervioso Digital**", capaz de conectar silos de información dispares, procesar datos en tiempo real y proteger los activos críticos con un enfoque proactivo e inteligente.

Para materializar esta visión, la arquitectura tecnológica propuesta deberá superar los enfoques de seguridad reactivos tradicionales. No basta con detectar incidentes después de que ocurran; la plataforma debe poseer capacidades de "**Inmunidad Digital**". Esto implica:

1. **Prevención por Defecto:** La capacidad de impedir configuraciones inseguras mediante políticas de software inmutables, antes incluso de que se desplieguen los recursos.

2. **Detección Inteligente sin Agentes:** El uso de inteligencia de amenazas global y actualizada en tiempo real para identificar patrones de ataque sofisticados (como campañas de phishing o malware de día cero) correlacionando la actividad interna con bases de datos de amenazas globales, sin la necesidad de gestionar complejos agentes de seguridad en cada servidor.

3. **Aislamiento Lógico de Servicios:** La implementación de perímetros de seguridad definidos por software alrededor de los servicios de datos (Service Perimeters), que impidan la exfiltración de información incluso en el caso de credenciales comprometidas, independientemente de la ubicación de la red.

Asimismo, en el ámbito de la Inteligencia Artificial, la visión es transitar de modelos genéricos a modelos "**Anclados en la Verdad**" (Grounded AI). Los sistemas de IA de la Fundación no deben "alucinar" ni inventar datos; deben actuar como asistentes expertos

que basan cada respuesta y cada decisión en la documentación oficial y los datos verificados de la entidad, garantizando la trazabilidad y la confianza en cada interacción.

### 2.3 Alineación con los Objetivos de la Fundación:

La transformación tecnológica descrita en este pliego no es un fin en sí misma, sino un instrumento crítico para la consecución de los fines fundacionales de Madri+d. La nueva plataforma actuará como habilitador directo de los cuatro objetivos estratégicos de la institución:

**1. Calidad y Mejora Continua:** La transición desde procesos manuales hacia una organización digitalizada y automatizada permitirá alcanzar la excelencia operativa. Esto impactará directamente en la **calidad del Sistema de Educación Superior**, garantizando procesos de evaluación y acreditación más ágiles, rigurosos y transparentes, optimizando el uso de los recursos públicos mediante la reducción de cargas administrativas.

**2. Promoción de Madrid como Centro de Excelencia:** Al implementar una infraestructura de vanguardia basada en la gestión inteligente de la información, la Fundación se posicionará como un referente tecnológico. Esto reforzará la imagen de la **Comunidad de Madrid como un nodo internacional de excelencia** en educación superior, ciencia, tecnología e innovación, demostrando que la gestión pública regional está al nivel de los estándares tecnológicos más avanzados.

**3. Fomento de la Cultura Científica y la Innovación:** La unificación del dato y el despliegue de capacidades de Inteligencia Artificial (IA) no solo mejoran la gestión, sino que **fomentan activamente la cultura de la innovación** interna. La plataforma permitirá a los equipos de la Fundación identificar nuevas tendencias, conectar investigadores y empresas, y gestionar el conocimiento científico de manera proactiva, actuando como un verdadero motor de innovación para la región.

**4. Asesoramiento Estratégico en Innovación:** Una gestión robusta y gobernada del dato transformará la capacidad de análisis de la Fundación. Al disponer de información veraz, consolidada y accesible en tiempo real, la Fundación estará mejor equipada para proporcionar **recomendaciones y asesoramiento estratégico** de alto valor a las administraciones y agentes del sistema, basando sus decisiones en evidencias de datos sólidos y auditables.

### 3. PRINCIPIOS DE ARQUITECTURA PARA EL DISEÑO FUTURO

Los principios que se detallan a continuación constituyen las directrices fundamentales que regirán el diseño, despliegue y operación de la nueva plataforma. La solución técnica propuesta deberá demostrar su adhesión estricta a estos principios para garantizar la sostenibilidad, la auditabilidad y la seguridad de la inversión de la Fundación a largo plazo.

