SUSTAINABILITY DATA SPACES

E6

Modelo de gobernanza y política de datos

Estructura organizativa, modelo operativo (RACI) y procesos de gobernanza de datos del SDS.

ENTREGABLE
E6

VERSIÓN
V2026-06-09

FECHA
2026-06-09

PROYECTO
Sustainability Data Spaces

RESPONSABLE
Oficina del Programa SDS

FORMATO
A4 · OOXML

Tabla de contenido

Contenido del entregable

Tabla 1 Ficha del entregable E6

CAMPO	VALOR
Proyecto	Sustainability Data Spaces (SDS)
Entregable	E6 - Gobernanza y política de datos
Paquete de trabajo	PT3 - Diseño del Marco de Gobernanza y Soberanía de Datos
Actividad principal	A3.1-A3.3 - Modelo de gobernanza, políticas de acceso y trazabilidad de datos
Versión	V1.0
Fecha	2026-06-18
Estado	Documento final
Responsable	Oficina del Programa SDS

1. Resumen ejecutivo

El entregable E6 especifica el modelo de gobernanza de referencia necesario para que Espacios de Datos de Sostenibilidad (SDS) pueda evolucionar hacia un espacio de datos europeo federado: los participantes intercambiarían conjuntos de datos mediante conectores bajo políticas explícitas de control de uso ejecutables por máquina. E6 convierte los activos técnicos y semánticos del proyecto en productos de datos gobernados, con metadatos, responsable, versión, condiciones de uso, procedencia y evidencia de auditoría.

Este entregable define: (1) **órganos de gobernanza y derechos de decisión**, (2) **procesos operativos** (incorporación, ciclo de vida del producto de datos, cambio de política, incidentes, disputas) y (3) **control de uso + ejecución de confianza**, con evidencia de auditoría apta para el aseguramiento y para partes interesadas del sector público. El enfoque se alinea con las prácticas europeas de espacios de datos (DSSC Blueprint; Gaia-X Trust Framework; perfiles de Dataspace Protocol) y adopta estándares ampliamente utilizados para política y confianza (modelo conceptual ODRL; identidad VC/DID).[1] [2] [3] [4] [5] [6] [7]

[1] Data Spaces Support Centre, *Data Spaces Blueprint v2.0*, 2025, https://dssc.eu/space/BVE2/1071251516/Data+Spaces+Blueprint+v2.0.

[2] Gaia-X European Association for Data and Cloud AISBL, *Gaia-X Trust Framework 22.10*, 2022, https://docs.gaia-x.eu/policy-rules-committee/trust-framework/22.10/.

[3] International Data Spaces Association, *Dataspace Protocol*, 2025, https://docs.internationaldataspaces.org/ids-knowledgebase/dataspace-protocol.

[4] Eclipse Foundation, *Eclipse Dataspace Protocol, 2025-1*, 2025, https://eclipse-dataspace-protocol-base.github.io/DataspaceProtocol/2025-1/.

[5] W3C, *ODRL Information Model 2.2*, W3C Recommendation, 2018, https://www.w3.org/TR/odrl-model/.

[6] W3C, *Verifiable Credentials Data Model v2.0*, 2025, https://www.w3.org/TR/vc-data-model-2.0/.

[7] W3C, *Decentralized Identifiers (DIDs) v1.0*, 2022, https://www.w3.org/TR/did-core/.

Resultados principales: - Una estructura de gobernanza (órganos, mandatos, cadencia, escalado) que separa la elaboración de reglas, las operaciones y el aseguramiento. - Un modelo operativo (roles + RACI) y procesos principales preparados para el libro de operaciones (incorporación, ciclo de vida del producto de datos, cambio de política, respuesta a incidentes, resolución de disputas). - Un modelo de políticas de control de uso (finalidad/geocerca/conservación/obligaciones) preparado para mapearse a ejecución por conector en la negociación y el acceso, pendiente de validación en un piloto federado. - Un modelo de confianza federada (VC/DID + registro de emisores de confianza + comprobaciones de revocación/estado) y una línea base de auditabilidad. - Controles de gobernanza para la línea base técnica de SDS: admisión de evidencia de estándares, publicación de relaciones revisadas, gobernanza de unidades/conversiones, contratos de cálculo, procedencia de datos de referencia y límites de valores operativos. - Controles de aceptación e indicadores clave de rendimiento medibles para la evaluación piloto (sección 11).

Capas clave de evidencia de gobernanza (definiciones + ejemplos):

Límite de implementación actual: el repositorio entrega artefactos de gobernanza legibles por máquina, configuraciones EDC/ODRL, registros de confianza, esquemas de auditoría y comprobaciones estáticas. La API FastAPI aplica autenticación y RBAC HTTP, pero no constituye por sí sola un conector federado ni demuestra negociación de contratos, transferencia entre conectores, ejecución completa de geocerca/conservación o emisión de todos los eventos del modelo E6. Esas capacidades son diseño y preparación de piloto hasta que exista evidencia operativa específica.

Tabla 2 Resumen ejecutivo

CAPA DE EVIDENCIA SDS	DEFINICIÓN (PARA QUÉ SE USA)	EJEMPLOS (ENTRADAS ILUSTRATIVAS)
Capa de registro de políticas	Registro de políticas legible por máquina con vocabularios controlados para finalidad, región/geocerca, conservación y valores policyId estables con políticas compatibles con ODRL.	8 políticas, incluida la política predeterminada de denegación total. Finalidades: reporting, audit, supervisory, research, interop_testing.
Capa de vinculación jurídico-técnica	Mapea cada restricción de política a artículos del RGPD/Reglamento de Datos y a los puntos de ejecución correspondientes.	Restricción de finalidad -> RGPD art. 5(1)(b); conservación -> art. 5(1)(e); región -> Reglamento de Datos art. 5.
Perfil de vinculación de finalidad	Define el vocabulario controlado, las reglas de validación y los puntos de ejecución para las restricciones de finalidad.	Códigos de error: PURPOSE_REQUIRED, PURPOSE_INVALID, PURPOSE_NOT_ALLOWED.

CAPA DE EVIDENCIA SDS	DEFINICIÓN (PARA QUÉ SE USA)	EJEMPLOS (ENTRADAS ILUSTRATIVAS)
Perfil de ejecución de conservación	Define periodos de conservación, patrones de deberes ODRL y eventos de evidencia de borrado.	Códigos de conservación: P30D-P730D. Eventos de borrado con integridad mediante cadena hash.
Modelo operativo y RACI	Define asignaciones de rol para actividades de gobernanza con control de cambios y respuesta a incidentes.	Actividades de gobernanza con asignaciones R/A/C/I para los roles operativos definidos.
Registro de emisores de confianza	Registro de emisores de confianza legible por máquina con cumplimiento de Bitstring Status List 2025.	4 emisores con DID, alcances, validez, puntos de conexión de lista de estado y política de rotación.
Esquema de eventos de auditoría	Define 22 tipos de evento con identificadores de correlación e integridad mediante cadena hash.	Tipos de evento: access.granted, policy.evaluated, retention.expired, deletion.executed.
Plantilla de Términos del Producto de Datos	Descripción contractual de un producto de datos con policyIds adjuntos.	ID de producto: urn:sds:dataproduct:e1:dataset-register:v2026-02-20.
Ejemplos de control de uso	Restricciones y deberes ODRL mapeados a JSON de política del conector.	Restricción: purpose == reporting. Deber: deleteAfter con retention <= P365D.
Perfil de incorporación y flujo de acceso	Incorporación DID/VC y flujo de acceso con comprobaciones de estado.	Flujos de emisión OIDC4VCI + presentación OIDC4VP.
Evidencia de controles de aceptación	Comprobaciones estáticas de gobernanza, paquete de conector y paquete de evidencia usadas para demostrar preparación.	Conformidad de gobernanza, consistencia de políticas, consistencia del paquete de conector e integridad del paquete de evidencia.
Gobernanza de evidencia de estándares	Controla la promoción de líneas base de estándares oficiales y de evidencia de granularidad de indicadores controlada a productos de datos SDS.	La evidencia técnica de NEIS (ESRS en inglés), Estándares GRI y Protocolo de GEI (GHG Protocol) se trata como evidencia estructural/de catálogo/de cálculo, no como valores operativos de empresa.
Gobernanza de publicación de relaciones	Controla cuándo las relaciones revisadas entre estándares	Las relaciones con estándares ausentes y pendientes de revisión permanecen en cuarentena hasta su aceptación explícita.

CAPA DE EVIDENCIA SDS	DEFINICIÓN (PARA QUÉ SE USA)	EJEMPLOS (ENTRADAS ILUSTRATIVAS)
	pueden afectar a mapeo, cálculo, búsqueda, exportación o comportamiento de presentación de información.	
Gobernanza de unidades, conversiones y datos de referencia	Controla la normalización del catálogo de unidades, los marcadores no convertibles, las trazas de cálculo y la procedencia de datos de referencia externos.	Los denominadores no convertibles no pueden convertirse silenciosamente; los datos de referencia deben incluir evidencia de fuente, periodo y versión.

2. Contexto, objetivos y alcance

2.1 Contexto: por qué la gobernanza es un entregable (no un anexo)

SDS se construye alrededor del principio "informar una vez, reutilizar muchas veces" para los datos de sostenibilidad. Bajo la CSRD, las organizaciones deben producir información de sostenibilidad estructurada, anclada en los estándares NEIS. Esto crea una demanda elevada de **conjuntos de datos trazables y de alta integridad** que puedan reutilizarse en aseguramiento, solicitudes supervisoras y presentación de información en la cadena de suministro.[8] [9]

Sin embargo, la reutilización requiere gobernanza. Sin controles explícitos de política y confianza, la interoperabilidad es frágil: las organizaciones no compartirán datos, los auditores no se apoyarán en ellos y el operador no podrá demostrar cumplimiento. Por tanto, E6 define el **modelo operativo** que hace desplegable SDS.

