

INFORME DE LA PUNTUACIÓN OBTENIDA POR LOS LICITADORES EN LOS CRITERIOS CUYA CUANTIFICACIÓN DEPENDE DE UN JUICIO DE VALOR, CORRESPONDIENTE A LA LICITACIÓN DEL CONTRATO MIXTO DE SUMINISTRO Y SERVICIOS PARA LA OFICINA DE TRATAMIENTO DEL REGLAMENTO Y EL ESPACIO EUROPEO DE DATOS SANITARIOS, CON CARGO AL PLAN DE RECUPERACION TRANSFORMACIÓN Y RESILIENCIA DEL GOBIERNO DE ESPAÑA - FINANCIADO POR LA UNIÓN EUROPEA – NEXTGENERATIONEU (C18.I06.P02.S18)” A ADJUDICAR POR PROCEDIMIENTO ABIERTO CON PLURALIDAD DE CRITERIOS

Expediente A/SUM-001523/2026

1 Contexto

A la licitación del contrato se han presentado las siguientes empresas:

- T-SYSTEMS ITC IBERIA S.A.U. en adelante T-SYSTEMS
- Mercanza S.L. en adelante MERCANZA
- ATOS IT Solutions & Services S.L. en adelante ATOS
- NTT DATA Spain, S.L.U. en adelante NTT
- BOSONIT, S.L. en adelante BOSONIT
- Specialist Computer Centres SL en adelante SCC
- UTE Evidenze Health España, S.L.U. y Medalla Technology Consulting, S.L. en adelante UTE Evidence-Medalla
- Telefónica Soluciones de Informática y Comunicaciones de España S.A.U. en adelante TELEFONICA

Según el pliego de cláusulas administrativas particulares, los criterios cuya cuantificación dependen de un juicio de valor (técnico), son los siguientes:

A.1. Alineamiento de la herramienta suministrada para el cumplimiento del Reglamento de Espacio Europeo de Datos de Salud y especificaciones TEHDAS2 (máximo 12 puntos)

Se valorará que la propuesta de la herramienta permita, sin necesidad de acometer nuevos desarrollos o de incorporar nuevos productos, los requisitos que debe cumplir un Organismo de Acceso a Datos de Salud según el Reglamento Europeo de Espacios de Datos de Salud y especificaciones TEHDAS2.

Se valorarán las funcionalidades propuestas y las tecnologías que las soportan para poder valorar su alineamiento con las especificaciones técnicas recomendadas desde la UE. En particular se valorará la tecnología que soporta las siguientes funciones:

- Punto único de acceso para uso secundario en modo portal web.
- Catálogo para la publicación de los datos disponibles.
- Sincronización con otros catálogos conformes al reglamento.
- Soporte para los flujos de evaluación de solicitudes.



- Emisión de permisos de acceso a datos.
- Disponibilidad de entornos de tratamiento seguro.
- Soluciones de integración y provisión de datos.
- Herramientas de auditoría y trazabilidad.

A.2. Solución tecnológica (máximo 12 puntos)

Para poder dar soporte al organismo de acceso seguro a datos de salud, la herramienta proporcionada debe cumplir con las siguientes características tecnológicas que en la oferta técnica debe explicarse, en detalle, cómo se resuelven tecnológicamente estas características:

- Debe poder desplegarse on premise.
- El catálogo de datos debe poder alimentarse desde diferentes entidades proveedoras de datos e incorporar la gestión del etiquetado Quantum.
- Herramientas de evaluación de riesgos de privacidad integrada con los procesos de gestión de las solicitudes.
- Detallar los mecanismos seguros para la ingesta de datos en el entorno seguro de procesamiento temporal.
- Barreras de seguridad automatizables que monitoricen y prevengan riesgos de privacidad dentro de los entornos seguros de procesamiento.
- Se valorarán las diferentes herramientas de análisis de datos y de inteligencia artificial disponibles, en los entornos seguros de procesamiento de datos, para su uso por los investigadores.
- Se valorará la capacidad de monitorización sobre los entornos seguros de procesamiento para detectar amenazas a la privacidad mediante el uso de *queries* o el intento de introducción de códigos maliciosos.

A.3. Propuesta de mecanismo centralizado de gestión de solicitudes de acceso a datos para su uso secundario (máximo 4 puntos)

Se valorará la propuesta de diseño del mecanismo centralizado de gestión de solicitudes de acceso a datos para su uso secundario y cómo se configura dicha propuesta en la herramienta que oferta el proveedor. Se tendrá en cuenta cómo de realista es el mecanismo propuesto en un entorno como el del Servicio Madrileño de Salud y si satisface o no todas las necesidades que impone el reglamento para este proceso.

A.4. Descripción de los procesos de integración de la solución con la plataforma corporativa Cloudera (máximo 2 puntos)

Se valorará cómo se resuelve técnicamente la integración de la solución suministrada con el datalake corporativo del fabricante Cloudera, en particular para:

- Sincronización del catálogo de un proveedor de datos (en este caso Cloudera) con el catálogo público del organismo de acceso a datos de salud.
- Ingesta de dataset desde el datalake corporativo (Cloudera) de salud, que haya sido autorizado, mediante un permiso de acceso a datos, para ponerlos a disposición en el espacio seguro de procesamiento cumpliendo con las

especificaciones técnicas de la UE.

Reglas de puntuación:

A continuación, se detallan los valores de puntuación que se otorgarán a cada uno de los criterios:

- **Excelente** (100% sobre la puntuación máxima posible del criterio). Presenta propuesta excelentemente detallada, en todos los aspectos requeridos y para todos los componentes del ámbito de aplicación, con gran aporte de valor para los requisitos del contrato.
- **Alta** (80% de la puntuación máxima posible del criterio). Presenta propuesta muy bien detallada en los aspectos requeridos, con una muy buena adaptación a la problemática de los componentes del ámbito de aplicación del expediente.
- **Medio** (60% sobre la puntuación máxima posible del criterio). Presenta propuesta bien detallada en los aspectos requeridos, adaptada de forma suficiente a la problemática de los componentes del ámbito de aplicación del expediente.
- **Bajo** (40% sobre la puntuación máxima posible del criterio). Presenta propuesta con un nivel bajo de detalle en los aspectos requeridos, generalista o no adaptada de forma suficiente a la problemática de los componentes del ámbito de aplicación del expediente.
- **Muy bajo** (10% sobre la puntuación máxima posible del criterio). Se asignará esta valoración a aquellas ofertas que presenten una propuesta extremadamente generalista, o con un nivel de detalle muy bajo en los aspectos requeridos.

Tras el análisis previo de las ofertas de los licitadores se observan las siguientes incidencias:

a) En el caso de la oferta de la empresa **SCC**:

- **Incumple un requerimiento esencial del pliego**, concretamente el suministro de licencias ya que introduce una restricción en este suministro por volumen de usuarios en una parte de la solución ofertada (10 licencias del módulo cliente HealthDCAT-AP) y el Pliego de Prescripciones Técnicas pide por su parte licencias corporativas.
 - Por una parte, en la oferta técnica del licitador SCC en su página 24, apartado A.2.5 Propuesta de licenciamiento, expresa que: *“Licencias para titulares de datos - Adicionalmente, se incluyen 10 licencias del módulo cliente HealthDCAT-AP Release 5, que permiten a hospitales y centros asistenciales del SERMAS: Crear y publicar datasets, Enriquecer metadatos semánticamente, Mantener la información en el catálogo federado”*.
 - Por la otra, en el PPT en su página 12, se indica que *“El adjudicatario, deberá proporcionar a la DGSD la licencia corporativa del sistema de soporte propuesto por un año”* y que *“El suministro de esta licencia, de titularidad de la*

DGSD, *no estará condicionado a ningún tipo de restricción por volumen de usuarios o uso de la aplicación*”.

Se debe indicar que en la Comunidad de Madrid existen un número de posibles usuarios de la plataforma muy superior al número de 10 licencias incluidas en su oferta.

b) En el caso de la oferta de la empresa **MERCANZA** no sigue la estructura establecida en el PCAP:

- No consta la página correspondiente a la **identificación de la empresa licitadora**.
- No consta la página correspondiente al **Resumen Ejecutivo**
- El número total de hojas de la Oferta sin incluir la identificación de la empresa licitadora ni el Resumen Ejecutivo es de 35 páginas.

c) En el caso de la oferta de la empresa **TELEFONICA** no sigue la estructura establecida en el PCAP:

- No consta la página correspondiente a la **identificación de la empresa licitadora**.
- No incluye un apartado titulado **Memoria Técnica**, Tras el **Resumen Ejecutivo** incluye un apartado titulado **Matriz de trazabilidad** y otro titulado **Marco del proyecto** que ocupan 4 páginas (de la página 4 a la 8). Tras estos apartados se incluyen los 4 apartados a evaluar.
- El número total de páginas de la Oferta sin incluir la identificación de la empresa licitadora es de 30 páginas.

Si bien en el PCAP, en la página 17, se indica que *“La estructura y contenido de la Oferta técnica en general y de la Memoria Técnica en particular debe ajustarse estrictamente a lo establecido en sus respectivos apartados. Toda información que no se encuentre dentro de dicha estructura no se tendrá en cuenta, salvo que los pliegos establezcan lo contrario”*, al considerarse un requisito no esencial de los pliegos, el presente informe ha valorado de manera íntegra las ofertas técnicas presentadas por Mercanza y Telefónica.