### 3.1 Orientación al Valor y Modularidad

La arquitectura no debe ser monolítica, sino modular y orientada a la entrega continua de valor:

- **Despliegue Incremental:** La arquitectura debe estar diseñada para permitir la implementación de casos de uso funcionales en ciclos cortos, evitando enfoques de "todo o nada".
- **Reusabilidad de Activos:** Los componentes de infraestructura y datos (tuberías de ingesta, reglas de calidad, modelos analíticos) deben diseñarse como activos reutilizables, de modo que la implementación de nuevos dominios de negocio en el futuro aproveche los cimientos existentes sin duplicar esfuerzos.

### 3.2 Principios de Datos: Auditabilidad y Desacoplamiento

Para garantizar la integridad histórica y la flexibilidad ante cambios en los sistemas origen, la arquitectura de datos deberá regirse por:

- **Separación de Historia e Interpretación:** Se exige un desacoplamiento estricto entre el almacenamiento de los datos tal cual se reciben de los sistemas origen (capa de datos crudos, inmutables y auditables) y la capa donde se aplican las reglas de transformación de negocio. Garantizando que un cambio en una regla de gestión nunca altere ni destruya la evidencia histórica original del dato.
- **Identificación Determinista y Distribuida:** Para evitar cuellos de botella y dependencias de sistemas centrales de secuenciación, la identificación única de los registros debe basarse en algoritmos deterministas y no en secuencias numéricas de base de datos. Es imprescindible que permita la integración paralela masiva de múltiples fuentes heterogéneas.
- **Integridad Referencial Sistémica:** La plataforma debe implementar mecanismos automáticos para gestionar la ausencia de datos o llegadas tardías, utilizando registros de sistema estandarizados que permitan realizar consultas de alto rendimiento sin recurrir a lógica compleja de gestión de nulos en tiempo de lectura.
- **Capa Semántica Universal ("The Knowledge Engine"):** La arquitectura no debe exponer directamente las tablas físicas a los usuarios o agentes de IA. Se requiere una capacidad de modelado semántico centralizado que define las métricas de negocio (ej. "Gasto Ejecutado", "Ratio de Calidad") una única vez. Esta capa debe actuar como un traductor universal, permitiendo que tanto los analistas humanos (Dashboards) como los Agentes de IA consuman las mismas definiciones de negocio, garantizando la coherencia absoluta de los resultados independientemente del canal de acceso.

### 3.3 Seguridad y Privacidad por Diseño

La seguridad no será un perímetro añadido a posteriori, sino una propiedad intrínseca de la configuración de la plataforma:

- **Modelo de Confianza Cero:** El diseño no debe confiar implícitamente en ningún usuario o servicio basándose únicamente en su ubicación de red. Cada solicitud de acceso a datos debe ser autenticada, autorizada y cifrada, evaluando la identidad y el contexto de seguridad del dispositivo en tiempo real.
- **Defensa en Profundidad Lógica:** La protección de los datos no debe depender exclusivamente de cortafuegos de red tradicionales. Se requiere la capacidad de establecer perímetros de seguridad lógicos a nivel de servicio, que impidan la transferencia de datos no autorizada incluso si las credenciales de un usuario legítimo fueran comprometidas.
- **Soberanía Operativa Configurable:** La plataforma debe permitir restringir, mediante políticas de software inmutables a nivel organizativo, las regiones físicas exactas donde se permite el almacenamiento y procesamiento de los datos, asegurando el cumplimiento normativo sin depender de la intervención humana manual.

### 3.4 Principios de Inteligencia Artificial: Veracidad y Control

La adopción de sistemas de IA Generativa debe regirse por principios que mitiguen sus riesgos inherentes de fiabilidad y privacidad:

- **Verificación y Trazabilidad:** Los sistemas de IA no deben generar respuestas basándose únicamente en su conocimiento general pre-entrenado. La arquitectura debe forzar técnicamente la vinculación de las respuestas generadas con fuentes documentales verificables dentro del repositorio de la Fundación, proporcionando citas a la fuente original para permitir la auditoría humana de cada afirmación.
- **Privacidad en la Inferencia:** Se debe garantizar contractualmente que los datos, documentos y consultas utilizados por la Fundación para interactuar con los modelos de IA no serán utilizados, en ningún caso, para el reentrenamiento de los modelos fundacionales del proveedor que son compartidos con otros clientes.