2.2 Objetivos

E6 tiene cuatro objetivos:

- **Definir la estructura de gobernanza** (órganos, mandatos, cadencia de decisión) necesaria para operar SDS como un espacio de datos federado.
- **Definir el modelo operativo** (roles, procesos y RACI) para incorporación, publicación, acceso, auditoría y respuesta a incidentes.

[8] Parlamento Europeo y Consejo, *Directiva (UE) 2022/2464 por lo que respecta a la presentación de información sobre sostenibilidad por parte de las empresas*, Diario Oficial de la Unión Europea, 2022, https://eur-lex.europa.eu/eli/dir/2022/2464/oj?locale=es.

[9] Comisión Europea, *Reglamento Delegado (UE) 2023/2772 por el que se completa la Directiva 2013/34/UE en lo que respecta a las normas de presentación de información sobre sostenibilidad*, Diario Oficial de la Unión Europea, 2023, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32023R2772.

- **Definir el modelo de políticas** (finalidad / geocerca / conservación / obligaciones) y cómo se mapea a políticas ejecutables por conectores.[10]
- **Mapear requisitos regulatorios a controles operativos** y a categorías de evidencia pública de gobernanza, creando una línea base de gobernanza medible.

2.3 Alcance y límites

Este entregable cubre la gobernanza de **productos de datos y metadatos** SDS (conjuntos de datos, indicadores, mapeos), y los controles necesarios para compartirlos de forma segura. Las normas nacionales sectoriales, los resultados detallados de DPIA y la selección de certificación quedan intencionadamente fuera del alcance de E6 y deben gestionarse en fases de implementación con asesoramiento jurídico.

3. Metodología (alineada con el estilo de entregables E1/E2)

E6 sigue los mismos principios usados en E1/E2: **estándares primero**, **vinculación con evidencia** y **reproducibilidad**.

3.1 Entradas y fuentes

E6 se basa en dos categorías de fuentes:

- **Evidencia pública de gobernanza SDS (lo que SDS publica hoy)** El registro de políticas, el modelo operativo de gobernanza, el modelo de confianza, el perfil de auditabilidad y las categorías de evidencia de validación ya usados por E1/E2 (vocabularios controlados, auditabilidad, enlaces de evidencia).
- **Estándares/reglamentos externos autorizados (lo que SDS debe cumplir)** Derecho de la UE (RGPD, Reglamento de Datos, Reglamento de Gobernanza de Datos) y estándares de espacios

[10] W3C, *ODRL Information Model 2.2.*

de datos/identidad/política ampliamente utilizados (ODRL; VC/DID; DSSC/Gaia-X/IDSA/Eclipse DSP).[11] [12] [13] [14] [15] [16] [17] [18] [19] [20] [21] [22] [23]

3.2 Disciplina de evidencia y verificación

E6 sigue la disciplina de evidencia utilizada en todos los entregables SDS:

- Los controles de gobernanza se mapean a capas de evidencia de gobernanza versionadas (registro de políticas, plantillas de términos, registro de emisores de confianza, flujo de incorporación).
- Las referencias normativas (reglamentos de la UE, Recomendaciones W3C, especificaciones de OpenID Foundation, versiones de protocolos de espacios de datos) se citan mediante el sistema de claves de cita Chicago de SDS, para permitir revisión trazable y futuras actualizaciones.
- Los controles de aceptación y los indicadores clave de rendimiento (sección 11) se definen con umbrales medibles y expectativas explícitas de evidencia, de modo que la ejecución piloto pueda auditarse.
- Los artefactos de gobernanza legibles por máquina son validados por las puertas de gobernanza SDS antes de tratarse como evidencia utilizable.
- La validación estática demuestra la preparación de los artefactos y la conformidad de políticas; los KPIs operativos siguen requiriendo evidencia del periodo piloto.

3.3 Línea base técnica gobernada de SDS

E6 define los controles de gobernanza para la línea base técnica y operativa de SDS. Los controles se aplican a la admisión de evidencia de estándares, la publicación de relaciones entre estándares, la semántica de unidades y conversiones, la preparación de cálculos, la procedencia de datos de referencia y el límite entre evidencia estructural, fixtures de muestra/entrenamiento y valores operativos:

---

[11] Parlamento Europeo y Consejo, *Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*, Diario Oficial de la Unión Europea, 2016, https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=es.

[12] Parlamento Europeo y Consejo, *Reglamento (UE) 2023/2854 sobre normas armonizadas para un acceso justo a los datos y su utilización*, Diario Oficial de la Unión Europea, 2023, https://eur-lex.europa.eu/legal-content/es/TXT/?locale=es&uri=CELEX%3A32023R2854.

[13] Parlamento Europeo y Consejo, *Reglamento (UE) 2022/868 relativo a la gobernanza europea de datos*, Diario Oficial de la Unión Europea, 2022, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32022R0868.

[14] W3C, *ODRL Information Model 2.2*.

[15] W3C, *Verifiable Credentials Data Model v2.0*.

[16] W3C, *Decentralized Identifiers (DIDs) v1.0*.

[17] W3C, *Bitstring Status List*, 2025, https://www.w3.org/TR/vc-bitstring-status-list/.

[18] OpenID Foundation, *OpenID for Verifiable Credential Issuance*, 2025, https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

[19] OpenID Foundation, *OpenID for Verifiable Presentations*, 2025, https://openid.net/specs/openid-4-verifiable-presentations-1_0.html.

[20] Data Spaces Support Centre, *Data Spaces Blueprint v2.0*.

[21] Gaia-X European Association for Data and Cloud AISBL, *Gaia-X Trust Framework 22.10*.

[22] International Data Spaces Association, *Dataspace Protocol*.

[23] Eclipse Foundation, *Eclipse Dataspace Protocol, 2025-1*.

Tabla 3 Metodología (alineada con el estilo de entregables E1/E2)

ÁREA SDS GOBERNADA	IMPLICACIÓN DE GOBERNANZA EN E6
Evidencia de estándares oficiales y de granularidad de indicadores controlada para NEIS, Estándares GRI y Protocolo de GEI[24] [25] [26] [27]	La gobernanza de admisión de estándares debe preservar el denominador del estándar oficial, la representación técnica SDS y los metadatos preparados para cálculo como capas de evidencia separadas. Los recuentos de indicadores SDS y los nodos de cálculo no redefinen las obligaciones oficiales de presentación de información.
Evidencia estructural/de catálogo/de cálculo separada de los envíos de valores operativos	Una línea base estructural de estándares puede aceptarse sin tratarla como datos de desempeño enviados por la empresa. Los valores operativos requieren su propia evidencia de fuente, periodo, unidad, procedencia y permiso antes de usarse.
Registros de relaciones revisadas entre estándares, incluidos estados de equivalencia exacta, parcial, más amplio/más estrecho, componente, transformación, contexto de apoyo, sin coincidencia y pendiente	La gobernanza de publicación de relaciones debe impedir falsas equivalencias. Solo las relaciones revisadas y aceptadas pueden afectar al mapeo, cálculo, búsqueda, exportación o comportamiento de presentación de información; las filas con estándares ausentes y pendientes de revisión permanecen en cuarentena.
Publicación de mapeo canónico y materialización por pares	La gobernanza de mapeos debe distinguir la evidencia de autoría/revisión del modelo de lectura usado por los servicios operativos. La promoción requiere evidencia, tipo de relación, compatibilidad con estándares instalados y trazabilidad de rollback.
Normalización del catálogo de unidades, marcadores de presentación de información no convertibles y trazas de conversión	La gobernanza de unidades y conversiones debe fallar en cerrado cuando las dimensiones o denominadores son incompatibles. Los marcadores específicos de organización o de unidad reportada requieren gestión explícita en lugar de conversión implícita.
Contratos de cálculo con dependencias de componentes y entradas externas en tiempo de ejecución	La gobernanza de cálculos debe verificar referencias a componentes, entradas requeridas, expectativas de unidad y estado de fórmula antes de que un cálculo sea ejecutable. Las entradas externas en tiempo de ejecución permanecen fuera de la evidencia estructural de estándares hasta que se aporten con metadatos a nivel de valor.
Datos de referencia trazados a fuente, incluidas líneas base de moneda y FX histórico	La gobernanza de datos de referencia debe registrar proveedor, periodo de fuente, versión y evidencia de idempotencia. Los datos de referencia son una dependencia operativa y deben separarse de fixtures de muestra o entrenamiento.
Datos solo de muestra y flujos guiados de recorrido	Los datos de muestra respaldan únicamente evidencia de usabilidad e incorporación. Deben permanecer segregados de la evidencia operativa, la evidencia de auditoría, los datos de referencia y las importaciones de valores de producción.

[24] Comisión Europea, *Reglamento Delegado (UE) 2023/2772 por el que se completa la Directiva 2013/34/UE en lo que respecta a las normas de presentación de información sobre sostenibilidad*.

[25] Global Reporting Initiative, *Estándares GRI: traducción al español y conjunto consolidado de Estándares GRI*, Amsterdam, 2025, https://www.globalreporting.org/how-to-use-the-gri-standards/gri-standards-spanish-translations/.

[26] World Resources Institute and World Business Council for Sustainable Development, *The Greenhouse Gas Protocol: A Corporate Accounting and Reporting Standard*, Revised edition, n.d., https://ghgprotocol.org/corporate-standard.

[27] World Resources Institute and World Business Council for Sustainable Development, *Corporate Value Chain (Scope 3) Accounting and Reporting Standard*, 2011, https://ghgprotocol.org/corporate-value-chain-scope-3-standard.

Estos controles forman parte del alcance de gobernanza de E6. Evitan la sobredeclaración de cobertura de estándares, la activación de relaciones no revisadas, la conversión de unidades incompatibles y la mezcla de evidencia estructural con valores operativos.