2 Valoraciones de las ofertas presentadas

De esta forma, las valoraciones a los criterios de juicios de valor quedan como sigue:

A.1. Alineamiento de la herramienta suministrada para el cumplimiento del Reglamento de EEDS y especificaciones TEHDAS2 (máximo 12 puntos)

Licitador	Descripción de la valoración
ATOS	<p>Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de A.1. Alineamiento de la herramienta suministrada para el cumplimiento del Reglamento de Espacio Europeo de Datos de Salud y especificaciones TEHDAS.</p> <ul style="list-style-type: none"> La solución propuesta se basa en la plataforma Promptly Health que incluye un portal web unificado y accesible que centraliza las operaciones para investigadores, evaluadores y DPOs, permitiendo desde la exploración de datos hasta la validación automática de los fines permitidos y prohibidos del Espacio de Datos de Salud (EEDS). Soporta autenticación federada. Cumple con diseño responsive, WCAG 2.0 nivel AA y la Directiva Europea de Accesibilidad Web. La plataforma propuesta implementa un catálogo nativo para la publicación de los datos disponibles bajo el estándar DCAT-AP y HealthDCAT-AP y los principios FAIRt e incluye el marco de etiquetado QUANTUM para evaluar automáticamente la calidad y utilidad de los <i>datasets</i> en múltiples dimensiones. Para la sincronización con otros catálogos cuenta con un Cross-Border Engine (CBE) basado en eDelivery AS4 para integrarse transfronterizamente con HealthData@EU. Además, expone APIs REST para sincronizar bidireccionalmente metadatos con el Catálogo Nacional y otras CCAA. Incorpora un Sistema de Gestión de Solicitudes (DAAMS) con flujos de trabajo de aprobación automatizados y configurables que incluyen control de SLAs temporales, un motor de validación de propósitos legales y un motor integrado de evaluación de riesgos de reidentificación. Genera permisos de acceso a datos en formato electrónico legible por máquina e interoperable (según el Art. 68 del EEDS) que estipulan condiciones específicas de uso, restricciones, fechas de validez, formato del dato a proveer (por defecto anonimizado) y seguimiento de la publicación de resultados. Proporciona Entornos Seguros de Procesamiento (SPE) aislados y desplegados sobre Kubernetes con control de red. Incluyen herramientas analíticas (Python, R, IA) y un mecanismo <i>airlock</i> de Control de Divulgación Estadística (SDC) que evita fugas de privacidad antes de la exportación. Para la integración y provisión de datos, permite la ingesta segura y controlada hacia el SPE exclusivamente cuando hay un permiso válido. Los datos se someten a seudonimización/anonimización previa a su carga y pueden ser armonizados a modelos estándar como OMOP CDM o HL7 FHIR. Mantiene un registro de auditoría completo e inmutable (<i>append-only</i>) de las acciones (validación, riesgos, decisiones justificadas, extracciones), garantizando total trazabilidad según el EEDS y acorde al nivel Alto del ENS. <p>Se le asigna el rango de ALTO con 9,6 puntos por las siguientes consideraciones:</p> <ul style="list-style-type: none"> Se valora positivamente el muy buen nivel de detalle en la explicación del alineamiento con el EEDS, especialmente en sincronización con otros catálogos y la disponibilidad de los SPE. Se valora negativamente el detalle de la explicación de las funcionalidades del portal web unificado y accesible.



BOSONIT

Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de **A.1. Alineamiento de la herramienta suministrada para el cumplimiento del Reglamento de EEDS y especificaciones TEHDAS2.**

- Propone un **portal web unificado** para el acceso a los datos con poco detalle.
- Propone un **catálogo** para la publicación de los datos interoperable y alineado con el estándar HealthDCAT-AP que permite describir de forma estructurada datasets, distribuciones y servicios, integrando vocabularios controlados y clasificando los datos por nivel de acceso.
- Para la **sincronización con otros catálogos** conformes al reglamento, la oferta propone implementar estándares abiertos, como RDF/DCAT-AP, que habilitan la federación con catálogos nacionales y europeos (como HealthData@EU) y sincronizan automáticamente sus metadatos desde fuentes existentes como Apache Atlas. Sin embargo, no detalla técnicamente dichos mecanismos.
- Respecto el **soporte para los flujos de evaluación de solicitudes**, propone de forma genérica integrar un motor de *workflows* configurable para definir y automatizar el ciclo completo de evaluación, abarcando las validaciones técnicas, legales y de privacidad para múltiples tipologías de solicitudes. Sin embargo, no cita que soporte el ciclo de tramitación (DAAMS) definido por TEHDAS2 ni detalla los mecanismos para la evaluación automática de riesgos de reidentificación.
- Cita de forma genérica y sin detalle que genera **permisos de acceso a datos**, estructurados, trazables e interoperables vinculados a las condiciones de uso del catálogo.
- Propone de forma genérica **habilitar SPE** integrados con Cloudera AI, donde los datos se analizan sin necesidad de extracción (data stays), garantizando la confidencialidad, el aislamiento y el control dinámico de las operaciones.
- Para la **integración y provisión de datos**, propone, de forma genérica y sin detalle, una capa de integración apoyada en APIs, pipelines (Apache Airflow) y conectores para automatizar la ingesta, transformación y provisión controlada de los datos desde múltiples fuentes, alineándose con el modelo DataService.
- Propone de forma genérica y sin detalle técnico el uso de capacidades de **auditoría** avanzada que registran el ciclo de vida de los datos y el acceso de extremo a extremo.

Se le asigna el **rango de BAJO con 4,8 puntos** por las siguientes consideraciones:

- Se valora **positivamente** que se proponga una integración con la plataforma de Cloudera, aunque ciertamente el detalle presentado es bajo.
- Se valora **negativamente** que presenta una propuesta con un nivel bajo de detalle en los aspectos del criterio. Entre otros, respecto al portal web no describe su cumplimiento de accesibilidad o diseño responsive, apenas detalla los mecanismos de sincronización con otros catálogos, no cita que soporte el ciclo de tramitación (DAAMS) definido por TEHDAS2 ni detalla los mecanismos para la evaluación automática de riesgos de reidentificación, cita de forma genérica la emisión de permisos de acceso a datos, los entornos de tratamiento seguro, la herramienta de auditoría y no cita ninguna recomendación TEHDAS2.



MERCANZA

Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de **A.1. Alineamiento de la herramienta suministrada para el cumplimiento del Reglamento de EEDS y especificaciones TEHDAS2.**

- En relación con el **punto único de acceso** para uso secundario en modo portal web, la oferta propone un portal, explicado de forma muy genérica, para la recepción de solicitudes y la canalización mediante formularios, basado en la herramienta "Sistema soporte HDAB" de Mercanza.
- Relativo al **catálogo para la publicación de los datos disponibles**, cita de forma genérica, sin detalle técnico la evolución del catálogo a HealthDCAT-AP.
- Respecto la **sincronización con otros catálogos** conformes al reglamento, la oferta cita de forma genérica, sin detalle técnico, que sincronizará catálogos.
- Relativo al **soporte para los flujos de evaluación de solicitudes**, no nombra modelo DAAMS. Cita de forma muy genérica sin detalle que incluye una gestión de los flujos de revisión, validación, subsanación, autorización o denegación.
- Cita de forma muy genérica sin detalle que incluye una generación del **permiso de acceso a datos** asociado a las solicitudes aprobadas.
- Menciona de forma muy genérica y sin detalle que habilitará **Entornos Seguros de Procesamiento (SPE)**.
- Manifiesta de forma muy genérica y sin detalle que habilitará la **provisión controlada de datos en entornos seguros de procesamiento**.
- Indica de forma muy genérica y sin detalle que habilitará **auditoria y trazabilidad** mediante un registro de acciones, seguimiento de solicitudes, control de decisiones, evidencias de acceso y capacidad de reconstrucción del ciclo completo de gestión y uso de la información.

Se le asigna el **rango de MUY BAJO con 1,2 puntos** por las siguientes consideraciones:

- Se valora **positivamente** que se proponga una integración con la Plataforma de Cloudera existente en la DGSD, aunque ciertamente el detalle presentado sea muy bajo y el contenido muy generalista.
- Se valora **negativamente** que presenta una propuesta extremadamente generalista, con un nivel de detalle muy bajo en los aspectos requeridos. Destacan, entre otros, la falta de detalle relativa al punto único de acceso en el portal web, al catálogo para la publicación, a la sincronización con otros catálogos, a la emisión de permisos de acceso a datos, al entorno de tratamiento seguro, a la integración y provisión de datos, a las herramientas de auditoría y trazabilidad y al soporte para flujo de evaluación de solicitudes donde no nombra el modelo DAAMS. Tampoco hace referencia a las especificaciones TEHDAS2, ni a artículos del Reglamento Europeo de Espacios de Datos de Salud para clarificar lo explicado



NTT	<p>Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de A.1. Alineamiento de la herramienta suministrada para el cumplimiento del Reglamento de EEDS y especificaciones TEHDAS2.</p> <ul style="list-style-type: none"> • Propone un portal unificado basado en su herramienta DSB (Data Space Builder), que actúa como punto de acceso único para todos los roles cumpliendo con diseño responsive y WCAG 2.1 AA. • Dispone de un catálogo basado en un grafo de conocimiento RDF que implementa nativamente HealthDCAT-AP v1.1. • Realiza sincronización bidireccional con otros catálogos mediante APIs REST DCAT-AP y el protocolo SPARQL Federation. Exporta automáticamente metadatos al Catálogo Nacional (ENDS) y se federa con HealthData@EU a través del <i>National Contact Point</i> usando eDelivery AS4. • Propone un motor de flujos de evaluación de solicitudes que soporta todo el ciclo de tramitación (DAAMS) definido por TEHDAS2 y configurable sin código. • Para la emisión de permisos de acceso a datos, utiliza la herramienta REMS (Resource Entitlement Management System) para la emisión automática de permisos interoperables en formato GA4GH Passport/Visa (JWT RS256), codificando las condiciones de uso en vocabulario ODRL y DUO. La decisión formal también se almacena como PDF firmado y sellado. • Proporciona Entornos de Procesamiento Seguro (SPE) en base a la plataforma OpenVRE habilitándolos en contenedores (Kubernetes) y aislados de Internet por proyecto y con volúmenes de almacenamiento cifrados. No se explica con claridad el mecanismo mediante el cual la emisión de un Data Permit aprobado desencadena la creación y aprovisionamiento del entorno seguro de procesamiento (SPE) según las características detalladas en el <i>Data Permit</i>. La integración con el flujo del OpenVR (SPE) no queda suficientemente clara. • Respecto la integración y provisión de datos, extrae los datos desde el datalake Cloudera CDP asegurando que solo lleguen al SPE los autorizados en el permiso. El módulo de ingesta traduce las reglas del permiso a políticas en Apache Ranger para realizar controles de acceso a nivel de fila y columna. La propuesta presenta el conector IDS/Eclipse como mecanismo de intercambio seguro de información entre instituciones basado en contratos. Este enfoque no se correspondería con la función principal de un organismo de acceso a datos (HDAB) puesto que no opera a través de contratos sino mediante la emisión de <i>Data Permits</i> asociadas a una solicitud concreta de uso de datos. • Como herramienta de auditoría y trazabilidad, propone OpenSearch para registrar logs operativos y evidencias de uso en un repositorio central inmutable. Entre otros, registra parámetros enviados, puntuaciones de riesgo (ARX), decisiones del comité y extracciones de datos. <p>Se le asigna el rango de BAJO con 4,8 puntos por las siguientes consideraciones:</p> <ul style="list-style-type: none"> • Se valora positivamente el detalle de la configuración de low-code del flujo de evaluación de solicitudes, aunque efectivamente realizado con un detalle bajo. • Se valora negativamente el nivel bajo de la propuesta en este ámbito. Entre otros puntos, la propuesta de uso de los SPE no esté suficientemente detallada para entender su alineamiento con el Reglamento EEDS. Además, en algunas partes de su descripción, se cita el uso de contratos cuando este concepto no pertenece a los HDAB; por lo que parece parte de una solución de propósito general de espacios de datos. Tampoco se explica detalladamente cómo se configuran los SPE en base a los Data Permits.
-----	--