## 4. REQUISITOS DE LA NUEVA ARQUITECTURA

Los requisitos que se detallan a continuación definen las capacidades técnicas y funcionales que la solución propuesta debe satisfacer para cumplir con los principios de arquitectura establecidos.

## 4.1 Requisitos Funcionales

### 4.1.1 Plataforma Unificada y Centralizada

4.1.1.1 **Consolidación Multimodal:** La plataforma deberá actuar como un repositorio analítico centralizado capaz de ingerir y almacenar nativamente tanto datos estructurados (registros financieros, bases de datos) como no estructurados (documentos PDF, expedientes escaneados) en un mismo entorno lógico, eliminando la necesidad de silos tecnológicos separados.

4.1.1.2 **Desacoplamiento de Cómputo y Almacenamiento:** Para garantizar la eficiencia en costes y rendimiento, la solución deberá permitir escalar los recursos de procesamiento de datos de manera independiente a la capacidad de almacenamiento, soportando picos de carga sin necesidad de sobre-aprovisionar infraestructura física.

### 4.1.2 Gestión Integral del Ciclo de Vida del Dato (Modelo Histórico)

4.1.2.1 **Separación de Historia e Interpretación:** La arquitectura de datos deberá implementar una separación física entre el almacenamiento de los datos tal como se reciben de los sistemas origen (capa cruda inmutable) y la capa donde se aplican las reglas de transformación de negocio. Esto es necesario para garantizar que un cambio en una regla de negocio nunca altere o destruya la evidencia histórica original.

4.1.2.2 **Identificación Determinista y Distribuida:** Para permitir la integración masiva de datos entre sistemas heterogéneos sin dependencias de secuencias centralizadas (que generan cuellos de botella), la identificación única de los registros deberá basarse en algoritmos deterministas calculados a partir de las propias claves de negocio. Esto permitirá integrar datos de diferentes fuentes sin necesidad de consultas cruzadas previas.

4.1.2.3 **Manejo Sistémico de la Integridad Temporal:** La plataforma debe incluir mecanismos automáticos para gestionar la integridad referencial en el tiempo, incluyendo la generación de registros de sistema (*registros fantasma*) que representen la ausencia de datos o llegadas tardías, permitiendo así realizar consultas de alto rendimiento (*equi-joins*) sin recurrir a lógica compleja de nulos en tiempo de lectura.

### 4.1.3 Clasificación Avanzada y Recuperación Eficiente

4.1.3.1 **Búsqueda Semántica y Vectorial:** El sistema no debe limitarse a la búsqueda por palabras clave. Deberá incluir capacidades nativas para indexar el significado conceptual de los documentos (vectorización), permitiendo localizar

expedientes o normativas basándose en la intención de la consulta y no solo en la coincidencia literal de texto.

**4.1.3.2 Estructuras de Aceleración de Consultas:** Para garantizar tiempos de respuesta óptimos en consultas históricas complejas, la arquitectura debe contemplar la creación automática de estructuras de virtualización o tablas puente que pre-calculen la lógica temporal de unión entre entidades, desacoplando la complejidad del modelo de almacenamiento de la capa de presentación al usuario.

**4.1.3.3 Protocolo de Contexto para Agentes:** La plataforma de explotación de datos debe exponer sus modelos semánticos a través de protocolos estándar de contexto para IA (tipo Model Context Protocol o similar). El objetivo es que los Agentes de IA puedan "dialogar" directamente con la capa semántica para obtener métricas calculadas fiables, en lugar de intentar inferir consultas SQL complejas sobre datos crudos, lo cual introduce riesgos de alucinación en cálculos financieros.