4. Modelo de gobernanza (estructura organizativa)

La gobernanza de SDS está diseñada para ser **federada**, **auditable** y **operativamente ligera**. Separa: (1) elaboración de reglas, (2) operaciones diarias y (3) aseguramiento independiente, de forma coherente con las prácticas europeas de espacios de datos.[28]

4.1 Principios de gobernanza (lo que optimizamos)

- **Federación por defecto:** los participantes conservan la soberanía de los datos; SDS gobierna el acceso mediante contratos y políticas en lugar de centralizar los datos.
- **Transparencia y previsibilidad:** las políticas, listas de confianza y perfiles de conformidad se versionan y comunican con ventanas de deprecación.
- **Proporcionalidad:** los controles de gobernanza escalan con el riesgo (por ejemplo, mayor escrutinio para productos de alto riesgo o exposición transfronteriza).
- **Responsabilidad:** toda decisión de acceso debe ser explicable y estar evidenciada (registros de auditoría + IDs de política).
- **Privacidad y seguridad desde el diseño:** la identidad y la ejecución de políticas están integradas en la incorporación y la negociación del conector.[29]

4.2 Órganos, mandatos y derechos de decisión

Tabla 4 Modelo de gobernanza (estructura organizativa)

ÓRGANO	COMPOSICIÓN	MANDATO	DERECHOS DE DECISIÓN	RESULTADOS CLAVE
Asamblea del Espacio de Datos (opcional en piloto; recomendada a escala)	Representantes de proveedores, consumidores y partes interesadas del sector público	Alineamiento estratégico y hoja de ruta anual	Aprobar la hoja de ruta; nombrar la presidencia del Consejo de Gobernanza	Hoja de ruta; informe anual de revisión
Consejo de Gobernanza (GB)	Representación equilibrada + presidencia independiente	Gobierna políticas base, anclajes de confianza y escalados	Aprobar versiones del registro de políticas y del registro de emisores de confianza; aprobar productos de alto riesgo; arbitrar disputas	Versiones de registros; decisiones de escalado

[28] Data Spaces Support Centre, *Data Spaces Blueprint v2.0*.

[29] Parlamento Europeo y Consejo, *Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*.

ÓRGANO	COMPOSICIÓN	MANDATO	DERECHOS DE DECISIÓN	RESULTADOS CLAVE
Autoridad / Operador del Espacio de Datos (DSAu)	Oficina del Programa SDS (operador)	Ejecuta la gobernanza diaria	Incorporar/suspender participantes; operar servicios de catálogo; ejecutar respuesta a incidentes; mantener evidencia	Registros de incorporación; resultados de conformidad; informes de incidentes; paquetes de auditoría
Comité Técnico y de Interoperabilidad (TIC)	Operadores de conectores + proveedores tecnológicos	Mantiene el perfil técnico y las líneas base de interoperabilidad	Recomendar perfil de conformidad de conectores; aprobar propuestas de cambio técnico (GB aprueba cambios disruptivos)	Perfil de interoperabilidad; pruebas de conformidad; avisos de seguridad
Comité Legal y de Cumplimiento (LCC)	Asesoría jurídica + rol de privacidad/DPO + propietario de riesgo	Mantiene plantillas legales y reglas de revisión	Aprobar plantillas; definir disparadores de revisión; asesorar en disputas/incidentes	Plantillas de términos; disparadores de DPIA; guía de transferencias; adendas legales
Función de Auditoría y Aseguramiento (AAF)	Evaluadores internos y/o independientes	Supervisión y aseguramiento independientes	Ejecutar auditorías; hacer seguimiento de remediaciones	Informes de auditoría; seguimiento de remediación

4.3 Cadencia y escalado

- Mensual: TIC y LCC (perfil técnico, plantillas, actualizaciones del registro de riesgos).
- Trimestral: aprobaciones de GB (registros de políticas y emisores; revisiones de productos de alto riesgo).
- Anual: hoja de ruta de la Asamblea (o GB en modo piloto), más revisión de controles de aceptación.

Ruta de escalado para asuntos urgentes (incidente de seguridad, compromiso de emisor, infracción crítica de política): DSAu activa el procedimiento de emergencia; LCC + TIC asesoran; GB ratifica las acciones de emergencia a posteriori en un plazo de 10 días laborables.

4.4 Federación y escalado entre dominios

SDS soporta múltiples dominios (por ejemplo, energía, agua, residuos) y puede federarse entre subespacios de datos. El modelo de gobernanza escala delegando las decisiones diarias de dominio en grupos de trabajo de dominio, manteniendo a la vez líneas base comunes (IDs de política, emisores de confianza, perfil de conector, requisitos de auditoría) aprobadas centralmente por GB. Las disputas de interoperabilidad entre dominios se resuelven a nivel de GB; las excepciones técnicas se acotan temporalmente y se rastrean como elementos de riesgo.

4.5 Decisiones clave de diseño (argumentación)

Tabla 5 Modelo de gobernanza (estructura organizativa)

TEMA	OPCIONES CONSIDERADAS	DECISIÓN	JUSTIFICACIÓN	RIESGOS RESIDUALES / MITIGACIONES
Modelo de confianza	IdP central vs credenciales federadas (VC/DID)	Incorporación VC/DID + registro de emisores	Confianza portable para la federación; evita dependencia de punto único; se alinea con patrones de espacios de datos.[30] [31]	Se requiere madurez operativa; mitigación mediante gobernanza de emisores + comprobaciones de estado.
Expresión de políticas	ACLs propietarias vs conceptos de política basados en estándares	Conceptos ODRL + vocabulario controlado + IDs de política estables	Mejora claridad y portabilidad; permite auditabilidad mediante policyId.[32]	El mapeo a motores de conector difiere; mitigación mediante ejemplos de política + pruebas preproducción.
Punto de ejecución	Pasarela central de políticas vs ejecución del lado del proveedor	El conector del proveedor ejecuta en negociación + acceso	Preserva la soberanía de los datos; escala con la federación; coherente con el patrón de conectores de espacios de datos.	Requiere perfil de conformidad; mitigación mediante pruebas TIC y monitorización.
Auditabilidad	Registros ad hoc frente a esquema mínimo de campos + evidencia de inalterabilidad	Campos mínimos de auditoría + requisito de evidencia de inalterabilidad	La preparación para auditoría depende de registros consistentes; respalda la investigación de incidentes.	Se necesita implementar la canalización de registros; se define como indicador operativo en la sección 11.
Estructura de gobernanza	Comité único vs derechos de decisión separados	GB + operador + comités + aseguramiento	Evita conflictos de interés y mejora la trazabilidad de las decisiones.	Sobrecarga en piloto pequeño; mitigación mediante cadencias ligeras y alcances claros.

[30] W3C, *Verifiable Credentials Data Model v2.0*.

[31] W3C, *Decentralized Identifiers (DIDs) v1.0*.

[32] W3C, *ODRL Information Model 2.2*.

5. Modelo operativo (roles + RACI)

5.1 Roles (conjunto operativo mínimo)

La gobernanza solo se vuelve implementable cuando los roles son explícitos. SDS adopta el siguiente conjunto mínimo de roles:

Tabla 6 Modelo operativo (roles + RACI)

ROL	RESPONSABILIDAD PRINCIPAL	EVIDENCIA TÍPICA BAJO SU RESPONSABILIDAD
Proveedor de datos	Publica productos de datos y define metadatos/términos específicos del producto	Metadatos del producto de datos; políticas adjuntas; evidencia de calidad
Consumidor de datos	Solicita productos de datos y usa datos dentro de finalidades declaradas	Solicitudes contractuales; declaraciones de finalidad; confirmaciones de obligaciones
Propietario del producto de datos	Responsable del ciclo de vida del producto	Términos; IDs de política; avisos de versionado/deprecación; punto de contacto
Data Steward	Garantiza coherencia semántica y reglas de calidad	Alineamiento de vocabulario controlado; reglas de procedencia/linaje; informes de validación
Operador del conector	Opera el conector de forma segura y reenvía registros	Registros de rotación de claves; gestión de parches; configuración de reenvío de registros
Operador de catálogo	Publica metadatos de descubrimiento y mantiene la calidad del catálogo	Exportaciones DCAT-AP; enlace con el registro de conjuntos de datos; informes de validación de catálogo[33]
Emisor de confianza	Emite credenciales de identidad/rol y mantiene listas de estado	Documentos DID del emisor; punto de conexión de lista de estado; eventos de revocación
DPO / Responsable de privacidad	Garantiza decisiones de gobernanza alineadas con el RGPD	Disparadores de DPIA; coordinación de respuesta a brechas; registros de base jurídica
Auditor / Evaluador	Verifica de forma independiente cumplimiento y evidencia	Planes de auditoría; informes; seguimiento de remediación
DSAu (Operador)	Ejecuta operaciones SDS y aplica líneas base	Decisiones de incorporación; registros; libros de operaciones de incidentes; paquetes de evidencia

[33] European Commission, SEMIC, *DCAT-AP 3.0.0*.

5.2 RACI (línea base piloto)

Tabla 7 Modelo operativo (roles + RACI)

ACTIVIDAD	GB	DSAU	TIC	LCC	PROVEEDOR	CONSUMIDOR	AUDITOR
Aprobar cambio del registro de políticas	A	R	C	C	C	C	I
Aprobar cambio del registro de emisores de confianza	A	R	C	C	I	I	C
Aprobar perfil de conformidad de conectores	A	C	R	C	C	C	I
Aprobar publicación de línea base de evidencia de estándares	A	R	C	C	C	I	C
Aprobar publicación de relaciones revisadas	A	R	R	C	C	I	C
Aprobar promoción de unidades, conversiones y datos de referencia	A	R	R	C	C	I	C
Aprobar cambio de regla de cálculo/límite de valores	A	R	R	C	C	C	C
Incorporar/suspender participante	I	R	C	C	C	C	I
Publicar nuevo producto de datos	I	C	C	C	R	I	I
Aprobar producto de alto riesgo / nueva finalidad	A	R	C	R	C	I	C
Respuesta a incidentes + revocación	A	R	R	R	C	C	C
Resolución de disputas (términos/política)	A	R	C	R	C	C	C
Auditoría periódica de cumplimiento	I	C	C	C	C	C	R

Leyenda: R=Responsable, A=Accountable, C=Consultado, I=Informado.