T-SYSTEMS	<p>Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de A.1.Alineamiento de la herramienta suministrada para el cumplimiento del Reglamento de EEDS y especificaciones TEHDAS2.</p> <ul style="list-style-type: none"> • Propone un portal web que actúa como interfaz unificada (<i>single point of contact</i>) para todos los perfiles de usuario (investigador, gestor, DPO, etc.), articulando el ciclo completo sin necesidad de software cliente. • Relativo al catálogo para la publicación de los datos disponibles, implementa un modelo de dos capas: el catálogo interno en Cloudera (Apache Atlas) y el catálogo público del Espacio de Datos bajo el estándar HealthDCAT-AP y principios FAIR, que incluye etiquetado QUANTUM. • Respecto la sincronización con otros catálogos conformes al reglamento, garantiza la federación bidireccional con el Catálogo Nacional (ENDS) y HealthData@EU. Asimismo, incluye un conector IDSA (Eclipse Dataspace Connector) para la interoperabilidad y federación con otros nodos y otros espacios de datos. • Ofrece soporte al modelo DAAMS de evaluación de solicitudes con flujos configurables para todo el ciclo: registro, subsanación, validación formal, evaluación material, revisión del DPO, decisión y emisión del permiso. • Genera permisos electrónicos de acceso a datos, estructurados e interoperables que rigen como base para la provisión técnica, incluyendo condiciones de uso, vigencia, organizaciones autorizadas y restricciones. • Habilita Entornos de Procesamiento Seguro (SPE) sobre la infraestructura de Cloudera con distintas modalidades (consulta SQL, análisis avanzado, federado), aplicando fuerte aislamiento y control de accesos. • Respecto la integración y provisión de datos, integra la capa de espacio de datos con los sistemas de identidad corporativa, mensajería, firma electrónica y la plataforma de datos Cloudera. • Como herramienta de auditoría y trazabilidad, registra el ciclo administrativo en el Espacio de Datos (DAAMS) y el acceso técnico mediante la API de Apache Ranger, vinculando todo acceso al permiso original y garantizando la trazabilidad EEDS. • Respecto la integración y provisión de datos, extrae los datos desde el datalake Cloudera CDP asegurando que solo lleguen al SPE los autorizados en el permiso. El módulo de ingesta traduce las reglas del permiso a políticas en Apache Ranger para realizar controles de acceso a nivel de fila y columna. La propuesta presenta el conector IDS/Eclipse como mecanismo de intercambio seguro de información entre instituciones basado en contratos. Este enfoque no se correspondería con la función principal de un organismo de acceso a datos (HDAB) puesto que no opera a través de contratos sino mediante la emisión de <i>Data Permits</i> asociadas a una solicitud concreta de uso de datos. <p>Se le asigna el rango de ALTA con 9,6 puntos por las siguientes consideraciones:</p> <ul style="list-style-type: none"> • Se valora positivamente que la propuesta esté muy bien detallada en los aspectos de este ámbito, especialmente en el catálogo para la publicación de los datos disponibles, la auditoría y la integración y provisión de datos. • Se valora negativamente que cuando trata los espacios de procesamiento seguro, no se explica claramente la relación entre las funciones de la solución y el artículo o recomendación correspondiente.
-----------	---



TELEFONICA

Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de **A.1.Alineamiento de la herramienta suministrada para el cumplimiento del Reglamento de EEDS y especificaciones TEHDAS2.**

- Propone un **portal web único**, con las capacidades de Espacio de Datos y del sistema DAAMS permitiendo gestionar el ciclo de vida de las solicitudes con vistas personalizadas para todos los roles de usuario.
- Propone un catálogo para la **publicación de los datos disponibles** por los proveedores (Data Holders) describiéndolos mediante metadatos estandarizados HealthDCAT-AP, garantizando el cumplimiento de los principios FAIR.
- El **catálogo** está diseñado para integrarse con otros catálogos HealthDCAT-AP y permite el intercambio transparente de datos con la futura infraestructura central del EHDS (HealthData@EU) y el ENDS nacional.
- Incorpora un módulo DAAMS que permite la creación automatizada de **flujos de aprobación de las solicitudes** a partir de formularios. Incluye evaluación de riesgos automática, justificaciones y flujos de revisión adaptados a roles como el DPO, Compliance Officer y HDAB. En el subapartado de estimaciones de costes hay un error porque se atribuyen únicamente al Dataholder cuando podrían existir otros costes de la disponibilidad, y luego no se detalla bien que es el Data User, que es quien solicita el acceso a los datos, quien acepte la estimación propuesta.
- Implementa la generación de forma automática de **permisos de acceso a datos** (Data Permits) en formato electrónico estándar y estructurado una vez que el HDAB aprueba la solicitud, notificándolo inmediatamente al investigador. La explicación presenta una confusión conceptual La solución describe el intercambio de datos usando ODRL (Open Digital Rights Language) para negociación desatendida entre Dataholders y otras entidades, cuando ODRL sirve para seguir un permiso fijado y no para una negociación desatendida. El enfoque es erróneo o no está detallado claramente y no respondería al modelo regulado por el EEDS sino para un Espacio de Datos genérico.
- Gestiona el aprovisionamiento ágil, automático o manual, de **Entornos de Procesamiento Seguro (SPE)** aislados en máquinas virtuales (VMs). Estos entornos incluyen herramientas analíticas preinstaladas (Python, R Studio, Jupyter) para que el investigador analice el dato.
- Respecto la **integración y provisión de datos**, propone integrarse directamente con la plataforma corporativa Cloudera para la extracción y transmisión segura de los datos hacia los SPE. La aplicación coordina la transferencia de datos *just-in-time* a través de conectores específicos.
- Respecto la **auditoría y trazabilidad**, todas las transacciones, flujos de aprobación, accesos dentro del SPE y cambios en el catálogo son grabadas de forma inmutable en el sistema, asegurando una trazabilidad total y permitiendo auditorías completas.

Se le asigna el **rango de BAJO con 4,8 puntos** por las siguientes consideraciones:

- Se valora **positivamente** que se proponga una integración con la Plataforma de Cloudera existente en la DGSD, aunque ciertamente el detalle presentado sea bajo.
- Se valora **negativamente** que presente un nivel bajo de detalle y explicación generalista en los aspectos requeridos en el criterio. Entre otras, no incluye ni referencias a especificaciones de TEHDAS2 ni a artículos concretos del Reglamento. Por otra parte, cita que la arquitectura técnica de referenciade de la solución es IDSA-RAM y GAIA-X, pero no explica adecuadamente cómo asegura el alineamiento con el EEDS.



UTE
EVIDENCE-
MEDALLA

Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de **A.1.Alineamiento de la herramienta suministrada para el cumplimiento del Reglamento de EEDS y especificaciones TEHDAS2**

- Propone un **portal web unificado** basado en la solución Anjana Data Platform que actúa como punto único de acceso a los datos de uso secundario para todos los perfiles de usuario. Es accesible desde cualquier navegador moderno, cuenta con soporte multilingüe nativo y permite integrarse con el Active Directory corporativo para ofrecer Single Sign-On (SSO).
- Propone que la plataforma actúa como **Catálogo Central** del HDAB con soporte nativo al estándar HealthDCAT-AP y principios FAIR.
- Respecto la **sincronización con otros catálogos** conformes al reglamento, la oferta propone el uso de una API REST completa para federar metadatos en formato DCAT-AP/HealthDCAT-AP con el Catálogo Nacional (ENDS) y el europeo (HealthData@EU). Incorpora el módulo ADP4DS, que incluye integración nativa con conectores Eclipse Dataspace Components (EDC), alineados con el protocolo IDSA y el Dataspace Protocol (DSP) para negociaciones transfronterizas automatizadas. Adicionalmente, aunque cita que *Anjana dispone de una API REST completa que permite la federación con el ENDS y con el catálogo europeo HealthData@EU,*”. Ambos están pendientes de desarrollo y publicación.
- Soporta un **flujo completo de evaluación de solicitudes** alineado al modelo DAAMS, que abarca desde la solicitud y evaluación automática de riesgos, hasta flujos de aprobación escalados (gestor para bajo riesgo, o DPO/comité ético para alto riesgo). Incluye también la gestión de subsanaciones, denegaciones motivadas y recursos.
- Implementa la emisión del **permiso de acceso a datos** mediante la entidad nativa Data Sharing Agreement (DSA), que incorpora condiciones de uso modeladas en el estándar ODRL. De forma automatizada, la plataforma actualiza el Active Directory del SERMAS y las políticas de Apache Ranger, activando y revocando accesos sin requerir intervención manual. No es lo más adecuado proponer el modelo de Espacios de Datos Genérico (Gaia-X/IDSA) en el contexto del EEDS sin adaptación: usa ODRL y DSA como si fueran contratos bilaterales, plantea la provisión de permisos automáticos (lo que en el ámbito del EEDS supondría preaprobaciones que no están contempladas), y propone la reevaluación autónoma de permisos activos por el sistema, algo igualmente inviable en el marco regulatorio.
- El **Entorno de Procesamiento Seguro** (EPS) se despliega sobre la infraestructura existente de Cloudera mediante sandboxes aislados. El investigador accede a su EPS a través de una *landing page* personalizada donde dispone de herramientas analíticas (HUE/Impala, Trino, Cloudera AI) bajo estrictas restricciones que bloquean las descargas y la función de copiar/pegar.
- Respecto la **integración y provisión de datos**, el modelo desacopla la capa de infraestructura (Cloudera) de la de gobierno (Anjana). Mantiene una sincronización automática con la fuente técnica en Cloudera enriqueciendo los metadatos para el catálogo público sin duplicar los activos originales de información.
- Respecto la **auditoría y trazabilidad**, la solución mantiene relaciones trazables completas entre solicitudes, evaluaciones de riesgo, permisos (DSA) y entornos (EPS). Esto permite la reconstrucción retrospectiva de cualquier decisión frente



a una auditoría, trazando de extremo a extremo desde el uso concreto de un dato hasta la petición original que justificó dicho acceso.

Se le asigna el **rango de MEDIO con 7,2 puntos** por las siguientes consideraciones:

- Se valora **positivamente** que la propuesta está bien detallada en los aspectos requeridos, especialmente en lo relativo al despliegue de los SPE sobre la infraestructura de Cloudera mediante sandboxes aislados y una *landing page* personalizada.
- Se valora **negativamente** que para la Emisión de permisos de acceso a datos propone el modelo de Espacios de Datos genérico (Gaia-X/IDSA), y no explica detalladamente como lo adapta al contexto del Espacio Europeo de Datos de Salud (EHDS). Propone el uso de ODRL y DSA como si fueran contratos bilaterales, plantea la provisión de permisos automáticos (lo que en el ámbito de EHDS supondría preaprobaciones que no están contempladas), y propone la reevaluación autónoma de permisos activos por el sistema, poco detallado su encaje.