#### 4.1.4 Colaboración Dinámica y Compartición Segura

**4.1.4.1 Federación de Identidades:** El acceso a los datos no debe requerir la creación de usuarios locales en la plataforma. La solución debe integrarse con los sistemas de identidad corporativos existentes mediante protocolos de federación estándar, evitando la duplicidad de credenciales.

#### 4.1.5 Automatización de Flujos de Trabajo y Procesos

**4.1.5.1 Orquestación sin Servidor (Serverless):** La ejecución de los flujos de ingestión y transformación de datos debe realizarse mediante servicios gestionados que no requieran el mantenimiento de servidores permanentes, ejecutándose únicamente bajo demanda (por eventos o planificación) para optimizar el consumo de recursos públicos.

#### 4.1.6 Digitalización y Captura Inteligente

**4.1.6.1 Anclaje Documental ("Grounding"):** Las capacidades de extracción de información mediante Inteligencia Artificial deben incluir mecanismos de verificación que vinculen cada respuesta generada con la fuente documental original custodiada en el repositorio, permitiendo al usuario auditar la veracidad de la información extraída.

#### 4.1.7 Control de Versiones y Trazabilidad Exhaustiva

**4.1.7.1 Auditoría Inmutable:** Todas las acciones de modificación de datos o configuración de infraestructura deben quedar registradas en un log de auditoría



inmutable, centralizado y protegido contra escrituras, garantizando la trazabilidad forense de cualquier cambio.

#### 4.1.8 Integración y Consolidación de Sistemas

4.1.8.1 **Conectividad Segura sin Intercambio de Claves:** La integración con sistemas externos deberá priorizar mecanismos de autenticación basados en la identidad del servicio (*service identity*) y tokens de corta duración, evitando el almacenamiento y rotación manual de claves estáticas o contraseñas en los códigos fuente o configuraciones.

### 4.2 Requisitos Operacionales

#### 4.2.1 Alta Disponibilidad y Recuperación Continua

4.2.1.1 **Resiliencia Regional:** La plataforma deberá ofrecer por diseño la capacidad de desplegar recursos en múltiples zonas de disponibilidad dentro de una misma región geográfica, garantizando la continuidad del servicio ante fallos físicos de un centro de datos sin intervención manual.

#### 4.2.2 Escalabilidad y Flexibilidad

4.2.2.1 **Escalado a Cero:** Los servicios de cómputo y análisis utilizados para la fase piloto deben tener la capacidad de escalar a cero cuando no estén en uso, eliminando costes residuales por infraestructura ociosa.

#### 4.2.3 Optimización de Costes

4.2.3.1 **Transparencia y Etiquetado:** La plataforma debe permitir la asignación de etiquetas de negocio a cada recurso consumido, facilitando la imputación automática de costes por departamento o proyecto (FinOps) en tiempo real.

### 4.3 Requisitos de Gobierno y Seguridad

#### 4.3.1 Gestión Centralizada de Identidades y Accesos (IAM)

4.3.1.1 **Principio de Mínimo Privilegio Contextual:** El control de acceso no debe basarse únicamente en roles estáticos, sino que debe permitir la evaluación de atributos contextuales (hora, ubicación, estado de seguridad del dispositivo) para autorizar cada petición de acceso a los datos.

#### 4.3.2 Conformidad Normativa y Legal

4.3.2.1 **Soberanía Operativa Configurable:** La plataforma debe disponer de controles técnicos que permitan restringir, mediante políticas de organización inmutables, las regiones físicas donde se permite el almacenamiento y procesamiento de datos, asegurando el cumplimiento del RGPD y el ENS.

4.3.2.2

#### 4.3.3 Seguridad de la Información y Continuidad del Negocio

4.3.3.1 **Perímetros de Seguridad Lógicos:** La solución debe permitir la definición de perímetros de seguridad a nivel de servicio (capa de aplicación/API), que impidan la transferencia de datos hacia recursos no autorizados incluso si el usuario dispone de credenciales válidas. Este control debe ser independiente de la topología de red subyacente.