5.3 Salvaguardas de neutralidad y separación de funciones

Para minimizar conflictos de interés (relevante cuando se opera como facilitador neutral), SDS separa: - Elaboración de reglas de política/confianza (GB) de ejecución operativa (DSAu). - Interpretación legal/plantillas (LCC) de decisiones técnicas de interoperabilidad (TIC). - Aseguramiento (AAF / auditores) tanto de elaboración de reglas como de operaciones.

6. Procesos principales (cómo opera SDS)

Esta sección está redactada como narrativa preparada para el libro de operaciones: cada proceso declara el objetivo, los pasos mínimos y los resultados de evidencia requeridos para la auditabilidad.

6.1 Incorporación (participante + conector)

Objetivo: garantizar que solo participantes verificados y conectores conformes puedan negociar contratos y acceder a productos de datos SDS.

Entradas: - Solicitud del participante + aceptación del acuerdo de participación. - Evidencia de identidad para KYB/KYC (según corresponda). - Metadatos de punto de conexión del conector y DID del conector.

Salidas (evidencia): - Registro de decisión de incorporación (aprobar/suspender/rechazar) con marca temporal. - Credenciales emitidas (identidad de organización + vinculación de rol) y puntos de conexión de comprobación de estado. - Resultados de conformidad del conector frente al perfil de interoperabilidad SDS.

Proceso (línea base piloto): 1. Solicitud y definición de alcance (roles de proveedor/consumidor; finalidades previstas). 2. KYB/KYC y emisión de OrgIdentityCredential por un emisor de confianza. 3. Registro del conector: crear/declarar DID del conector; vincular el conector a la identidad de la organización. 4. Asignación de rol: emitir SDSRoleCredential al DID del conector con roles permitidos y alcances de finalidad. 5. Comprobaciones de conformidad: verificar soporte del perfil de protocolo, capacidad de evaluación de políticas y capacidad de reenvío de registros (perfil TIC). 6. Activación: añadir participante/conector a allowlists y habilitar negociación contractual. 7. Monitorización continua: comprobaciones periódicas de estado, revalidación de conformidad y disparadores de incidentes.

La suspensión/desincorporación se produce por expiración, revocación, infracciones repetidas de política o incidentes de seguridad; las credenciales se revocan o suspenden y las entradas de registro se actualizan.

Swimlane (simplificado):

```
Organización        Emisor de confianza   Operador SDS (DSAu)      Comité técnico (TIC)
Conectores
     |                    |                     |                        |
```

```
(Proveedor/Consumidor)
     | Solicitud + alcances|                      |                          |
|
     |-------------------->|                      |                          |
|
     | Evidencia KYB/KYC   |                      |                          |
|
     |-------------------->| Verificar + emitir VC|                          |
|
     |<--------------------| OrgIdentityCredential |                           |
|
     | Registrar DID del conector + metadatos     |                          |
|
     |------------------------------------------->| Validar emisor + vincular DID
|
     |                                             |--------------->| Ejecutar
comprobaciones de conformidad (perfil) |
     |                                             |<---------------| Resultado de
conformidad                          |
     |<-------------------------------------------| Activar participante + roles
|
     |
Ejecutar políticas en negociación/acceso
```

Evidencia: - Evidencia del flujo de incorporación. - Evidencia de gobernanza de emisores de confianza.

6.2 Ciclo de vida del producto de datos (crear → publicar → acceder → retirar)

SDS trata los conjuntos de datos como **Productos de Datos**. Un producto de datos debe ser publicable, contratable y auditable.

Los metadatos mínimos requeridos (línea base piloto) se alinean con las prácticas de catálogo (DCAT-AP) y la trazabilidad del inventario SDS.[34]

Tabla 8 Procesos principales (cómo opera SDS)

CAMPO	REQUISITO
Identificador	URN estable (productId)
Título/descripción	Legible por humanos, no ambiguo
Proveedor/contacto	Entidad responsable y contacto de soporte

[34] European Commission, SEMIC, *DCAT-AP 3.0.0*.

CAMPO	REQUISITO
Licencia/derechos de acceso	Condiciones explícitas de reutilización
Puntos de conexión de distribución	AccessURL / downloadURL / puntos de conexión API
IDs de política	Una o más referencias policyId (finalidad/región/conservación/obligaciones)
Versionado	Semver y reglas de aviso de deprecación
Integridad	Hash de conjunto de datos o hash de versión

Pasos del ciclo de vida: 1. Borrador de metadatos + clasificación (proveedor + steward). 2. Adjuntar Términos e IDs de política (plantilla LCC + registro de políticas).[35] 3. Publicar en catálogo y habilitar negociación. 4. Monitorizar registros de uso y eventos de obligación (traza de auditoría). 5. Versionar, deprecar y retirar de forma previsible (anunciar cambios disruptivos).

Evidencia: - Evidencia de Términos del Producto de Datos. - Evidencia del registro de políticas.

6.3 Negociación contractual y decisión de acceso (mediada por conector)

El acceso a un producto de datos se concede mediante un flujo de negociación contractual alineado con prácticas de protocolos de espacios de datos.[36] [37]

Comprobaciones mínimas en el momento de la negociación: - Validación de identidad/rol del consumidor (verificación VC + comprobaciones de estado). - La declaración de finalidad coincide con las finalidades permitidas del producto. - Compatibilidad de políticas (finalidad/región/conservación/obligaciones). - Aceptación de Términos del Producto de Datos (formación del contrato).

Comprobaciones mínimas en el momento del acceso: - ID de contrato válido y vinculación al acuerdo negociado. - Ejecución de restricciones técnicas disponibles para el conector (por ejemplo, restricciones de punto de conexión, ventanas temporales). - Emisión de eventos de obligación (eventos LOG) a la canalización de auditoría.

6.4 Gestión de cambios de política (con disparadores explícitos de revisión legal)

Los cambios de política son sensibles porque afectan directamente a la ejecutabilidad y a las expectativas contractuales.

Disparadores de cambio que requieren revisión LCC (mínimo): - Nuevo valor de finalidad o ampliación del alcance de finalidad. - Nuevo valor de región/geocerca, o cualquier expansión transfronteriza más allá de la línea base UE. - Ampliación de la ventana de conservación más allá de los valores predeterminados de línea base. - Introducción de datos personales o aumento del riesgo de identificabilidad (disparador de DPIA). - Adición/eliminación de emisores de confianza o cambio de alcances de credenciales.

[35] W3C, *ODRL Information Model 2.2*.

[36] International Data Spaces Association, *Dataspace Protocol*.

[37] Eclipse Foundation, *Eclipse Dataspace Protocol, 2025-1*.

Pasos de cambio: 1. Solicitud de cambio con justificación y productos afectados. 2. Evaluación de impacto (LCC + TIC), incluidas ventanas de migración y deprecación. 3. Pruebas preproducción de políticas en conectores (TIC). 4. Aprobación del Consejo de Gobernanza y publicación versionada del registro de políticas. 5. Comunicación, fecha de efecto y verificación de ejecución.

6.5 Respuesta a incidentes y revocación (brecha de política o confianza)

El operador debe responder a claves comprometidas, conectores con comportamiento indebido o infracciones de política.

Libro de operaciones mínimo: 1. Triaje y contención (pausar negociaciones; bloquear rutas de acceso). 2. Preservación de evidencia (exportar registros de auditoría; preservar resúmenes hash). 3. Revocación/rotación (acción del emisor + actualización de registro). 4. Notificación (participantes y, cuando corresponda, autoridades supervisoras). 5. Revisión postincidente y acciones correctivas (TIC/LCC/GB).

6.6 Resolución de disputas y reclamaciones

SDS mantiene un canal de disputas previsible para términos, denegaciones de acceso y presuntas infracciones de política: - Recepción -> recopilación de evidencia -> mediación por DSAu -> escalado a GB (decisión vinculante) -> seguimiento de remediación por AAF.

6.7 Promoción de estándares, relaciones y datos de referencia

E6 gobierna la promoción de evidencia de estándares de sostenibilidad y líneas base técnicas a productos de datos SDS. Este proceso cubre admisión de evidencia de estándares, relaciones revisadas entre estándares, semántica de unidades/conversiones, contratos de cálculo y procedencia de datos de referencia.

Controles mínimos de gobernanza: - La admisión de evidencia de estándares debe distinguir el denominador del estándar oficial, la representación técnica SDS, la evidencia de validación y la ausencia o presencia de valores operativos de empresa. Un paquete estructural de estándares no se trata como paquete de envío de valores salvo que existan filas de valor y metadatos a nivel de valor. - La promoción de relaciones debe usar registros de relación tipados y evidenciados. La equivalencia exacta, el alcance más amplio/más estrecho, el componente, la transformación, el contexto de apoyo, la ausencia de coincidencia y los estados pendientes de revisión se gobiernan por separado para que SDS no cree falsas equivalencias entre estándares. - Las relaciones con estándares ausentes permanecen en cuarentena fuera del comportamiento en vivo hasta que el estándar referenciado esté instalado y revisado. Las relaciones pendientes no pueden dirigir mapeo, cálculo, búsqueda, exportación ni comportamiento de presentación de información. - La promoción de unidades, conversiones y datos de referencia debe registrar fuente, versión, periodo efectivo, semántica de unidad, política de conversión y marcadores no convertibles. Las etiquetas de unidad que representan marcadores de presentación de información o denominadores específicos de organización no deben convertirse silenciosamente como unidades físicas. - Los contratos de cálculo deben definir dependencias de componentes, unidades esperadas, entradas externas en tiempo de ejecución y metadatos de valor requeridos antes de su uso operativo. - Los datos de

muestra y los flujos guiados de recorrido deben permanecer separados de la evidencia operativa, la evidencia de auditoría y los envíos de valores con calidad de producción.