A.2. Solución tecnológica (máximo 12 puntos)

Licitador	Descripción de la valoración
ATOS	<p>Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de A.2. Solución tecnológica:</p> <ul style="list-style-type: none"> La arquitectura de la plataforma Promply Health ofertada se despliega íntegramente en la infraestructura on-premise de la DGSD utilizando contenedores y microservicios (Kubernetes). La persistencia de la información se realiza mediante una base de datos PostgreSQL 3 Respecto el catálogo de datos e interoperabilidad propuesto, este catálogo es conforme a los principios del Espacio Europeo de Salud (EEDS) y THEDAS2 integrando múltiples fuentes heterogéneas (i.e. Data Lake, registros sanitarios y fuentes externas) e implementa de forma nativa el etiquetado de calidad QUANTUM, evaluando 12 dimensiones del dato mediante perfilado automático y metadatos. Se habilitan mecanismos de sincronización con otros catálogos. Como herramientas de evaluación de riesgos de privacidad, Integra un motor de riesgos en el sistema de gestión de acceso a datos (DAAMS) integrado con los procesos de gestión de las solicitudes que, previo a la aprobación (Nivel 1), evalúa la sensibilidad del tipo de dato solicitado mediante un algoritmo de puntuación basado en reglas y generando informes con recomendaciones de mitigación. Respecto la ingesta segura de datos en el SPE, tras validar el permiso, el sistema aplica un protocolo automatizado de múltiples capas: extracción selectiva, procesos de seudo o anonimización (hash irreversible), transmisión por canales cifrados (TLS 1.3) y verificación criptográfica de integridad (hash SHA-256). Respecto las barreras de seguridad que prevengan riesgos de privacidad en el SPE, se aplican salvaguardas (Nivel 2) monitorizando en tiempo real para bloquear consultas de baja granularidad. Incluye un mecanismo Airlock para Control de Divulgación Estadística (ej. k-anonimato, redondeo) previo a cualquier exportación de resultados, bloqueando salidas no anonimizadas. Respecto las herramientas de análisis de datos y de IA disponibles en los entornos SPE, se proponen las siguientes preinstaladas: JupyterLab, RStudio, librerías de ML (scikit-learn, XGBoost, LightGBM), <i>Deep Learning/IA</i> (TensorFlow, PyTorch), procesamiento de datos (Pandas, Apache Spark, dplyr), Visualización (matplotlib, seaborn, ggplot2, plotly), SQL, ámbito sanitario (OHDSI, OMOP CDM), permitiendo aceleración por GPU. Respecto la monitorización y detección de amenazas de privacidad en el SPE, incorpora una capa de monitorización continua sobre los SPE que detecta consultas (<i>queries</i>) anómalas e identifica código malicioso a través de análisis estático y dinámico del código ejecutado por los usuarios (ej. intentos de exfiltración o escalada de privilegios). Son registradas en pistas de auditoría inmutables, permitiendo trazabilidad completa. <p>Se le asigna el rango de MEDIO con 7,2 puntos por las siguientes consideraciones</p> <ul style="list-style-type: none"> Se valora positivamente que presente una propuesta bien detallada en los aspectos, especialmente en las herramientas de análisis de datos y de IA. Se valora negativamente que se eche en falta un mayor detalle en la de explicación de lo relativo al componente intermedio seguro y de la monitorización.



BOSONIT

Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de **A.2. Solución tecnológica**:

- La **arquitectura** propuesta se despliega on-premise sobre la infraestructura tecnológica de la DGSD, integrándose de forma nativa con la plataforma Cloudera.
- Respecto el **catálogo de datos e interoperabilidad** propuesto, explica, de forma genérica y con poco detalle, que el catálogo se alimenta de múltiples fuentes integrándose con herramientas de gobierno de datos y metadatos como Apache Atlas. Incorpora nativamente mecanismos de etiquetado avanzado, incluyendo modelos de clasificación tipo QUANTUM, para segmentar los *datasets* por sensibilidad y condiciones. Sin embargo, lo explica de forma genérica con poco detalle.
- Como herramientas de evaluación de **riesgos de privacidad**, incluye un motor de evaluación de riesgos de privacidad integrado en el flujo de solicitudes para realizar evaluaciones automatizadas y asistidas bajo el principio de *privacy by design*. Sin embargo, lo explica de forma genérica.
- Respecto los **mecanismos seguros** de la ingesta de datos en el SPE, la oferta propone que la ingesta se realice mediante pipelines, orquestados con Apache Airflow, y se active exclusivamente tras emitir el permiso. Incluye extracción controlada desde Cloudera, transformación (seudonimización/anonimización), carga directa en el SPE. Sin embargo, lo explica de forma genérica.
- Respecto las **barreras de seguridad** que prevengan riesgos de privacidad en el SPE, se controles de acceso granular, limitación de exportaciones, control dinámico de *queries*, aislamiento de sesiones y políticas estrictas de no extracción.
- La oferta propone **herramientas para el análisis de datos** y la Inteligencia Artificial dentro de los entornos de procesamiento seguro (SPE) apoyándose en los recursos del ecosistema Cloudera, poniendo a disposición entornos interactivos como Jupyter y librerías de machine learning. Sin embargo, lo explica de forma genérica sin citar herramientas.
- Respecto la **monitorización** y detección de amenazas de privacidad en el SPE, la propuesta propone de forma genérica una monitorización que permita el uso de los datos y detectar posibles amenazas a la privacidad.

Se le asigna el **rango de BAJO con 4,8 puntos** por las siguientes consideraciones:

- Se valora **positivamente** que se proponga una integración con la Plataforma de Cloudera existente en la DGSD, aunque ciertamente el detalle presentado sea generalista.
- Se valora **negativamente** que presenta una propuesta con un nivel bajo de detalle y generalista de la solución tecnológica ofertada; principalmente en la explicación del catálogo de datos, del uso del etiquetado de calidad QUANTUM, del motor de evaluación automatizada de riesgos de privacidad y de las herramientas para el análisis de datos (no cita soluciones concretas).



<p>MERCANZA</p>	<p>Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de A.2. Solución tecnológica:</p> <ul style="list-style-type: none"> • Respecto el despliegue de la arquitectura de la solución propuesta, basada en la herramienta 'Sistema Soporte HDAB' de Mercanza, la oferta ni define, ni detalla, el modelo de despliegue de infraestructura si es on-premise o nube pública. La arquitectura se complementa con las herramientas: Cloudera, Protegrity para refuerzo de privacidad, Denodo/Callibra de catálogo y gobierno y Red Hat Openshift. • Respecto el catálogo de datos e interoperabilidad propuesto, la oferta describe de forma generalista con poco detalle cómo resuelve explícitamente la clasificación y etiquetado conforme al enfoque QUANTUM (atributos de calidad, utilidad, integridad). Tampoco detalla cómo se alimenta desde múltiples entidades proveedoras. • Respecto las herramientas de evaluación de riesgos de privacidad, la propuesta no describe el uso de un motor específico o herramienta para puntuar riesgos de reidentificación o privacidad en los extractos provistos. • No se describen los mecanismos técnicos seguros de la ingesta de datos en el SPE. • No se describen barreras técnicas de seguridad que prevengan riesgos de privacidad dentro del SPE, • La oferta no menciona ninguna herramienta concreta para la el análisis de datos y de inteligencia artificial. • La propuesta no detalla la capacidad tecnológica de auditoria activa a nivel de consultas para la monitorización y detección de amenazas de privacidad en el SPE. <p>Se le asigna el rango de MUY BAJO con 1,2 puntos por las siguientes consideraciones:</p> <ul style="list-style-type: none"> • Se valora positivamente que se proponga una solución tecnológica que intenta integrar con la Plataforma de Cloudera existente en la DGSD, aunque ciertamente el detalle presentado sea generalista. • Se valora negativamente que presenta una propuesta extremadamente generalista, con un nivel de detalle muy bajo en la explicación de la solución tecnológica. Concretamente ni define, ni detalla, el tipo de modelo de despliegue de la infraestructura propuesta (si es on-premise o nube pública) Asimismo, también describe de forma generalista y con muy poco detalle cómo resuelve la clasificación y etiquetado de QUANTUM, cómo se alimenta desde múltiples entidades proveedores y el uso de un motor específico o herramienta para puntuar riesgos de reidentificación o privacidad en los extractos provistos, o la capacidad tecnológica de auditoría para la monitorización. De forma adicional, no describe con detalle los mecanismos seguros de la ingesta de datos en el SPE; ni tampoco las barreras técnicas de seguridad que prevengan riesgos de privacidad dentro del SPE, ni herramientas concretas para el análisis de datos.
------------------------	--



NTT

Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de **A.2. Solución tecnológica**:

- La oferta propone una **arquitectura** basada en OpenVRE (Open Virtual Research Environment, del BSC-CNS) desplegado on-premise sobre Kubernetes en la infraestructura tecnológica de la DGSD. Se complementa con las herramientas DSB para el DAAMS, REMS para permisos, ARX para riesgos y el conector IDSA.
- Respecto el **catálogo de datos e interoperabilidad** propuesto, propone que el catálogo RDF ingiera metadatos de múltiples proveedores simultáneamente (i.e. Apache Atlas, fuentes externas vía API DCAT-AP y carga manual). Implementa un pipeline que se integra con QUANTUM Labelling Tool para calcular automáticamente las dimensiones de calidad y agregarlas al grafo del catálogo.
- Respecto las herramientas de evaluación de **riesgos de privacidad**, se integra nativamente con la herramienta ARX principalmente para la conversión de *datasets* en el flujo de DAAMS para evaluar automáticamente el riesgo de reidentificación de los datos y devolver una puntuación que desencadena flujos de aprobación específicos de manera automatizada.
- Respecto los **mecanismos seguros** de la ingesta de datos en el SPE, la ingesta opera bajo un flujo automático activado por el permiso (REMS). Traduce las condiciones en políticas de Apache Ranger, aplica transformaciones de protección (seudonimización con ARX), y transfiere los datos a los entornos (OpenVRE) mediante mTLS con cifrado AES-256 y verificación de integridad SHA-256. Asimismo, cita el uso de un SPE intermedio; sin embargo, no explica su ubicación, su configuración y cómo y quién accede y cómo se supervisa en relación con el Reglamento. En algunos casos el uso de ODRL no se consideraría suficiente para plasmar todas las condiciones establecidas en un *Data Permit*.
- Respecto las **barreras de seguridad** que prevengan riesgos de privacidad en el SPE, las implementa de múltiples capas, como el aislamiento de red sin acceso a Internet, un proxy SQL que bloquea consultas de baja granularidad y un módulo ARX para Control Estadístico de Divulgación antes de toda exportación.
- El SPE propuesto, basado en la plataforma OpenVRE, incluye **herramientas de análisis de datos** y de IA interactivas como JupyterHub (Python, R, Julia), RStudio Server, SQL y potentes librerías de Machine Learning / IA como scikit-learn, XGBoost, TensorFlow, PyTorch y Hugging Face.
- Respecto la **monitorización** y detección de amenazas de privacidad en el SPE, la propuesta propone utilizar el SIEM Wazuh como gestor de eventos de seguridad para analizar patrones. Adicionalmente, cuenta con un proxy SQL que evalúa y bloquea *queries* de riesgo en tiempo real e incluye un módulo de análisis estático de código que inspecciona `<i>scripts</i>` Python/R detectando patrones de exfiltración, rutas no autorizadas o red sospechosa antes de su ejecución.