4.3.3.2 **Detección de Amenazas sin Agentes:** Se requiere un sistema de seguridad centralizado que analice la telemetría de la infraestructura y los logs de auditoría en busca de patrones de comportamiento malicioso (ej. minería de criptomonedas, exfiltración), utilizando inteligencia de amenazas actualizada globalmente, sin necesidad de desplegar agentes de software en cada servidor.

#### 4.3.4 Trazabilidad y Auditoría de Cumplimiento

4.3.4.1 **Transparencia de Acceso del Proveedor:** En el caso de servicios gestionados, la plataforma debe proporcionar registros de auditoría que visibilicen cualquier acceso administrativo realizado por el personal del proveedor de nube (si ocurriera por motivos de soporte), incluyendo la justificación del mismo.

#### 4.3.5 Gobierno del Dato Integrado

4.3.5.1 **Descubrimiento y Clasificación Automática:** La solución debe incluir capacidades para escanear automáticamente los datos en reposo, identificar información sensible (PII, financiera) mediante patrones predefinidos o aprendizaje automático, y aplicar etiquetas de clasificación de seguridad que persistan con el dato.

4.3.5.2 **Catálogo Universal Inteligente:** Se requiere un plano de control unificado que no solo catalogue tablas técnicas, sino que organice lógica y semánticamente los activos de datos, modelos de IA y métricas de negocio. Este catálogo debe utilizar IA para enriquecer automáticamente los metadatos y linaje, proporcionando a los agentes autónomos el contexto necesario sobre la calidad y sensibilidad del dato antes de consumirlo.

## 5. OBJETIVOS CUANTIFICABLES E INDICADORES CLAVE DE RENDIMIENTO (KPIs)

El éxito de la transformación digital no se medirá únicamente por el despliegue de la tecnología, sino por su impacto tangible en la eficiencia operativa de la Fundación. Se

establece un cuadro de mando de indicadores diseñado para monitorizar la transición desde un modelo manual hacia un modelo industrializado de gestión del dato.

### 5.1 Eficiencia en la Entrega:

Estos indicadores miden la capacidad de la nueva arquitectura ("Fábrica de Datos") para acelerar la puesta en producción de nuevos servicios frente al modelo tradicional.

- **Reducción del *Time-to-Market* en Nuevos Dominios:**
  - **Objetivo:** Reducir en un **50%** el tiempo necesario para integrar nuevas fuentes de datos en fases futuras, gracias a la reutilización de los patrones de ingestión y modelos de datos estandarizados (hubs/satélites) desplegados en la Fase I.
- **Frecuencia de Despliegue:**
  - **Objetivo:** Pasar de ciclos de actualización monolíticos (mensuales/trimestrales) a una capacidad de despliegue continuo (semanal o bajo demanda) para correcciones y mejoras, garantizada por la automatización de la infraestructura como código.
- **Tasa de Automatización de Ingesta:**
  - **Objetivo:** Alcanzar un **90%** de automatización en la carga de datos para el dominio piloto (Proyectos Europeos y Administración y Financiero), eliminando la intervención manual en la transformación de ficheros.

### 5.2 Productividad y Satisfacción del Usuario:

Indicadores centrados en la experiencia del departamento de Proyectos Europeos y Administración y área Financiera:

- Reducción de Carga de trabajo Manual y optimización de procesos.
- Respuestas a Preguntas (Question Answering): Puede ir más allá de devolver el documento completo, y responder directamente a la pregunta del usuario con el fragmento de texto más relevante dentro del documento.
- Latencia del Dato para Toma de Decisiones.
- Precisión y Utilidad de la IA.
- Clasificación y Etiquetado Inteligente de Datos.
- Extracción Inteligente de datos.
- Detección de Duplicados e identificación de la última versión.
- Búsqueda Semántica.
- Análisis avanzado para la búsqueda de grandes volúmenes.
- Control de Acceso Refinado, garantizando que solo el personal autorizado pueda acceder, ver o modificar ciertos archivos.
- Detección de anomalías: para detectar accesos o descargas inusuales.
- Automatización de Flujos de Trabajo: Puede activar acciones o mover documentos automáticamente a la siguiente etapa de un proceso.