Resultados de evidencia: - Registro de gobernanza de evidencia de estándares. - Registro de publicación de relaciones revisadas. - Registro de gobernanza de unidades, conversiones y datos de referencia. - Registro de límite de cálculo y valores operativos.

7. Modelo de políticas y control de uso (ODRL → ejecución por conector)

E6 trata el control de uso como una característica de gobernanza de primer nivel: cada producto de datos debe tener IDs de política y términos contractuales explícitos, y cada decisión de acceso debe quedar registrada. ODRL aporta el vocabulario conceptual (permisos, prohibiciones, deberes) usado para estructurar políticas, mientras SDS mantiene un vocabulario controlado para que las políticas sean implementables entre conectores.[38]

7.1 Modelo de políticas (línea base SDS)

Las políticas SDS se expresan usando cuatro dimensiones ejecutables: - Limitación de la finalidad (vocabulario controlado; véase registro de políticas). - Geocerca/jurisdicción (códigos de región; línea base UE para contextos regulados). - Ventana de conservación (P30D…P730D) como restricción máxima de conservación. - Obligaciones/deberes (LOG, delete-after, notify, aggregate-only, etc.).

Las políticas se referencian mediante valores policyId estables definidos en la capa de evidencia del registro de políticas SDS.

7.2 Qué se ejecuta y cuándo (negociación vs acceso)

Ejecución en tiempo de negociación (antes del contrato): - Verificar credenciales del consumidor (confianza del emisor + estado + alcances de rol). - Verificar que la finalidad declarada y la región solicitada son compatibles con los IDs de política del producto. - Verificar que el consumidor acepta los deberes (registro, conservación, borrado) como condición de formación del contrato.

Ejecución en tiempo de acceso (durante transferencia / llamada API): - Verificar un ID de contrato válido y vinculación al acuerdo negociado. - Ejecutar restricciones técnicas disponibles para el conector (por ejemplo, alcance del punto de conexión; validez de token; límites de tasa). - Emitir eventos de obligación (LOG) y señales de integridad (hash de conjunto de datos) a la traza de auditoría.

[38] W3C, *ODRL Information Model 2.2.*

7.3 Ejemplo concreto (extremo a extremo)

Ejemplo: publicar el registro de conjuntos de datos E1 como producto de datos restringido para presentación de información dentro de la UE durante un máximo de 365 días, con registro obligatorio de acceso.

- Los términos del producto de datos adjuntan policy-reporting-365d-retention y policy-geofence-eu.
- El consumidor solicita acceso declarando purpose=reporting y region=EU.
- El conector del proveedor evalúa las políticas en la negociación; si el resultado es correcto, concluye un contrato y habilita el acceso.
- Cada acceso emite un evento de log de auditoría que incluye policyId, purpose, contractId y datasetHash (sección 9).

Expresión ilustrativa estilo ODRL (el paquete de evidencia de gobernanza contiene los ejemplos completos):

```
permission:
  action: use
  constraint:
    - leftOperand: purpose
      operator: eq
      rightOperand: reporting
    - leftOperand: region
      operator: in
      rightOperand: [EU]
  duty:
    - action: logUse
    - action: deleteAfter
      constraint:
        - leftOperand: retention
          operator: lte
          rightOperand: P365D
```

7.4 KPIs de control de uso (piloto)

Estos KPIs se miden de forma continua durante el piloto y se reportan al Consejo de Gobernanza:

- KPI-UC-01 Adopción de políticas: ≥90% de los productos de datos publicados tienen ≥1 policyId adjunto.
- KPI-UC-02 Cobertura de ejecución: el 100% de las negociaciones de acceso incluye un resultado registrado de evaluación de política.

- KPI-UC-03 Cobertura de auditoría: ≥99% de los accesos correctos producen un evento LOG con los campos requeridos (sección 9.1).
- KPI-UC-04 Cumplimiento de deberes: ≥95% de los deberes requeridos (LOG, confirmaciones delete-after cuando aplique) quedan registrados.
- KPI-UC-05 Propagación de políticas: los cambios del registro de políticas se hacen efectivos en todos los conectores en <15 minutos (medidos en pruebas escenificadas).
- KPI-UC-06 Infracciones: 0 infracciones de política sin resolver; cualquier infracción tiene contención en <4 horas (véase KPI-IR-01).
- KPI-UC-07 Tiempo hasta política: crear+aprobar+publicar un nuevo ID de política en ≤10 días laborables (cadencia GB con vía de emergencia).

Evidencia: - Evidencia del registro de políticas. - Evidencia de Términos del Producto de Datos. - Evidencia de ejemplos de control de uso.

8. Identidad y confianza (SSI/VC) — modelo operativo

SDS usa Verifiable Credentials (VC) y Decentralized Identifiers (DID) de W3C para respaldar decisiones de confianza federada que son portables entre participantes y no dependen de un único proveedor central de identidad.[39] [40]

Este diseño se alinea con las expectativas europeas de espacios de datos sobre confianza federada y puede alinearse con la evolución de la modificación eIDAS / marco europeo de identidad digital.[41] También complementa la señalización de cumplimiento al estilo Gaia-X (por ejemplo, emisión de credenciales que acreditan resultados de validación).[42]

8.1 Conjunto mínimo de credenciales (línea base piloto)

SDS define un conjunto mínimo de credenciales para que la incorporación y la ejecución sean auditables:

- **OrgIdentityCredential** — acredita la identidad de la entidad jurídica (KYB/KYC verificado por emisor, según corresponda).
- **SDSRoleCredential** — vincula un DID de conector a roles (proveedor/consumidor/auditor) y alcances de finalidad permitidos.
- **(Opcional) ConnectorConformanceCredential** — acredita que una instancia de conector superó un perfil de conformidad (emitida por TIC o por tercero).

[39] W3C, *Verifiable Credentials Data Model v2.0*.

[40] W3C, *Decentralized Identifiers (DIDs) v1.0*.

[41] Parlamento Europeo y Consejo, *Reglamento (UE) 2024/1183 por el que se modifica el Reglamento (UE) n.° 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital*, Diario Oficial de la Unión Europea, 2024, https://eur-lex.europa.eu/eli/reg/2024/1183?locale=ES.

[42] Gaia-X European Association for Data and Cloud AISBL, *Gaia-X Trust Framework 22.10*.

8.2 Presentación y verificación

Cuando estén disponibles, los flujos de emisión y presentación pueden estandarizarse usando OpenID4VCI / OpenID4VP.[43] [44]

Requisitos mínimos de verificación en el momento de la negociación: - Validación de firma y vinculación del titular. - Validación de confianza del emisor frente al registro de emisores de confianza. - Verificación de estado de credencial (revocación/suspensión) usando un mecanismo estándar como Bitstring Status List.[45] - Comprobaciones de claims: los alcances de rol y finalidad coinciden con el contrato solicitado y los IDs de política.

8.3 Gobernanza de emisores de confianza

El operador mantiene un registro de emisores de confianza con control de versiones, política de rotación y control de cambios.

Los cambios de emisor (alta, baja, cambios de alcance) son acciones controladas por GB porque afectan directamente a quién puede participar en el espacio de datos.

Evidencia: - Evidencia de gobernanza de emisores de confianza. - Evidencia de flujo de incorporación y acceso.

9. Auditabilidad y trazabilidad

La auditabilidad es un requisito del entregable porque es la base del aseguramiento, la resolución de disputas y la confianza del sector público. Por ello, SDS define una línea base mínima de evidencia de auditoría que puede implementarse de forma consistente entre conectores y dominios.

9.1 Campos mínimos del log de auditoría

Tabla 9 Auditabilidad y trazabilidad

CAMPO	FINALIDAD
timestamp_utc	Cronología y secuenciación de evidencia
provider_connector_id / consumer_connector_id	Trazabilidad entre partes
subject_org_id (o DID del sujeto)	Responsabilidad
issuer_id	Evidencia del anclaje de confianza utilizado
contract_id	Vincular negociación con acceso posterior
data_product_id	Vincular con entrada de catálogo y términos
purpose + policy_ids[]	Limitación de la finalidad y condiciones aplicadas

[43] OpenID Foundation, *OpenID for Verifiable Credential Issuance*.

[44] OpenID Foundation, *OpenID for Verifiable Presentations*.

[45] W3C, *Bitstring Status List*.

CAMPO	FINALIDAD
decision (permit/deny) + reason_code	Explicabilidad de la ejecución
obligations[] (emitidas/cumplidas)	Seguimiento de deberes (LOG, delete-after, notify)
dataset_hash / version_hash	Evidencia de integridad
request_id / correlation_id	Trazabilidad entre sistemas/canalizaciones de registros

9.2 Evidencia de inalterabilidad

SDS requiere que los registros de auditoría sean de solo anexado, encadenados por resúmenes hash, o ambas cosas, de modo que la evidencia no pueda alterarse silenciosamente. La conservación de los registros de auditoría sigue el deber de conservación aplicable más estricto adjunto al contrato (véanse las ventanas de conservación del registro de políticas) y es revisada por LCC para alinearse con la limitación de conservación del RGPD.[46]

9.3 Ciclo de aseguramiento (piloto)

Acciones mínimas de aseguramiento: - Monitorización continua de decisiones de acceso y eventos de obligación (DSAu). - Revisión trimestral de gobernanza de KPIs e incidentes (GB). - Revisión periódica de cumplimiento (LCC), incluidos cambios del registro de políticas y del registro de emisores. - Auditoría/evaluación independiente (AAF) con la cadencia acordada en el piloto (al menos una vez al año, o tras un incidente mayor).