Se le asigna el **rango de MEDIA con 7,2 puntos** por las siguientes consideraciones

- Se valora **positivamente** que presente una propuesta bien detallada con una buena adaptación a la problemática requerida, especialmente en lo relativo a las barreras de seguridad y la monitorización.
- Se valora **negativamente** que se proponga el uso de un SPE intermedio sin apenas detalle sobre su encaje en la solución, no se detalla dónde se ubica, cómo es su configuración y cómo y quién accede y cómo se supervisa según el Reglamento. No queda claro en que parte de la solución propuesta opera a nivel de arquitectura.



TELEFONICA

Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de **A.2. Solución tecnológica**:

- La oferta declara que la solución propuesta Savana Data Space (SDS) es un producto modular diseñado para ser **desplegado on-premise** en el centro de datos de la DGSD mediante el uso de tecnologías basadas en contenedores.
- Respecto el **catálogo de datos e interoperabilidad** propuesto, el Espacio de Datos Savana (SDS) se conecta con los repositorios existentes de los distintos proveedores de datos (Data Holders). Incorpora un módulo de Data Quality que calcula automáticamente métricas y scores por dimensión para generar el etiquetado QUANTUM de los conjuntos de datos.
- Respecto las herramientas de evaluación de **riesgos de privacidad**, la oferta propone un módulo integrado que evalúa automáticamente las solicitudes para analizar el nivel de privacidad y sensibilidad de los datos. Este motor genera un informe de riesgos detallado que se adjunta automáticamente al flujo de la solicitud para los aprobadores.
- Respecto los **mecanismos seguros** de la ingesta de datos en el SPE, la oferta describe que se integra con Cloudera para la extracción y transmisión segura de los datos hacia los SPE, aplicando cifrado en tránsito y en reposo, pero no detalla un pipeline técnico de ingesta paso a paso. La oferta describe un intercambio de datos entre conectores del Dataholder y del Data User, lo que puede contradecir el EHDS. El modelo correcto sería el acceso controlado a los datos dentro de un SPE, no una transferencia de datos entre partes. Se indica que un *Data User* puede solicitar la creación de un SPE cuando lo más correcto es que sea el Data Access Body a través de un Data Permit quién genere la creación de un SPE.
- Respecto las **barreras de seguridad** que prevengan riesgos de privacidad en el SPE implementa SDC sobre las solicitudes de extracción.
- Los SPE propuestos incluyen de serie **herramientas analíticas** de datos y de IA open source preinstaladas como Jupyter Notebook, Python y R Studio.
- Respecto la **monitorización** y detección de amenazas de privacidad en el SPE, la oferta no describe las capacidades técnicas de monitorización para detectar la introducción de código malicioso o *queries* anómalas. Sin embargo, describe que la solución realiza una auditoría completa registrando todas las transacciones y acciones de forma inmutable para permitir su trazabilidad total.

Se le asigna el **rango de BAJO con 4,8 puntos** por las siguientes consideraciones:

- Se valora **positivamente** que se proponga una integración con la Plataforma de Cloudera existente en la DGSD, aunque ciertamente el detalle presentado sea generalista.
- Se valora **negativamente** que explique con un bajo nivel de detalle y de forma la solución tecnológica. Existe confusión entre la transferencia de datos y el acceso en entorno seguro (SPE): el EHDS no contemplaría en principio la transferencia de datos entre partes, sino la disponibilidad del acceso a los datos de manera controlada dentro de un entorno de procesamiento seguro. Esta falta de aclaración se repite en varias páginas de la oferta, lo que revelaría un desconocimiento estructural del reglamento. De forma adicional, tampoco incluye referencias a especificaciones de TEDHAS2 ni a artículos concretos del Reglamento, o detalla las capacidades técnicas de detección de amenazas de privacidad en el SPE.



T-SYSTEMS	<p>Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de A.2. Solución tecnológica:</p> <ul style="list-style-type: none"> • Despliega íntegramente la arquitectura on-premise en la infraestructura de la DGSD, como modelo desacoplado pero integrado con la plataforma Cloudera. • Respecto el catálogo de datos e interoperabilidad propuesto, por su parte, el catálogo interno en Apache Atlas alimenta al catálogo público HealthDCAT-AP. Aplica etiquetado QUANTUM evaluando dimensiones de calidad (consistencia, precisión, etc.) para clasificar la sensibilidad. • Respecto las herramientas de evaluación de riesgos de privacidad, la oferta cita la evaluación de riesgos integrado en el DAAMS, sin embargo, no explica de forma detallada el funcionamiento cómo se realiza dicha evaluación de riesgos, no declarando por ejemplo la evaluación previa automática a la aprobación o el control de divulgación estadística aplicada antes de cualquier difusión. • Respecto los mecanismos seguros de la ingesta de datos en el SPE, no se mueven ni copian datos hacia silos externos; se otorgan accesos y perfiles en Apache Ranger a través del Directorio Activo, aplicando anonimización previa mediante herramientas si es necesario. Sin embargo, su propuesta no contiene el detalle para responder a las especificaciones de TEDHAS2. Asimismo, la ingesta de datos de orígenes externos podría generar un conflicto ya que puede suponer un riesgo de conflicto de intereses entre entidades: la necesidad de ingestar datos de Data Holders externos dentro del Datalake Corporativo implica que el administrador del Datalake Corporativo tenga acceso a datos externos, lo que podría implicar autorizaciones adicionales. • Respecto las barreras de seguridad que prevengan riesgos de privacidad en el SPE, se aplican controles de accesos basados en identidad y contexto, restricciones de operaciones y herramientas, y revisión continua para evitar divulgaciones indebidas. • Respecto las herramientas de análisis de datos e IA en los SPE, la oferta proporciona acceso vía Cloudera a Apache HUE (SQL/Impala), Apache Trino (federado), Cloudera AI Workbench (Python, R, ML), AI Studios (RAG, datos sintéticos) y entrenamiento federado (NVIDIA Flare). • Respecto la monitorización y detección de amenazas de privacidad en el SPE, propone una monitorización en segundos las peticiones SQL, Spark y modelos ejecutados. Se auditan todos los comandos a través de la API de Apache Ranger, registrando cualquier acceso anómalo en tiempo casi real. <p>Se le asigna el rango de MEDIO con 7,2 puntos por las siguientes consideraciones:</p> <ul style="list-style-type: none"> • Se valora positivamente que presente una solución tecnológica bien detallada, especialmente en las herramientas de catálogo de datos, de análisis de datos y de IA y en la monitorización. Asimismo, se valora la explicación del detalle de la integración de Cloudera. • Se valora negativamente porque no explica de forma detallada el funcionamiento cómo se realiza la evaluación de riesgos, no declarando por ejemplo la evaluación previa automática a la aprobación o el control de divulgación estadística aplicada antes de cualquier difusión. Además, respecto la ingesta de datos en el SPE temporal, su propuesta no contiene el detalle para responder a las especificaciones de TEDHAS2. Adicionalmente, la solución propuesta puede añadir complejidad de autorizaciones y restricciones a personas ajenas a la operativa del HDAB y en el Data Lake corporativo.
-----------	--



UTE
EVIDENCE-
MEDALLA

Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de **A.2. Solución tecnológica**:

- La **arquitectura** propuesta, basada en la plataforma Anjana Data, permite un despliegue on-premise, integrándose de forma contenerizada sobre la infraestructura de la DGSD.
- Respecto el **catálogo de datos e interoperabilidad** propuesto, soporta una arquitectura multi-entidad donde hospitales, centros de investigación, etc., gestionan sus propios datos. La solución describe un proceso de etiquetado de calidad que requiere que los datos que se vayan a publicar en el catálogo sean importados previamente a Cloudera. Esta descripción tiene un bajo nivel de detalle, ya que no se puede obligar a un Dataholder a importar sus datos a la plataforma solo para publicar metadatos en el catálogo. Los datos únicamente pueden moverse al amparo de un permiso de datos y hacia un entorno seguro de procesamiento.
- Respecto las herramientas de evaluación de **riesgos de privacidad**, la propuesta incorpora un motor de riesgos nativo directamente en los flujos (workflows). Calcula una puntuación analizando la sensibilidad del dato y el propósito, lo que desencadena flujos de aprobación automatizados y sugiere acciones de mitigación (puede integrar motores como ARX).
- Respecto los **mecanismos seguros** de la ingesta de datos en el SPE, se basan en el principio de soberanía del dato: los datos ni se mueven ni se replican. El SPE propuesto opera sobre los datos en su ubicación original en Cloudera. Anjana automatiza la creación de políticas en Apache Ranger para conceder acceso temporal y granular. No se detalla cómo será el caso para otros Data Holders fuera de Cloudera y no detalla si se eliminan tras su uso y cómo los SPEs.
- Respecto las **barreras de seguridad** que prevengan riesgos de privacidad en el SPE, implementa una doble capa de seguridad: reglas de gobierno en Anjana y ejecución en Ranger. Aísla entornos, bloquea la función copiar/pegar y descargas, y soporta la integración de SDC antes de exportar resultados, mitigando riesgos como la inferencia de pertenencia.
- Respecto las **herramientas de análisis de datos e IA** en los SPE, se proporciona a través de Cloudera, ofrece Apache HUE (consultas SQL/Trino federadas), Cloudera AI Workbench (Python, R, Scala), aceleración por GPU (NVIDIA NIM/Triton) y herramientas no-code "AI Studios" para datos sintéticos, RAG y fine-tuning. Además, soporta entrenamiento federado con Flower y NVIDIA Flare.
- Respecto la **monitorización** y detección de amenazas de privacidad en el SPE, propone registrar y monitorizar todas las peticiones SQL, Spark y modelos mediante Cloudera y Apache Ranger. Detecta intentos de exfiltración (ej. SELECT * masivos), ataques de inferencia, instalación de herramientas no autorizadas e intentos de introducción de código malicioso, centralizando las alertas en Anjana. Pero no se detalla suficientemente cómo se resuelve.