### 5.3 Cumplimiento y Seguridad:

Métricas diseñadas para validar la robustez de la arquitectura de seguridad y la soberanía del dato.

- **Cobertura de Auditoría:**
  - **Objetivo:** 100% de trazabilidad en las acciones de acceso y modificación de datos. Cada consulta debe poder vincularse inequívocamente a una identidad federada, eliminando los accesos anónimos o compartidos.
- **Tiempo de Detección y Respuesta (MTTD/MTTR):**
  - **Objetivo:** Detección proactiva de configuraciones inseguras o vulnerabilidades en la infraestructura en tiempo casi real (< 1 hora), gracias a los sistemas de escaneo continuo sin agentes.
- **Índice de Soberanía del Dato:**
  - **Objetivo:** 0% de incidentes relacionados con la ubicación del dato fuera de la región designada, garantizado mediante políticas de organización inmutables que impiden despliegues no conformes.

### 5.4 Optimización de Costes:

Indicadores financieros para asegurar el uso responsable de los fondos públicos mediante arquitecturas elásticas.

- **Eficiencia de Recursos en Reposo:**
  - **Objetivo:** Reducción de costes operativos mediante el uso de servicios que escalen a cero (*Scale-to-Zero*) cuando no estén en uso (ej. entornos de desarrollo fuera de horario laboral o motores de análisis sin consultas activas).
- **Transparencia de Costes (FinOps):**
  - **Objetivo:** Capacidad de imputar el 100% de los costes de la plataforma a proyectos o departamentos específicos mediante etiquetado automático, permitiendo un control presupuestario granular y evitando costes ocultos de infraestructura compartida.

## 6. EQUIPO DE TRABAJO Y PLANIFICACIÓN DE ALTO NIVEL

La ejecución del contrato deberá regirse estrictamente por una metodología **Ágil centrada en el Usuario**, diseñada para maximizar la entrega de valor temprana y reducir la incertidumbre técnica. El adjudicatario deberá demostrar capacidad para invertir el ciclo de desarrollo tradicional, priorizando la validación visual de la solución antes de acometer el desarrollo de la infraestructura subyacente.

### 6.1 Requisitos del Equipo de Trabajo: Célula Ágil Unificada

Para garantizar la fluidez en la comunicación y la entrega, el adjudicatario deberá constituir una única **Célula Ágil Multidisciplinar (Squad)**. Se desestimarán propuestas que planteen equipos silos aislados o departamentos estancos. El equipo ofertado deberá integrar todas las capacidades

necesarias para completar historias de usuario de principio a fin (*End-to-End*).

El equipo de trabajo deberá contar, como mínimo, con los siguientes roles y responsabilidades:

- **Scrum Master (Responsabilidad del Adjudicatario):** Será el responsable de facilitar las ceremonias ágiles, eliminar bloqueos operativos y asegurar la velocidad de entrega del equipo técnico.
- **Equipo de Entrega Técnica (Responsabilidad del Adjudicatario):** Deberá estar compuesto por perfiles técnicos cruzados que cubran las siguientes competencias: Arquitectura Cloud y Seguridad, Ingeniería de Datos (*Data Engineering*), Especialistas en IA Generativa y Diseño de Experiencia de Usuario (UX/UI).
- **Interlocución con la Fundación:** El equipo deberá trabajar en coordinación directa con el *Product Owner* designado por la Fundación Madri+D, quien será el responsable de priorizar la pila de producto (*Backlog*) y validar los prototipos.