9.4 Paquete de evidencia (lo que reciben los auditores)

Para un producto y periodo determinados, SDS puede producir un paquete de evidencia que contenga: - Los Términos del Producto de Datos aplicables (versionados) y sus policyIds adjuntos. - Una muestra de registros de auditoría con prueba de cadena de resúmenes hash (o prueba de almacenamiento de solo anexado). - Las versiones de registro pertinentes (registro de políticas, registro de emisores de confianza). - Informes de incidentes (si los hay) y estado de remediación. - Un registro de cambios de modificaciones de política/emisor que afecten al producto.

10. Mapeo regulatorio (línea base UE)

Esta sección mapea los controles de gobernanza SDS a expectativas regulatorias de la UE. Se proporciona para transparencia y aseguramiento del proyecto; no constituye asesoramiento jurídico.

[46] Parlamento Europeo y Consejo, *Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*.

10.1 Mapeo resumido (instrumento -> controles operativos -> evidencia)

Tabla 10 Mapeo regulatorio (línea base UE)

INSTRUMENTO	REQUISITOS CLAVE RELEVANTES PARA SDS	CONTROLES OPERATIVOS (LO QUE IMPLEMENTA SDS)	EVIDENCIA
RGPD (UE) 2016/679[47]	Art. 5 (limitación de la finalidad, minimización, limitación de conservación, responsabilidad); art. 6 (licitud); art. 25 (privacidad desde el diseño); art. 32 (seguridad); art. 33/34 (notificación de brechas)	policylds controlados por finalidad; ventanas de conservación; incorporación con alcances de rol; registro de acceso y evidencia de inalterabilidad; libro de operaciones de respuesta a incidentes; disparadores de revisión DPIA/legal	Evidencia del registro de políticas; evidencia de Términos del Producto de Datos; campos de auditoría de la sección 9; proceso de incidentes de la sección 6.5
Reglamento de Gobernanza de Datos (UE) 2022/868[48]	Condiciones para servicios de intermediación de datos (neutralidad, transparencia, no discriminación); gobernanza para la reutilización de datos protegidos del sector público (cuando aplique)	Modelo de gobernanza con neutralidad y separación de funciones; transparencia sobre condiciones de acceso; ruta de resolución de disputas; línea base de auditabilidad	Secciones 4-6; proceso de disputas de la sección 6.6; versionado de registros de políticas/emisores
Reglamento de Datos (UE) 2023/2854[49]	Términos justos, razonables y no discriminatorios (FRAND) en contextos relevantes; transparencia de condiciones de acceso; expectativas de interoperabilidad y cambio de proveedor (cuando aplique)	Términos del Producto de Datos estandarizados; condiciones de acceso transparentes; versionado/deprecación previsible; consideraciones de portabilidad/cambio capturadas en el flujo de disputas	Evidencia de Términos del Producto de Datos; ciclo de vida de la sección 6.2; disputas de la sección 6.6
modificación eIDAS / marco europeo de identidad digital (UE) 2024/1183[50]	Orientación del marco europeo de identidad digital; servicios de confianza transfronterizos	Enfoque de incorporación VC/DID compatible con perfiles de cartera EUDI; gobernanza de emisores y comprobaciones de	Modelo de identidad de la sección 8; evidencia de gobernanza de emisores de confianza

[47] Parlamento Europeo y Consejo, *Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*.

[48] Parlamento Europeo y Consejo, *Reglamento (UE) 2022/868 relativo a la gobernanza europea de datos*.

[49] Parlamento Europeo y Consejo, *Reglamento (UE) 2023/2854 sobre normas armonizadas para un acceso justo a los datos y su utilización*.

[50] Parlamento Europeo y Consejo, *Reglamento (UE) 2024/1183 por el que se modifica el Reglamento (UE) n.° 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital*.

INSTRUMENTO	REQUISITOS CLAVE RELEVANTES PARA SDS	CONTROLES OPERATIVOS (LO QUE IMPLEMENTA SDS)	EVIDENCIA
		estado	

Nota de riesgo legal (disciplina de redacción): los controles SDS se describen como mecanismos que *apoyan* el cumplimiento y *permiten* una gobernanza auditable; no garantizan el cumplimiento legal sin evaluación específica de contexto y revisión legal.

10.2 Directrices éticas y uso responsable

Estas directrices complementan el mapeo jurídico. Definen decisiones de gobernanza para pilotos y productos de datos; no se presentan como controles automatizados ya ejecutados por el runtime.

PRINCIPIO	DIRECTRIZ SDS	RESPONSABLE	EVIDENCIA
No discriminación	No producir trato discriminatorio directo o indirecto; evaluar impactos diferenciados.	Órgano de gobernanza y responsable ético/legal	Evaluación de impacto y decisión documentada.
Proporcionalidad y minimización	Compartir y conservar solo datos necesarios para la finalidad aprobada.	Responsable del dato y privacidad	Finalidad, campos, conservación y justificación.
Calidad y sesgo	Hacer visibles procedencia, cobertura, incertidumbre, ausencias y sesgos.	Responsable de calidad y custodio semántico	Perfil de calidad y limitaciones.
Explicabilidad y revisión humana	Explicar cálculos y relaciones; decisiones materiales requieren revisión humana competente.	Propietario del producto y actor decisor	Traza y constancia de revisión.
Reclamación y reparación	Permitir impugnación, corrección y retirada.	Secretaría de gobernanza	Ticket, decisión y corrección.
Usos prohibidos	Prohibir reidentificación, usos ajenos a finalidad, equivalencias no evidenciadas y decisiones automatizadas no autorizadas.	Órgano de gobernanza	Catálogo de usos prohibidos y denegaciones.

En cada piloto, la plantilla del producto de datos debe indicar qué directrices aplican, quién responde de ellas y qué evidencia permite comprobarlas. La ausencia de esa información bloquea la promoción del producto a intercambio operativo.

11. Controles de aceptación e indicadores clave de rendimiento (E6)

E6 se considera “entregable-completo” cuando (a) la evidencia de gobernanza requerida existe y es internamente consistente, y (b) el piloto define cómo se medirán los indicadores operativos. Durante el piloto, los indicadores se evalúan frente a umbrales y se comunican a GB.

La verificación estática se realiza mediante las puertas de validación de gobernanza E6, conformidad, paquete de conector y paquete de evidencia. La verificación estática no sustituye la evidencia piloto para las puertas de KPIs operativos.

11.1 Puertas de artefactos (preparación estática)

Tabla 11 Controles de aceptación e indicadores clave de rendimiento (E6)

PUERTA	UMBRAL	EVIDENCIA	ESTADO (2026-06-08)
G6-A1 Registro de políticas	JSON legible por máquina con denegación por defecto y vocabularios de finalidad/región/conservación	Evidencia del registro de políticas más validación de esquema	PASS
G6-A2 Plantilla de términos del producto de datos	La plantilla de términos referencia IDs de política, justificación de base jurídica y campos de auditoría	Evidencia de Términos del Producto de Datos	PASS
G6-A3 Ejemplos de control de uso	La política de ejemplo incluye mapeo finalidad+región+conservación+deber (ODRL->política de conector)	Evidencia de ejemplos de control de uso	PASS
G6-A4 Registro de emisores de confianza	JSON legible por máquina con cumplimiento de Bitstring Status List 2025	Evidencia de gobernanza de emisores de confianza	PASS
G6-A5 Flujo de incorporación	El flujo de incorporación documenta vinculación DID/VC y comprobaciones de estado	Evidencia de flujo de incorporación y acceso	PASS
G6-A6 RACI del modelo operativo	Asignaciones explícitas de rol con control de cambios y respuesta a incidentes	Evidencia del modelo operativo	PASS
G6-A7 Esquema de eventos de auditoría	JSON Schema con 22 tipos de evento, identificadores de correlación e integridad mediante cadena hash	Evidencia del esquema de eventos de auditoría	PASS
G6-A8 Perfil de vinculación de finalidad	Vocabulario controlado, reglas de validación y códigos de error	Evidencia de vinculación de finalidad	PASS
G6-A9 Ejecución de conservación	Periodos de conservación, patrones de deber ODRL y eventos de evidencia de borrado	Evidencia de ejecución de conservación	PASS
G6-A10 Matriz de vinculación legal	Mapea restricciones de política a artículos del RGPD/Reglamento de	Evidencia de vinculación	PASS

PUERTA	UMBRAL	EVIDENCIA	ESTADO (2026-06-08)
	Datos	jurídico-técnica	
G6-A11 Líneas base de gobernanza	Controles de aceptación entre entregables con evidencia de validación	Evidencia de controles de aceptación	PASS
G6-A12 Paquete de políticas de conector	La evidencia de políticas, activos y definiciones contractuales EDC se alinea con el registro de entregas	Evidencia del paquete de políticas de conector que cubre 1,805 activos y 1,805 definiciones contractuales	PASS
G6-A13 Gobernanza de evidencia de estándares	Las líneas base de estándares oficiales y la evidencia de granularidad de indicadores controlada se promueven solo con alcance, validación y estado de límite de valores	Registro de gobernanza de evidencia de estándares	PASS
G6-A14 Gobernanza de publicación de relaciones	Las relaciones revisadas están tipadas, evidenciadas y separadas de registros pendientes o con estándar ausente	Registro de publicación de relaciones	PASS
G6-A15 Gobernanza de unidades, conversiones y datos de referencia	La semántica de unidades, marcadores no convertibles, reglas de conversión, procedencia de fuente y periodos efectivos se registran antes de la promoción	Registro de gobernanza de unidades, conversiones y datos de referencia	PASS
G6-A16 Límite de cálculo y valores operativos	Las dependencias de componentes, entradas externas en tiempo de ejecución, unidades esperadas y metadatos a nivel de valor son explícitos antes del uso operativo	Registro de límite de cálculo y valores operativos	PASS