Se le asigna el **rango de Medio con 7,2 puntos** por las siguientes consideraciones:

- Se valora **positivamente** que presente una solución tecnológica bien detallada, apreciando la explicación del detalle de la integración con Cloudera y las herramientas de análisis.
- Se valora **negativamente** que no aporte gran detalle respecto cómo resuelve ciertas funcionalidades requeridas con la herramienta propuesta. No aclara si es obligatoria la importación de datos de todos los *Data Holders* a Cloudera, ni explica detalladamente la funcionalidad de etiquetado según QUANTUM; tampoco se explica con el detalle necesario el ciclo de vida vinculado a un SPE, por ejemplo, la fase crítica de su eliminación.

A.3. Propuesta de mecanismo centralizado de gestión de solicitudes de acceso a datos para su uso secundario (máximo 4 puntos)

Licitador	Descripción de la valoración
ATOS	<p>Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de A.3. Propuesta de mecanismo centralizado de gestión de solicitudes de acceso a datos para su uso secundario.</p> <ul style="list-style-type: none"> El flujo de trabajo definido en la oferta implementa y monitoriza los tres plazos secuenciales establecidos legalmente por el Reglamento EEDS: 3 meses para la decisión del permiso (Art. 68), 3 meses para la provisión de datos por los titulares (Art. 60) y 2 meses para la disponibilidad de los datos para el usuario. El sistema permite configurar un Nivel de Servicio (SLA) por franja de servicio que asigne plazos según la puntuación de riesgo de la solicitud: <5 días hábiles para riesgo bajo, <15 días hábiles para riesgo medio, y <30 días hábiles para riesgo alto. Define siete roles adaptados al contexto del SERMAS y alineados con el EEDS: Administrador del HDAB, Gestor de solicitudes, Evaluador técnico, Evaluador legal/privacidad, DPO / Responsable de cumplimiento, Administrador de datos y Usuario de datos (Investigador). Respecto la gestión de modificaciones / recursos / retiradas (TEHDAS2 D6.3/D6.4), cubre la gestión posterior a la presentación conforme a TEHDAS2 D6.3 y D6.4. Incluye la suspensión de plazos para modificaciones o solicitudes de información adicional, permite la retirada de la solicitud por parte del usuario, y soporta un flujo para presentar recursos de apelación en caso de denegación. Para la evaluación continua y actualización regulatoria, menciona la evolución controlada del mecanismo y mejora continua, incorpora un proceso de mejora continua y seguimiento regulatorio. Las actualizaciones de la plataforma derivadas de nuevas normativas o especificaciones (como actos de ejecución de la CE o entregables de TEHDAS2) se incluyen en el mantenimiento estándar de la licencia, sin coste ni desarrollo adicional. Respecto la Oficina técnica con conocimiento HDAB nacional, asume la responsabilidad de la oficina de apoyo y pilotaje con experiencia en sector público, pero no especifica tener experiencia nacional directa con HDAB. Respecto la oficina técnica con conocimiento HDAB nacional, Incluye servicios de oficina técnica de apoyo, destacando explícitamente su experiencia funcional y operativa a nivel nacional, al liderar el aterrizaje, definición y conceptualización del modelo HDAB para el SNS en colaboración con el Ministerio de Sanidad. <p>Se le asigna el rango de ALTO con 3,2 puntos por las siguientes consideraciones:</p> <ul style="list-style-type: none"> Se valora positivamente que presente muy bien detallados los mecanismos centralizados de gestión de solicitudes de acceso a datos para su uso secundario. Asimismo, describe de esta forma el flujo con los plazos secuenciales del reglamento, permite configurar el SLA por franja de servicio, define los roles en el contexto del SERMAS y del reglamento, cubre la gestión de modificaciones del TEHDAS2 y menciona la evolución continua necesaria. Se valora negativamente que no defina con profundidad dentro del mecanismo los roles implicados en la ingesta de datos dentro de un SPE.



<p>BOSONIT</p>	<p>Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de A.3. Propuesta de mecanismo centralizado de gestión de solicitudes de acceso a datos para su uso secundario.</p> <ul style="list-style-type: none"> • Define un flujo de trabajo centralizado end-to-end que cubre el ciclo de vida integral de la gestión de solicitudes de acceso a datos para su uso secundario (desde la presentación hasta el cierre y auditoría) que se encuentra alineado con el modelo operativo EHDS y TEHDAS2. Sin embargo, no enumera explícitamente la duración de los "3 plazos legales" en la descripción del proceso. • El sistema permite configurar y adaptar procesos, así como generar métricas operativas sobre los "tiempos de evaluación" y "niveles de riesgo". No obstante, no detalla la configuración de SLAs fijos en franjas exactas de "5, 15 y 30 días". • Respecto la definición de roles SERMAS alineados con EEDS, el diseño tiene en cuenta la "participación de múltiples actores" y se adapta a distintos niveles de acceso, pero no llega a enumerar un listado de ≥ 7 roles específicos alineados con el SERMAS. • Gestión de modificaciones / recursos / retiradas (TEHDAS2 D6.3/D6.4): Cuenta con un motor de workflows configurable diseñado para adaptar los procesos a distintos tipos de solicitudes y requisitos regulatorios del EHDS, aunque no hace mención explícita y directa a la gestión de modificaciones, recursos o retiradas. • Evaluación continua y actualización regulatoria: Incluye expresamente una fase de "Cierre, auditoría y mejora continua" donde el sistema genera métricas operativas para facilitar la mejora del proceso y la toma de decisiones. Sin embargo, no incluye el compromiso literal de que las actualizaciones regulatorias sean "sin coste". • Propone un modelo operativo de la Oficina técnica basado en la creación de una "Oficina de Apoyo al Organismo de Acceso a Datos de Salud" para implantar, configurar y operar el mecanismo. Se apoya en su experiencia previa con un demostrador de Espacios de Datos multisectorial, pero no afirma tener conocimiento o liderazgo de un HDAB a nivel "nacional". <p>Se le asigna el rango de BAJO con 1,6 puntos por las siguientes consideraciones:</p> <ul style="list-style-type: none"> • Se valora positivamente el detalle del mecanismo centralizado de gestión de solicitudes de acceso a datos, aunque ciertamente el detalle presentado sea generalista. También como equivalente nivel se precia la descripción del flujo con los plazos secuenciales del reglamento, permite configurar el SLA por franja de servicio, define los roles en el contexto del SERMAS y del reglamento, cubre la gestión de modificaciones del TEHDAS2 y menciona la evolución continua. • Se valora negativamente que presenta una propuesta con un nivel bajo de detalle en los diferentes aspectos requeridos. De forma adicional, se debe recalcar que la oferta planteada no detalla la configuración de SLAs fijos en franjas exactas, no enumera un listado
-----------------------	--



MERCANZA	<p>Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de A.3. Propuesta de mecanismo centralizado de gestión de solicitudes de acceso a datos para su uso secundario.</p> <ul style="list-style-type: none">• La oferta define de forma genérica un flujo de trabajo end-to-end desde la recepción hasta la resolución de solicitudes de acceso a datos para su uso secundario.• No se mencionan acuerdos de niveles de servicio temporales específicos en la documentación.• No identifica roles funcionales de SERMAS alineados con el EEDS, pero describe de forma genérica los perfiles técnicos de su equipo de trabajo (analistas, consultores).• Respecto la gestión de modificaciones / recursos / retiradas (TEHDAS2 D6.3/D6.4), contempla un flujo que incluye la revisión, validación y subsanación documental, aunque no menciona la gestión de recursos o retiradas.• Para la evaluación continua y actualización regulatoria, menciona la evolución controlada del mecanismo y mejora continua.• Respecto la Oficina técnica con conocimiento HDAB nacional, asume la responsabilidad de la oficina de apoyo y pilotaje con experiencia en sector público, pero no especifica tener experiencia nacional directa con HDAB. <p>Se le asigna el rango de BAJO con 1,6 puntos por las siguientes consideraciones:</p> <ul style="list-style-type: none">• Se valora positivamente que se proponga un mecanismo centralizado de gestión de solicitudes de acceso a datos, aunque ciertamente el detalle presentado sea muy bajo y generalista.• Se valora negativamente que presenta una propuesta con un nivel bajo de detalle y muy generalista en la gestión de solicitudes de acceso a datos para su uso secundario; concretamente la explicación del flujo de trabajo o la gestión de modificaciones al no concretar la de recursos o retiradas. Asimismo, no se mencionan acuerdos de niveles de servicio, no se identifican roles funcionales del SERMAS.
-----------------	---



	<p>Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de A.3. Propuesta de mecanismo centralizado de gestión de solicitudes de acceso a datos para su uso secundario.</p> <ul style="list-style-type: none">• Define un flujo de trabajo completo ("user's journey") basado en TEHDAS2 D6.4 e incluye los plazos legales del Art. 68 del EEDS: 10 días para pre-screening, 2 meses para evaluación (ampliables a 3), 1 mes para subsanación y 15 días para aceptación.• El motor asigna puntuaciones de riesgo desencadenando distintos flujos de aprobación, y se gestionan plazos.• Identifica múltiples roles del SERMAS alineados con el EEDS (Investigador, Gestor, DPO, Custodio, Admin. catálogo, Firmante) y comités adaptados (ST, OTED, CAEP, CEIm-Regional, CDED).• Respecto la gestión de modificaciones / recursos / retiradas (TEHDAS2 D6.3/D6.4), da soporte completo a los procesos de subsanación documental, apelación e informes motivados a través de la herramienta.• Para la evaluación continua y actualización regulatoria, contempla la configuración, mantenimiento y revisión continua de los flujos para evolucionar el modelo.• Respecto la Oficina técnica con conocimiento HDAB nacional, incluye servicios de oficina de apoyo y destaca la alianza estratégica con empresas especializadas para aportar la experiencia operativa, funcional y regulatoria propia del ámbito sanitario.
NTT	<p>Se le asigna el rango de ALTO con 3,2 puntos por las siguientes consideraciones:</p> <ul style="list-style-type: none">• Se valora positivamente que presente un muy buen detalle el mecanismo de la gestión de solicitudes de acceso a datos para su uso secundario y la explicación del flujo de trabajo. Asimismo, identifica los roles en el contexto del SERMAS y del reglamento, da soporte completo a los procesos de la gestión de modificaciones del TEHDAS2 y menciona la evolución continua necesaria.• Se valora negativamente que no detalle suficientemente el seguimiento de la obligación de publicar resultados de las investigaciones y la configuración de un SLA por franja de servicio.