## 6.2 Metodología de Ejecución Requerida: Estrategia "Mockup First"

El adjudicatario deberá adoptar una estrategia de ejecución guiada por el diseño y no por la infraestructura. El ciclo de desarrollo deberá cumplir los siguientes pasos obligatorios:

1. **Definición de Historias de Usuario:** El adjudicatario deberá traducir las necesidades de negocio de los departamentos piloto (Proyectos Europeos y Administración y Financiero) en un catálogo de Historias de Usuario concretas y aceptadas por la Fundación.
  - **Validación Visual Previa ("Mockup First"):** Como requisito previo a la escritura de código de procesamiento, el adjudicatario deberá diseñar y presentar **prototipos visuales (*Mockups*) de alta fidelidad**. **Requisito:** La Fundación deberá validar visualmente el resultado final esperado durante las primeras semanas. No se autorizará el desarrollo técnico de componentes que no hayan sido validados visualmente mediante prototipo.
2. **Construcción del "Esqueleto Funcional" (*Walking Skeleton*):** Una vez aprobado el diseño, el equipo técnico deberá construir la infraestructura mínima necesaria (tuberías de datos y modelos de datos) para conectar dicho diseño visual con datos reales del repositorio.
3. **Iteración e Inteligencia:** Sobre la funcionalidad base, se añadirán las capas de inteligencia (Agentes de IA) para enriquecer la experiencia del usuario final.

## 6.3 Planificación y Hitos de Entrega (Fase I - 9 Semanas)

El adjudicatario deberá estructurar el plan de trabajo en tres ciclos iterativos (*Sprints*) de 3 semanas de duración máxima cada uno. Cada ciclo deberá culminar con un hito de entrega tangible y demostrable ante el Comité de Dirección.

Sprint 1: Visualización y Cimientos (Semanas 1-3)

- **Objetivo:** Definición de la experiencia de usuario y despliegue de la infraestructura base.
- **Entregables obligatorios:**
  - Catálogo de Historias de Usuario priorizado y aprobado.

- Prototipos interactivos (*Mockups*) validados por la Fundación.
- Informe de despliegue de la Zona de Aterrizaje (*Landing Zone*) segura y configurada según normativa.

Sprint 2: Conexión del Dato Real - MVP Funcional (Semanas 4-6)

- **Objetivo:** Ingesta de datos históricos y materialización del prototipo.
- **Entregables obligatorios:**
  - Cuadros de Mando Operativos funcionales, conectados al repositorio de datos unificado.
  - Informe de validación de calidad y veracidad del dato histórico cargado (concordancia con fuentes originales).

Sprint 3: Inteligencia Artificial y Cierre (Semanas 7-9)

- **Objetivo:** Activación de capacidades cognitivas y transferencia.
- **Entregables obligatorios:**
  - Asistente de IA Integrado operativo, con capacidad de búsqueda semántica y justificación documental (*Grounding*).
  - Documentación técnica final y ejecución del plan de formación y transferencia al equipo de la Fundación.

## 7. TRANSFERENCIA DE CONOCIMIENTO Y DOCUMENTACIÓN.

El adjudicatario deberá garantizar que, durante la ejecución de los Sprints, se realicen sesiones de trabajo conjuntas con el personal técnico de la Fundación (*Training on the Job*), con el objetivo de asegurar que, a la finalización del contrato, la institución disponga de la autonomía necesaria para operar y gobernar la nueva plataforma.

Adicionalmente, el adjudicatario deberá elaborar la documentación adecuada para asegurar el objetivo antes descrito de la autonomía que deberá alcanzar la Fundación. Esta documentación debe formalizar y respaldar todo el proceso de capacitación y la entrega de manuales operativos, técnicos y de usuario, asegurando la trazabilidad y permanencia del conocimiento adquirido.

Se valorará positivamente que el adjudicatario, además del formato escrito, proporcione dicha documentación en modalidad de piezas en formato audiovisual (tutoriales, vídeos explicativos, etc.) que hagan más amigable y eficiente el proceso formativo y la consulta posterior del conocimiento.

## 8. DURACIÓN DEL CONTRATO.

La duración del contrato será de UN (1) año, desde el día siguiente a la fecha de firma del contrato sin posibilidad de prórroga. (máxima duración del contrato UN (1) año)

## **9. PRESUPUESTO MÁXIMO DEL CONTRATO.**

El precio máximo del contrato por UN AÑO será por el que resulte del acuerdo de adjudicación que en ningún caso podrá exceder de CIENTO VEINTE MIL EUROS (120.000,00 euros), importe al que habrá que añadir el IVA en vigor, en la actualidad el 21%.