11.1.1 Puertas de validación técnica

Tabla 12 Controles de aceptación e indicadores clave de rendimiento (E6)

PUERTA	UMBRAL	EVIDENCIA DE VALIDACIÓN	ESTADO (2026-06-08)
G6-T1 Denegación por defecto	Todas las políticas ejecutan denegación por defecto; no hay patrones de permitir todo	Validación estática de gobernanza	PASS
G6-T2 Pruebas de conformidad	32 pruebas de conformidad pasan para conformidad de gobernanza más el comprobador estricto de gobernanza	Suite de pruebas de conformidad y comprobador estricto de gobernanza	PASS
G6-T3 Enlaces de política NGSI-LD	Las exportaciones incluyen relaciones hasPolicy	La evidencia de exportación NGSI-LD	PASS

PUERTA	UMBRAL	EVIDENCIA DE VALIDACIÓN	ESTADO (2026-06-08)
		incluye relaciones de política	
G6-T4 Auditoría -> NGSI-LD	Eventos de auditoría convertibles a entidades NGSI-LD	Evidencia de conversión de eventos de auditoría	PASS
G6-T5 Paquete de evidencia	Generación automatizada de paquete de evidencia que cubre 24 artefactos de gobernanza	Evidencia de generación de paquete de evidencia	PASS
G6-T6 Consistencia del paquete EDC	1,805 activos y 1,805 definiciones contractuales se generan desde el registro de entregas bajo políticas de denegación por defecto	Evidencia de consistencia del paquete de conector para 1,805 activos y 1,805 definiciones contractuales	PASS
G6-T7 Gobernanza de línea base técnica SDS	E6 cubre admisión de evidencia de estándares, publicación de relaciones, gobernanza de unidades/conversiones/datos de referencia, contratos de cálculo y separación muestra/operacional	Validación de contenido E6	PASS

11.2 Controles de indicadores operativos (evaluación piloto)

Tabla 13 Controles de aceptación e indicadores clave de rendimiento (E6)

PUERTA	UMBRAL (OBJETIVO PILOTO)	MÉTODO DE MEDICIÓN	EVIDENCIA
G6-O1 Tiempo de ciclo de incorporación	Tiempo medio de incorporación ≤ 24h (tras completar KYB/KYC)	Seguir N casos de incorporación extremo a extremo	Logs de incorporación + marcas temporales de emisión de credenciales
G6-O2 Cobertura de ejecución de políticas	El 100% de las negociaciones registra resultado de evaluación de política	Muestreo de registros de auditoría + comprobaciones automatizadas	Registros de auditoría con decisión + IDs de política
G6-O3 Integridad de auditoría	≥99% de los accesos correctos emiten eventos LOG con campos requeridos	Comparar eventos de acceso con eventos de registro	Registros de auditoría + registros de solicitudes de acceso
G6-O4 Propagación de políticas	Cambio de registro efectivo en conectores en <15 min (prueba escenificada)	Prueba controlada de actualización de políticas	Registro de cambios + registros de ejecución antes/después

PUERTA	UMBRAL (OBJETIVO PILOTO)	MÉTODO DE MEDICIÓN	EVIDENCIA
G6-O5 Contención de incidentes	Contención de incidente crítico en <4h (ejercicio de mesa)	Libro de operaciones de ejercicio de incidentes + cronómetro	Informe de ejercicio de incidentes + extractos de registros
G6-O6 SLA de resolución de disputas	Respuesta inicial ≤5 días laborables; resolución ≤30 días laborables	Seguir tickets de disputa	Registro de disputas + decisiones

Estos indicadores están diseñados para ser medibles y estar respaldados por evidencia; pueden endurecerse tras la calibración piloto.

12. Limitaciones y preguntas abiertas

A tratar con partes interesadas y asesoría jurídica durante la implementación:

- En qué circunstancias SDS (o el operador) califica como “servicio de intermediación de datos” bajo el Reglamento de Gobernanza de Datos, y qué registros/controles adicionales podrían aplicar.
- Cómo gestionar el tratamiento transfronterizo más allá de la geocerca UE para escenarios piloto específicos (adecuación, SCCs, cláusulas contractuales), y cómo se codifican dichas excepciones en IDs de política.
- El perfil mínimo de conformidad de conectores para el piloto SDS (línea base de seguridad, SLA de parcheo, campos de auditoría obligatorios, reenvío de registros).
- Qué emisor(es) se usarán en producción, qué nivel de aseguramiento se requiere y cómo se alinea la gobernanza de emisores con las expectativas del sector público.
- Cómo se ejecutan y evidencian técnicamente de extremo a extremo los deberes de “conservación” y “delete-after” (eventos de confirmación de obligación, auditorías).
- Qué umbrales de promoción a producción y reglas de rollback deben aplicarse cuando relaciones revisadas, datos de referencia o políticas de conversión se actualicen tras la calibración piloto.
- Qué campos de metadatos a nivel de valor pasan a ser obligatorios para los envíos de valores piloto antes de que los contratos de cálculo se usen como evidencia operativa.

Anexo A — Índice de evidencia (evidencia de gobernanza)

Este anexo enumera las categorías clave de evidencia de gobernanza referenciadas en E6. La capa de validación ejecutable sigue formando parte de la puerta de gobernanza del proyecto y del registro de entregables, mientras este anexo público mantiene la superficie de evidencia conceptual y revisable.

Tabla 14 Anexo A — Índice de evidencia (evidencia de gobernanza)

ÁREA	CATEGORÍA DE EVIDENCIA	FINALIDAD	USADO EN SECCIONES
Registro de políticas	Evidencia del registro de políticas	Políticas legibles por máquina con ODRL + denegación por defecto	6, 7, 10, 11
Esquema de políticas	Evidencia de esquema de políticas	JSON Schema para validación del registro de políticas	7, 11
Vinculación legal	Evidencia de vinculación jurídico-técnica	Mapea restricciones a artículos del RGPD/Reglamento de Datos	7, 10
Vinculación de finalidad	Evidencia de vinculación de finalidad	Perfil de ejecución de limitación de la finalidad	7
Ejecución de conservación	Evidencia de ejecución de conservación	Perfil de ejecución de obligaciones de conservación	7, 10
Términos del producto de datos	Evidencia de Términos del Producto de Datos	Plantilla de términos con políticas adjuntas	6, 7, 10, 11
Ejemplos de control de uso	Evidencia de ejemplos de control de uso	Ejemplos de restricciones/deberes de política	7
Modelo operativo	Evidencia del modelo operativo	RACI + control de cambios + respuesta a incidentes	5, 6
Registro de emisores de confianza	Evidencia de gobernanza de emisores de confianza	Registro de emisores legible por máquina con Bitstring Status List 2025	6, 8, 11
Esquema de eventos de auditoría	Evidencia del esquema de eventos de auditoría	JSON Schema para eventos de auditoría (22 tipos)	9
Flujo de incorporación	Evidencia de flujo de incorporación y acceso	Incorporación VC/DID y flujo de acceso	6, 8
Controles de aceptación	Evidencia de controles de aceptación	Umbrales + evidencia de validación	11
Gobernanza de evidencia de estándares	Registro de gobernanza de evidencia de estándares	Denominador de estándar oficial, representación técnica SDS, estado de validación y estado de límite de	3, 5, 6, 11

ÁREA	CATEGORÍA DE EVIDENCIA	FINALIDAD	USADO EN SECCIONES
		valores	
Publicación de relaciones	Registro de gobernanza de publicación de relaciones	Tipo de relación de mapeo revisada, evidencia, estado de compatibilidad, estado de cuarentena y decisión de publicación	3, 5, 6, 11
Unidades/conversiones/datos de referencia	Registro de gobernanza de unidades, conversiones y datos de referencia	Semántica de unidades, política de conversión, marcadores no convertibles, procedencia, versión y periodo efectivo	3, 5, 6, 11
Límite de cálculo/valores	Registro de límite de cálculo y valores operativos	Dependencias de componentes, entradas externas en tiempo de ejecución, unidades esperadas y requisitos de metadatos a nivel de valor	3, 5, 6, 11

Anexo A.1 — Paquete de evidencia de validación

Tabla 15 Anexo A — Índice de evidencia (evidencia de gobernanza)

CAPA DE VALIDACIÓN	FINALIDAD	EVIDENCIA PRODUCIDA
Validación de artefactos de gobernanza	Valida artefactos de gobernanza, registros de políticas, emisores de confianza, consistencia del paquete de conector y referencias del entregable.	Resultado estático de preparación de gobernanza.
Generación del paquete de políticas de conector	Genera evidencia de políticas, activos y definiciones contractuales desde el registro de entregas.	1,805 activos y 1,805 definiciones contractuales bajo políticas de denegación por defecto.
Generación de paquete de evidencia	Genera un paquete de revisión para auditores y gobernanza del proyecto.	Cobertura de evidencia para 24 artefactos de gobernanza.
Conversión de eventos de auditoría	Convierte eventos de auditoría en entidades compatibles con NGSI-	Evidencia de auditabilidad para eventos de acceso, política, conservación, borrado e incidente.

CAPA DE VALIDACIÓN	FINALIDAD	EVIDENCIA PRODUCIDA
	LD.	
Ejecución de políticas y conformidad de gobernanza	Prueba la evaluación de políticas y el comportamiento de conformidad de gobernanza.	32 pruebas de conformidad más validación estricta de gobernanza.

