
# Guía Técnica EDGE/DM

EDGE/DM public documentation

**EDGE/DM** | Medical-Device Data Space

# Guía Técnica EDGE/DM

*Data Products, políticas, ontología y acceso confiable*

## Documento público EDGE/DM para descarga web · Estado final del piloto

| | |
|---|---|
| **Código documental** | EDGEDM-PUB-TG-ES |
| **Versión** | v1.0 |
| **Fecha** | 2026-06-09 |
| **Ámbito** | Modelo operativo final del piloto |
| **Audiencia** | Integradores técnicos, data spaces, gobernanza técnica, equipos de plataforma |

***Nota de publicación: este documento describe el modelo final de operación del piloto EDGE/DM para descarga pública desde la web. No sustituye acuerdos contractuales específicos, evaluaciones regulatorias ni revisiones legales aplicables a participantes concretos.***

# Índice

### Control documental

| Campo | Valor |
|---|---|
| Responsable | Idneo Technologies S.A.U. / EDGE/DM |
| Estado | Versión pública formal |
| Confidencialidad | Documento público para stakeholders |
| Uso previsto | Información, onboarding, participación y revisión técnica de alto nivel |

## Visión general

Esta guía técnica describe la arquitectura final del piloto EDGE/DM a alto nivel. Está pensada para participantes técnicos, integradores y revisores de gobernanza que necesitan comprender cómo se conectan metadatos, políticas, decisiones y evidencias.

## Arquitectura de referencia

### Capas de referencia

| Capa | Función |
|---|---|
| Portal público | Descubrimiento, documentación, participación y catálogo. |
| Catálogo y metadata | Descripción de Data Products y condiciones. |
| Semántica | Ontología, perfiles y alineamiento entre sistemas. |
| Políticas | DUA/DUP, ODRL-lite, policy bundle y enforcement. |
| Conectores | Canal controlado entre proveedor y consumidor. |
| Evidencia | Registros de publicación, solicitud, decisión y uso. |

## Fundamento semántico y ontología

La ontología proporciona un lenguaje común para participantes, roles, Data Products, políticas, propósitos, evidencias y decisiones de acceso.

- Participante, proveedor, consumidor, operador técnico y autoridad de gobernanza.
- DataProduct, Dataset, InferenceService, ComplianceService y AIModel.
- Permission, Prohibition, Obligation y Constraint.
- Evidence, AnonymisationEvidence, ModelCard e InferenceRecord.
- AccessDecision como resultado trazable de una solicitud gobernada.

## Especificación de Data Product

Cada Data Product se describe mediante una especificación que recoge metadatos obligatorios, política aplicable, evidencias, sensibilidad, riesgo funcional y ciclo de vida.

### Campos de referencia

| Campo | Descripción |
|---|---|
| identifier/title/provider | Identidad, título y organización responsable. |
| type | Dataset, servicio de inferencia, agente IA, tarea federada o servicio de trazabilidad. |
| allowed purposes | Finalidades permitidas. |
| prohibited purposes | Usos excluidos. |
| evidence | Documentación y pruebas de soporte. |
| geography | Restricciones de procesamiento, por ejemplo UE/EEE. |

## Modelo de políticas: DUA/DUP, ODRL-lite y bundle

DUA/DUP expresa condiciones de uso en lenguaje comprensible. ODRL-lite permite representar dichas condiciones de forma máquina-legible. El policy bundle traduce la capa semántica a una entrada determinista para evaluación de políticas.

1. El proveedor define condiciones de uso.
2. El Data Product referencia su DUA/DUP.
3. La proyección ODRL-lite expresa permisos, prohibiciones, obligaciones y restricciones.
4. El bundle operativo alimenta la evaluación de solicitudes.

## AccessRequest y AccessDecision

AccessRequest recoge quién solicita, para qué finalidad, qué acción pretende ejecutar, con qué organización y bajo qué aceptación de términos. AccessDecision devuelve resultado, razones, obligaciones y evidencias vinculadas.

### Flujo

| Entrada | Salida |
|---|---|
| requester, organización, propósito, acción, geografía, aceptación DUA/DUP | GRANT/DENY, motivo, política aplicada, obligaciones, registro trazable |

## Capa de conectores y acceso controlado

Los conectores constituyen el canal controlado para interacciones proveedor-consumidor. El objetivo es evitar rutas paralelas, mantener identidad, aplicar políticas y registrar evidencias relevantes.

## Servicios IA y colaboración federada

Los servicios de IA se tratan como capacidades gobernadas. Un agente IA o servicio de inferencia puede operar como Data Product si se definen tarea, límites, entradas, salidas, logs, evidencias y condiciones de uso.

Los patrones federados permiten colaboración sin centralizar necesariamente datos brutos. La gobernanza del data space aporta identidad, catálogo, políticas y trazabilidad.

## Controles de seguridad, privacidad y uso responsable

- Limitación de finalidad.
- UE/EEE como restricción de procesamiento cuando aplique.
- No redistribución.
- No reidentificación.

- No extracción no autorizada de pesos o datasets.
- Trazabilidad y auditoría de decisiones relevantes.