En el precio del contrato se entenderán comprendidos todos los gastos, incluido cualquier impuesto o gravamen que fuera de aplicación, en cuyo caso deberá figurar desglosado este concepto.

## **10. FORMA DE PAGO**

Por los servicios realizados mensualmente, se podrá emitir factura en los últimos 5 días del mes. Una vez recibida la factura por cualquier medio válido en derecho, incluido el correo electrónico, se pagará mediante transferencia en el plazo máximo de 30 días desde la fecha de factura emitida correctamente conforme a derecho, y previa conformidad del servicio realizado.

## **11. LUGAR DE PRESTACIÓN DEL SERVICIO.**

La prestación de los servicios objeto del presente contrato, se realizarán mayoritariamente en las oficinas de la adjudicataria. Acudirá a la sede de la Fundación, sita en Madrid, calle Maestro Ángel Llorca, 6 -1ª planta (28003), cuando sea requerida para mantener las reuniones necesarias para la prestación óptima del servicio.

## **12. CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**

La empresa adjudicataria queda expresamente obligada a realizar los trabajos bajo las cláusulas de secreto profesional y, en consecuencia, a mantener absoluta confidencialidad y reserva sobre la totalidad de los documentos que le sean confiados o que sean elaborados en el desarrollo del proyecto.

Esta confidencialidad es extensible a cualquier dato que pudiera conocer con ocasión del cumplimiento del contrato, especialmente los de carácter personal, que no podrá copiar o utilizar con fin distinto al que figura en este pliego, ni tampoco podrá ceder a terceros ni siquiera a efectos de conservación.

El adjudicatario está obligado a respetar la normativa nacional y de la Unión Europea en materia de protección de datos. Si el contrato implica la cesión de datos al contratista, esta

obligación será condición especial de ejecución del contrato, con el carácter de obligación contractual esencial, cuyo incumplimiento será causa de resolución del contrato, de conformidad con lo dispuesto en el artículo 211.1.f) de la LCSP.

En el caso en que la prestación del servicio suponga el acceso a datos por parte del adjudicatario como encargado del tratamiento, queda obligado al cumplimiento de lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD), en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, especialmente en lo indicado en sus artículos 5, 28 y 33, así como en los esquemas nacionales de seguridad e interoperabilidad en todo lo que sea de aplicación al presente contrato, conforme a lo establecido en las leyes y decretos de aplicación.

En este caso el adjudicatario deberá aportar con carácter previo a la firma del contrato declaración responsable relativa a la comunicación de dónde van a estar ubicados los servidores y desde dónde se van a prestar los servicios asociados a los mismos, así como si está prevista la subcontratación de dichos servicios indicando el nombre o el perfil empresarial de los subcontratistas. Igualmente queda obligado a comunicar cualquier cambio que se produzca a este respecto a lo largo de la vida del contrato.

El adjudicatario deberá firmar además un contrato de acceso a datos de carácter personal donde se recogen las obligaciones establecidas en el artículo 28 del RGPD y aportar una memoria descriptiva de las medidas que adoptará para asegurar la confidencialidad e integridad de los datos tratados y de la documentación facilitada.

Para la información, no sujeta al RGPD, el contratista deberá respetar el carácter confidencial de toda aquella información a la que tenga acceso con ocasión de la ejecución del contrato de acuerdo con lo establecido en el pliego de prescripciones técnicas, o que por su propia naturaleza deba ser tratada como tal. En este caso, el plazo durante el cual deberá mantener el deber de respetar el carácter confidencial de la información será de 5 años.

En Madrid, a 29 de diciembre de 2025

CONFORME:  
EL ADJUDICATARIO  
FECHA Y FIRMA

DIRECTOR

D. Federico MORÁN ABAD

GERENTE

D. Juan SOLER-ESPIAUBA GALLO