TELEFONICA

Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de **A.3. Propuesta de mecanismo centralizado de gestión de solicitudes de acceso a datos para su uso secundario.**

- Describe un diagrama de un **flujo de trabajo end-to-end** completo (solicitud, evaluación de riesgos, aprobación, provisión de SPE y extracción de resultados). Sin embargo, no enumera explícitamente cuáles son los plazos asociados a cada paso.
- La plataforma permite definir flujos de aprobación asociados a tipos de solicitud y evaluaciones de riesgo automáticas. Sin embargo, no se especifican SLAs configurados o predefinidos en tramos temporales ligados a distintas franjas de riesgo.
- Enumera varios **roles funcionales** del SERMAS habilitados en la plataforma, como Health Data Access Bodies (HDAB), Data Holders (DH), Data Users (DU), Administradores del DS y, en el flujo de aprobación, menciona las figuras del DPO y Compliance Officer.
- Respecto la **gestión de modificaciones** / recursos / retiradas (TEHDAS2 D6.3/D6.4), el módulo DAAMS propuesto gestiona el ciclo de vida y contempla, en caso de denegación, que el sistema notifique al usuario para que este inicie una "nueva solicitud" pudiendo para ello reutilizar la solicitud original, modificando las partes que corresponda", habilitando funcionalmente la gestión de modificaciones o subsanaciones.
- Para la **evaluación continua** y actualización regulatoria, la propuesta indica que el ciclo de vida de la solución se gestiona "mediante un modelo de actualización controlada", en el cual se proporcionan periódicamente "parches, mejoras y evolutivos". Sin embargo, no se compromete a que dichas actualizaciones de ser necesarias por cambios regulatorios se vayan a realizar.
- Respecto la **Oficina técnica** con conocimiento HDAB nacional, el licitador cuenta con partners del sector salud (Medsavana y CGM) y aporta como experiencia previa y caso de éxito su trabajo experto con el Data Lake sanitario de la DG del Dato.

Se le asigna el **rango de MEDIO con 2,4 puntos** por las siguientes consideraciones:

- Se valora **positivamente** que se proponga un mecanismo centralizado de gestión de solicitudes de acceso a datos, aunque ciertamente el detalle presentado sea generalista.
- Se valora **negativamente** que falte detalle en los diferentes aspectos de este criterio; destacando entre ellos los plazos del flujo de trabajo alineados con el EEDS. Tampoco se especifican SLAs configurados en los tramos temporales definidos en el EEDS.



T-SYSTEMS	<p>Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de A.3. Propuesta de mecanismo centralizado de gestión de solicitudes de acceso a datos para su uso secundario.</p> <ul style="list-style-type: none">• La oferta define un flujo de trabajo end-to-end muy exhaustivo con los plazos legales EEDS nombrados (desde la Secretaría Técnica hasta la provisión).• Respecto los SLAs por franja de riesgo configurables, el motor asigna puntuaciones de riesgo desencadenando distintos flujos de aprobación, y se gestionan plazos.• Identifica múltiples roles de SERMAS alineados con el EEDS (i.e. Investigador, Gestor, DPO, Custodio, Admin. catálogo, Firmante) y comités adaptados (i.e. ST, OTED, CAEP, CEIm-Regional, CDED).• Respecto la gestión de modificaciones / recursos / retiradas (TEHDAS2 D6.3/D6.4), ofrece soporte completo a los procesos de subsanación documental, apelación e informes motivados a través de la herramienta.• Para la evaluación continua y actualización regulatoria, contempla la configuración, mantenimiento y revisión continua de los flujos para evolucionar el modelo.• Respecto la Oficina técnica con conocimiento HDAB nacional, incluye servicios de oficina de apoyo y destaca la alianza estratégica con empresas especializadas para aportar la experiencia operativa, funcional y regulatoria propia del ámbito sanitario. <p>Se le asigna el rango de Excelente con 4 puntos por las siguientes consideraciones:</p> <ul style="list-style-type: none">• Se valora positivamente que presente un nivel excelente de detalle en todos los aspectos requeridos del mecanismo centralizado de gestión de solicitudes de acceso a datos para su uso secundario; y con gran aporte para los requisitos del contrato. Entre otros, define un flujo de trabajo muy exhaustivo con los plazos legales EEDS nombrados, la gestión de los acuerdos niveles de servicio por franja de riesgo, la identificación de múltiples roles del SERMAS alineados con el EEDS, un soporte completo a los procesos de modificaciones del TEHDAS2 y la evaluación continua necesaria para la evolución del modelo.
------------------	--



<p>UTE Evidence- Medalla</p>	<p>Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de A.3. Propuesta de mecanismo centralizado de gestión de solicitudes de acceso a datos para su uso secundario.</p> <ul style="list-style-type: none">• Propone un mecanismo integral alineado con el modelo operativo DAAMS y el Reglamento EHDS (Art. 57-61). La herramienta incluye cuadros de mando para la "monitorización operativa del HDAB" y el "seguimiento de solicitudes y tiempos de procesamiento", pero no enumera explícitamente los plazos de cada uno de ellos.• El sistema es capaz de "sugerir una puntuación de riesgo preliminar antes de que el gestor humano realice la evaluación formal" y monitoriza KPIs de cumplimiento, pero no detalla que los SLAs estén divididos en franjas.• El modelo propuesto por la oferta adapta los flujos a la estructura organizativa del SERMAS, integrándose con el Directorio Activo. Sin embargo, no proporciona un listado de los roles que estarían implicados en la operativa del mecanismo.• Respecto la gestión de modificaciones / recursos / retiradas (TEHDAS2 D6.3/D6.4), implementa de forma nativa el concepto DAAMS bajo las especificaciones TEHDAS2. La UTE indica que ha construido los SEPs completos para la gestión de permisos. Sin embargo, no se detallan los flujos exactos de modificaciones o dotación de recursos.• No se detallan de forma suficiente los procesos de evaluación continua y actualización regulatoria.• Respecto la Oficina técnica con conocimiento HDAB nacional, menciona su experiencia operativizando organismos de acceso a datos de salud en España. Menciona despliegues en Baleares, Canarias, Cantabria sin concretar si son Espacios de Datos de carácter general o específicos de salud según el reglamento. <p>Se le asigna el rango de BAJO con 1,6 puntos por las siguientes consideraciones:</p> <ul style="list-style-type: none">• Se valora positivamente que se proponga un mecanismo centralizado de gestión de solicitudes de acceso a datos, aunque ciertamente el detalle presentado sea generalista.• Se valora negativamente que presente una propuesta generalista y con un nivel bajo de detalle en la gestión centralizada de solicitudes de datos; destacando, entre otros, las siguientes faltas de concreción: no detalla los SLAs divididos en franjas, ni tampoco los flujos de modificaciones o dotación de recursos, ni tampoco los procesos de evaluación continua y actualización regulatoria.
---	---

A.4. Descripción de los procesos de integración de la solución con la plataforma corporativa Cloudera (máximo 2 puntos)

Licitador	Descripción de la valoración
ATOS	<p>Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de A.4. Descripción de los procesos de integración de la solución con la plataforma corporativa Cloudera:</p> <ul style="list-style-type: none"> El mecanismo de integración de la solución propuesta con Cloudera consiste en la extracción de los metadatos del datalake para transformarlo automáticamente al perfil HealthDCAT-AP mediante el API Rest de Apache Atlas. En el documento se incluye una tabla con la correspondencia exacta campo a campo (ej. entity.name a dct:title, lineage a dct:provenance). Para la Provisión de datos al SPE activada por permiso digital, el proceso de ingesta segura estipula que la transferencia de datos hacia los entornos seguros (SPE) se desencadena única y exclusivamente tras la validación de un permiso de datos vigente y firmado electrónicamente. La seguridad propuesta se basa en un modelo unificado que utiliza el Directorio Activo (AD) corporativo para el Single Sign-On (SSO) que traduce las decisiones de acceso en políticas técnicas mediante Apache Ranger y protege cada sesión de transferencia a los SPE empleando tickets de Kerberos. Respecto la auditoria, propone integrar los registros de Cloudera para garantizar la trazabilidad completa, implementando un linaje de datos de extremo a extremo, manteniendo un registro inmutable de operaciones y permitiendo el <i>reporting</i> automático requerido por el Reglamento EEDS. El modelo operativo se estructura de forma alineada a la DGSD en cuatro fases específicas de ejecución: Definición, Configuración, Validación y Pilotaje, para asegurar una implantación progresiva y controlada. <p>Se le asigna el rango de Alto con 1,6 puntos por las siguientes consideraciones:</p> <ul style="list-style-type: none"> Se valora positivamente el alto nivel de detalle de la propuesta, especialmente procesos de integración de la solución con la plataforma corporativa Cloudera. Se valora negativamente que el modelo operativo propuesta para la ingesta no se encuentre excelentemente detallada.



BOSONIT	<p>Se señalan a continuación los elementos más destacables de la oferta para el criterio de A.4. Descripción de los procesos de integración de la solución con la plataforma corporativa Cloudera:</p> <ul style="list-style-type: none">Describe un mecanismo de sincronización bidireccional donde se extraen metadatos técnicos, linaje y atributos de Apache Atlas y se transforman semánticamente al modelo HealthDCAT-AP.Para la Provisión de datos al SPE activada por permiso digital, establece expresamente que la ingesta de datos desde el Data Lake hacia los entornos seguros (SPE) se realiza "exclusivamente tras la emisión de un permiso de acceso por parte del Access Body".Existe una falta de alineamiento entre el diagrama de arquitectura de integración y el texto de la oferta. Por una parte, sitúa a la herramienta Apache Ranger como el componente responsable del control de acceso y las políticas, pero el texto indica que las condiciones del permiso se traducen en controles técnicos directos en Cloudera.Respecto la auditoria, garantiza la trazabilidad extrayendo el data <i>lineage</i> de Cloudera (Atlas). En su pipeline de ingesta (Paso 6) estipula el registro de todo el proceso para mantener "trazabilidad completa desde origen hasta uso", garantizando el cumplimiento del EEDS.El modelo operativo propone una integración nativa y directa con Cloudera reutilizando el ecosistema ya implantado (Data Lake, Atlas, Airflow, Cloudera AI). <p>Se le asigna el rango de ALTO con 1,6 puntos por las siguientes consideraciones:</p> <ul style="list-style-type: none">Se valora positivamente el alto nivel de detalle (muy buen detalle) de la propuesta, especialmente procesos de integración de la solución con la plataforma corporativa Cloudera y de la garantía de la trazabilidad.Se valora negativamente que la propuesta en la sincronización Apache Atlas ↔ HealthDCAT-AP no incluya una tabla de mapeo y que en la seguridad unificada no ha tenido en cuenta el uso del Directorio Activo ni de Kerberos. Asimismo, se observa una falta de claridad en lo relativo a la explicación del permiso de acceso a datos.
----------------	--



MERCANZA

Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de **A.4. Descripción de los procesos de integración de la solución con la plataforma corporativa Cloudera:**

- Contempla la integración y **sincronización** del catálogo con la plataforma corporativa Cloudera.
- Para la Provisión de datos al SPE activada por permiso digital, la generación del permiso de datos asociado a las solicitudes aprobadas es lo que activa la provisión controlada de los datos.
- Para el modelo de **seguridad**, la propuesta menciona una integración genérica con "directorio activo", pero no detalla la integración técnica con Apache Ranger o Kerberos.
- Respecto la **auditoria**, dispone de capacidades de registro de hitos y trazabilidad.
- Propone un modelo operativo de **integración** concebido para asegurar su encaje con el entorno tecnológico corporativo de la Dirección General de Salud Digital desde el inicio del piloto.

Se le asigna el **rango de ALTO con 1,6 puntos** por las siguientes consideraciones:

- Se valora **positivamente** el alto nivel de detalle (muy buen detalle) de la propuesta, especialmente procesos de integración de la solución con la plataforma corporativa Cloudera
- Se valora **negativamente** la falta de concreción en la parte de integración del catálogo y en la descripción de su modelo propuesto de seguridad en lo relativo a la integración técnica con Apache Ranger o Kerberos.



NTT	<p>Se señalan a continuación los elementos más destacables de la oferta para el criterio de A.4. Descripción de los procesos de integración de la solución con la plataforma corporativa Cloudera:</p> <ul style="list-style-type: none">• Propone un componente de sincronización que invoca la API REST v2 de Apache Atlas para recuperar metadatos y transformarlos al modelo RDF HealthDCAT-AP. El documento detalla explícitamente el mapeo campo a campo.• Propone que el proceso de ingesta se desencadena automáticamente cuando un permiso (Data Permit) en la herramienta REMS alcanza el estado PERMIT_ACTIVE. El sistema lee este permiso digital y extrae sus condiciones de acceso (codificadas en ODRL) para garantizar que solo se transfieren los datos exactamente especificados al SPE. Sin embargo, la solución no explica con claridad el mecanismo mediante el cual la emisión de un DataPermit aprobado desencadena la creación y aprovisionamiento del entorno seguro de procesamiento (SPE). Falta la explicación técnica entre el proceso de aprobación y la disponibilización del acceso. La integración de la plataforma OpenVR como SPE parece que no está integrada de forma nativa en el flujo.• Propone una seguridad basada en la integración del Directorio Activo (AD) del SERMAS mediante un proxy OIDC/SAML2 con Keycloak para la gestión de identidades. Además, traduce las condiciones del permiso digital a políticas de Apache Ranger para aplicar control de acceso dinámico a nivel de fila y columna en el Data Lake. Sin embargo, no menciona explícitamente el uso de Kerberos.• Respecto la auditoria, el linaje técnico de los datos (<i>lineage</i>) se extrae directamente de la herramienta Apache Atlas. Los eventos de acceso se registran en la auditoría nativa de Apache Ranger y se integran en el repositorio central OpenSearch del sistema, permitiendo reporting en base al reglamento de EEDS y trazabilidad completa de cada decisión y extracción.• La arquitectura está concebida para desplegarse íntegramente on-premise sobre la infraestructura del perímetro tecnológico de la DGSD, cumpliendo el ENS Alto y garantizando la soberanía del dato exigida en los pliegos. <p>Se le asigna el rango de Alto con 1,6 puntos por las siguientes consideraciones:</p> <ul style="list-style-type: none">• Se valora positivamente el alto nivel de detalle (muy buen detalle) de la propuesta, especialmente procesos de integración de la solución con la plataforma corporativa Cloudera• Se valora negativamente que en la descripción de la seguridad unificada en la integración no haya explicado con detalle que no esté integrada de forma nativa la plataforma OpenVRE en el flujo (se echa de menos la explicación técnica entre el proceso de aprobación y la disponibilización del acceso) y el uso de Kerberos que forma parte de la solución dentro de Cloudera.



TELEFONICA	<p>Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de A.4. Descripción de los procesos de integración de la solución con la plataforma corporativa Cloudera:</p> <ul style="list-style-type: none">• Menciona la sincronización de metadatos en formato HealthDCAT-AP desde el Lakehouse corporativo hacia el catálogo del Espacio de Datos, así como la creación automática de entradas en el catálogo a través de su API tras la extracción.• Para la Provisión de datos al SPE activada por permiso digital, se propone que aprobada la solicitud, el sistema emita un Data Permit. Si el investigador solicita un SPE estándar, este es provisionado de forma automática y en tiempo real en base a los datos exactos del Data Permit, coordinando la transferencia segura a través de los conectores.• La solución de seguridad se integra con el Directorio Activo corporativo (LDAPs del cliente, como MS Entra) para la autenticación y gestión de identidades. No obstante, indica que los controles de acceso se implementan de forma "desacoplada" del Lakehouse. Por su parte, no menciona explícitamente el uso de "Apache Ranger" o "Kerberos" para la unificación de la seguridad en la integración.• Respecto la auditoria, garantiza una trazabilidad total "end-to-end" grabando todas las transacciones de forma inmutable. Además, genera los informes periódicos y estructurados de actividad obligatorios conforme al Artículo 20 del Reglamento EEDS. Sin embargo, no utiliza el término técnico "lineage" al describir la integración con Cloudera.• En la descripción del modelo operativo basado en el producto Savana Data Space, la integración con Cloudera no queda clara porque no cita elementos básicos de cloudera como Apache Ranger, Apache Atlas ni Kerberos. <p>Se le asigna el rango de Medio con 1,2 puntos por las siguientes consideraciones:</p> <ul style="list-style-type: none">• Se valora positivamente el nivel medio de detalle (buen detalle) de la propuesta, especialmente en lo relativo al uso de la plataforma corporativa Cloudera.• Se valora negativamente que no se clarifique la integración con la plataforma Cloudera al no citar elementos básicos como Apache Ranger, Apache Atlas o Kerberos.



T-SYSTEMS	<p>Se señalan a continuación los elementos expuestos por la oferta más destacables referidos al criterio de A.4. Descripción de los procesos de integración de la solución con la plataforma corporativa Cloudera:</p> <ul style="list-style-type: none">• Existe sincronización continua en dos capas (Apache Atlas como fuente interna y HealthDCAT-AP como catálogo público).• La ejecución técnica (provisión de acceso a Cloudera) se activa única y exclusivamente tras la emisión formal y aprobación del permiso administrativo digital.• Para el modelo de seguridad, utiliza las identidades del Directorio Activo/LDAP y aplica las políticas de control de acceso granulares a través de Apache Ranger en el ecosistema Cloudera.• Respecto la auditoria, el linaje de datos se gestiona internamente desde Cloudera, y el reporting/auditoría se nutre de la API de Apache Ranger para registrar de forma inmutable todas las operaciones del SPE.• Respecto el modelo operativo propuesto, la solución no genera silos, sino que se integra como aplicaciones dentro de la plataforma Cloudera ya existente de la DGSD, reduciendo riesgos operativos y acelerando plazos. <p>Se le asigna el rango de Excelente con 2 puntos por las siguientes consideraciones:</p> <ul style="list-style-type: none">• Se valora positivamente el excelente nivel de detalle de la propuesta, especialmente procesos de integración de la solución con la plataforma corporativa Cloudera, y la no generación de silos.



<p>UTE EVIDENCE- MEDALLA</p>	<p>Se señalan a continuación los elementos más destacables de la oferta para el criterio de A.4. Descripción de los procesos de integración de la solución con la plataforma corporativa Cloudera:</p> <ul style="list-style-type: none">• La solución integra Apache Atlas mediante una sincronización en dos capas: primero extrae los metadatos técnicos (vía API REST y plugin JDBC/Hive) y luego los enriquece en Anjana con los atributos de HealthDCAT-AP.• Para la Provisión de datos al SPE activada por permiso digital, en lugar de realizar una ingesta física tradicional, cuando un permiso digital (Data Sharing Agreement - DSA) es aprobado en Anjana, el sistema invoca automáticamente la API de Apache Ranger para crear las políticas de acceso temporal que habilitan los datos al investigador.• Para el modelo de seguridad utiliza el Active Directory (AD) corporativo del SERMAS para ofrecer un Single Sign-On (SSO) y mapear los roles. Asimismo, Apache Ranger gestiona la autorización y el control de acceso en todo el entorno Cloudera integrándose de forma nativa con Anjana.• Respecto la auditoria, una doble capa de auditoría que combina los logs técnicos de acceso a datos generados por Apache Ranger en Cloudera con los registros funcionales del ciclo de vida en Anjana (evaluación, emisión de permisos, revocaciones). Esto asegura una trazabilidad de extremo a extremo conforme a los requisitos del EEDS.• El modelo operativo de integración es nativo entre los productos ofertados de Anjana Data y Cloudera; y se basa en el principio de potenciar la infraestructura existente de la DGSD sin duplicar capacidades ni mover los datos de su ubicación original. <p>Se le asigna el rango de EXCELENTE con 2 puntos por las siguientes consideraciones:</p> <ul style="list-style-type: none">• Se valora positivamente el excelente nivel de detalle de la propuesta, destacando el modelo operativo de integración entre Anjana Data y Cloudera.
---	---

3 Conclusión

En consecuencia, las puntuaciones de las valoraciones para los criterios de juicios de valor para las empresas presentadas son las siguientes:

Criterios de Valoración					
Empresa	A1	A2	A3	A4	Puntuación total
	Alineamiento de la herramienta con el Reglamento de Espacio Europeo de Datos de Salud y especificaciones TEHDAS2 (hasta 12 puntos)	Solución tecnológica (hasta 12 puntos)	Propuesta de mecanismo centralizado de gestión de solicitudes de acceso a datos para su uso secundario (hasta 4 puntos)	Descripción de los procesos de integración de la solución con la plataforma corporativa Cloudera (hasta 2 puntos)	
ATOS	9,6	7,2	3,2	1,6	21,6
BOSONIT	4,8	4,8	1,6	1,6	12,8
MERCANZA	1,2	1,2	1,6	1,6	5,6
NTT	4,8	7,2	3,2	1,6	16,8
TELEFONICA	4,8	4,8	2,4	1,2	13,2
T-SYSTEMS	9,6	7,2	4	2	22,8
UTE EVIDENCE-MEDALLA	7,2	7,2	1,6	2	18,0

Se debe comentar que no se ha valorado la oferta de la empresa SCC, ya que incumple un requerimiento esencial del pliego, como es el suministro de licencias. Introduce una restricción por volumen de usuarios de una parte de la solución ofertada (10 licencias del módulo cliente HealthDCAT-AP). Por su parte, el Pliego de Prescripciones Técnicas pide el suministro de licencias corporativas.

Lo cual se indica a los efectos oportunos.

Madrid, a la fecha de la firma

SUBDIRECTOR GENERAL DE PLANIFICACIÓN, OPERACIONES Y SERVICIOS
DIRECCIÓN GENERAL DE SALUD DIGITAL / CONSEJERÍA DE DIGITALIZACIÓN

Firmado por JOSE LUIS BEZARES DEL CUETO - [REDACTED] el día 22/06/2026 con un certificado emitido por AC CAMERFIRMA FOR NATURAL PERSONS - 2016