Referencias

- Data Spaces Support Centre. *Data Spaces Blueprint v2.0*. 2025. https://dssc.eu/space/BVE2/1071251516/Data+Spaces+Blueprint+v2.0.[51]
- Eclipse Foundation. *Eclipse Dataspace Protocol, 2025-1*. 2025. https://eclipse-dataspace-protocol-base.github.io/DataspaceProtocol/2025-1/.[52]
- ETSI. *ETSI GS CIM 009: NGSI-LD API*. 2024. https://cim.etsi.org/NGSI-LD/official/front-page.html.[53]
- Comisión Europea. *Reglamento Delegado (UE) 2023/2772 de la Comisión, de 31 de julio de 2023, por el que se completa la Directiva 2013/34/UE en lo que respecta a las normas de presentación de información sobre sostenibilidad*. 2023. https://eur-lex.europa.eu/eli/reg_del/2023/2772/oj.[54]
- Comisión Europea, SEMIC. *DCAT-AP 3.0.0*. 2024. https://semiceu.github.io/DCAT-AP/releases/3.0.0/.[55]
- Parlamento Europeo y Consejo. *Directiva (UE) 2022/2464 en lo que respecta a la presentación de información sobre sostenibilidad por parte de las empresas*. 2022. https://eur-lex.europa.eu/eli/dir/2022/2464/oj.[56]
- Parlamento Europeo y Consejo. *Reglamento (UE) 2016/679 relativo a la protección de datos personales y a la libre circulación de estos datos*. 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj.[57]
- Parlamento Europeo y Consejo. *Reglamento (UE) 2022/868 relativo a la gobernanza europea de datos*. 2022. https://eur-lex.europa.eu/eli/reg/2022/868/oj.[58]
- Parlamento Europeo y Consejo. *Reglamento (UE) 2023/2854 sobre normas armonizadas para un acceso justo a los datos y su utilización*. 2023. https://eur-lex.europa.eu/eli/reg/2023/2854/oj.[59]

[51] Data Spaces Support Centre, *Data Spaces Blueprint v2.0*.

[52] Eclipse Foundation, *Eclipse Dataspace Protocol, 2025-1*.

[53] European Telecommunications Standards Institute, *ETSI GS CIM 009: NGSI-LD API*.

[54] Comisión Europea, *Reglamento Delegado (UE) 2023/2772 por el que se completa la Directiva 2013/34/UE en lo que respecta a las normas de presentación de información sobre sostenibilidad*.

[55] European Commission, SEMIC, *DCAT-AP 3.0.0*.

[56] Parlamento Europeo y Consejo, *Directiva (UE) 2022/2464 por lo que respecta a la presentación de información sobre sostenibilidad por parte de las empresas*.

[57] Parlamento Europeo y Consejo, *Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*.

[58] Parlamento Europeo y Consejo, *Reglamento (UE) 2022/868 relativo a la gobernanza europea de datos*.

[59] Parlamento Europeo y Consejo, *Reglamento (UE) 2023/2854 sobre normas armonizadas para un acceso justo a los datos y su utilización*.

- Parlamento Europeo y Consejo. *Reglamento (UE) 2024/1183 por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital*. 2024. https://eur-lex.europa.eu/eli/reg/2024/1183/oj.[60]
- Gaia-X European Association for Data and Cloud AISBL. *Gaia-X Trust Framework 22.10*. 2022. https://docs.gaia-x.eu/policy-rules-committee/trust-framework/22.10/.[61]
- Global Reporting Initiative. *GRI Standards: full set of GRI Standards*. Ámsterdam: Global Reporting Initiative, 2025. https://www.globalreporting.org/standards/gri-standards-download-center/gri-standards/.[62]
- Greenhouse Gas Protocol. *Corporate Value Chain (Scope 3) Accounting and Reporting Standard*. World Resources Institute y World Business Council for Sustainable Development, 2011. https://ghgprotocol.org/corporate-value-chain-scope-3-standard.[63]
- Greenhouse Gas Protocol. *The Greenhouse Gas Protocol: A Corporate Accounting and Reporting Standard, revised edition*. World Resources Institute y World Business Council for Sustainable Development. https://ghgprotocol.org/corporate-standard.[64]
- International Data Spaces Association. *Dataspace Protocol*. 2025. https://docs.internationaldataspaces.org/ids-knowledgebase/dataspace-protocol.[65]
- OpenID Foundation. *OpenID for Verifiable Credential Issuance*. 2025. https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.[66]
- OpenID Foundation. *OpenID for Verifiable Presentations*. 2025. https://openid.net/specs/openid-4-verifiable-presentations-1_0.html.[67]
- W3C. *Bitstring Status List*. 2025. https://www.w3.org/TR/vc-bitstring-status-list/.[68]
- W3C. *Decentralized Identifiers (DIDs) v1.0*. 2022. https://www.w3.org/TR/did-core/.[69]
- W3C. *ODRL Information Model 2.2*. 2018. https://www.w3.org/TR/odrl-model/.[70]
- W3C. *Verifiable Credentials Data Model v2.0*. 2025. https://www.w3.org/TR/vc-data-model-2.0/.[71]

[60] Parlamento Europeo y Consejo, *Reglamento (UE) 2024/1183 por el que se modifica el Reglamento (UE) n.° 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital*.

[61] Gaia-X European Association for Data and Cloud AISBL, *Gaia-X Trust Framework 22.10*.

[62] Global Reporting Initiative, *Estándares GRI: traducción al español y conjunto consolidado de Estándares GRI*.

[63] World Resources Institute and World Business Council for Sustainable Development, *Corporate Value Chain (Scope 3) Accounting and Reporting Standard*.

[64] World Resources Institute and World Business Council for Sustainable Development, *The Greenhouse Gas Protocol: A Corporate Accounting and Reporting Standard*.

[65] International Data Spaces Association, *Dataspace Protocol*.

[66] OpenID Foundation, *OpenID for Verifiable Credential Issuance*.

[67] OpenID Foundation, *OpenID for Verifiable Presentations*.

[68] W3C, *Bitstring Status List*.

[69] W3C, *Decentralized Identifiers (DIDs) v1.0*.

[70] W3C, *ODRL Information Model 2.2*.

[71] W3C, *Verifiable Credentials Data Model v2.0*.

Comisión Europea. *Reglamento Delegado (UE) 2023/2772 por el que se completa la Directiva 2013/34/UE en lo que respecta a las normas de presentación de información sobre sostenibilidad*. Diario Oficial de la Unión Europea, 2023. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32023R2772.

Data Spaces Support Centre. *Data Spaces Blueprint v2.0*. 2025. https://dssc.eu/space/BVE2/1071251516/Data+Spaces+Blueprint+v2.0.

Eclipse Foundation. *Eclipse Dataspace Protocol, 2025-1*. 2025. https://eclipse-dataspace-protocol-base.github.io/DataspaceProtocol/2025-1/.

European Commission, SEMIC. *DCAT-AP 3.0.0*. 2024. https://semiceu.github.io/DCAT-AP/releases/3.0.0/.

European Telecommunications Standards Institute. *ETSI GS CIM 009: NGSI-LD API*. 2024. https://cim.etsi.org/NGSI-LD/official/front-page.html.

Gaia-X European Association for Data and Cloud AISBL. *Gaia-X Trust Framework 22.10*. 2022. https://docs.gaia-x.eu/policy-rules-committee/trust-framework/22.10/.

Global Reporting Initiative. *Estándares GRI: traducción al español y conjunto consolidado de Estándares GRI*. Amsterdam, 2025. https://www.globalreporting.org/how-to-use-the-gri-standards/gri-standards-spanish-translations/.

International Data Spaces Association. *Dataspace Protocol*. 2025. https://docs.internationaldataspaces.org/ids-knowledgebase/dataspace-protocol.

OpenID Foundation. *OpenID for Verifiable Credential Issuance*. 2025. https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html.

OpenID Foundation. *OpenID for Verifiable Presentations*. 2025. https://openid.net/specs/openid-4-verifiable-presentations-1_0.html.

Parlamento Europeo y Consejo. *Directiva (UE) 2022/2464 por lo que respecta a la presentación de información sobre sostenibilidad por parte de las empresas*. Diario Oficial de la Unión Europea, 2022. https://eur-lex.europa.eu/eli/dir/2022/2464/oj?locale=es.

Parlamento Europeo y Consejo. *Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*. Diario Oficial de la Unión Europea, 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=es.

Parlamento Europeo y Consejo. *Reglamento (UE) 2022/868 relativo a la gobernanza europea de datos*. Diario Oficial de la Unión Europea, 2022. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32022R0868.

Parlamento Europeo y Consejo. *Reglamento (UE) 2023/2854 sobre normas armonizadas para un acceso justo a los datos y su utilización*. Diario Oficial de la Unión Europea, 2023. https://eur-lex.europa.eu/legal-content/es/TXT/?locale=es&uri=CELEX%3A32023R2854.

Parlamento Europeo y Consejo. *Reglamento (UE) 2024/1183 por el que se modifica el Reglamento (UE) n.° 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital*. Diario Oficial de la Unión Europea, 2024. https://eur-lex.europa.eu/eli/reg/2024/1183?locale=ES.

W3C. *Bitstring Status List*. 2025. https://www.w3.org/TR/vc-bitstring-status-list/.

W3C. *Decentralized Identifiers (DIDs) v1.0*. 2022. https://www.w3.org/TR/did-core/.

W3C. *ODRL Information Model 2.2*. W3C Recommendation, 2018. https://www.w3.org/TR/odrl-model/.

W3C. *Verifiable Credentials Data Model v2.0*. 2025. https://www.w3.org/TR/vc-data-model-2.0/.

World Resources Institute, and World Business Council for Sustainable Development. *Corporate Value Chain (Scope 3) Accounting and Reporting Standard*. 2011. https://ghgprotocol.org/corporate-value-chain-scope-3-standard.

World Resources Institute, and World Business Council for Sustainable Development. *The Greenhouse Gas Protocol: A Corporate Accounting and Reporting Standard*. Revised edition. n.d. https://ghgprotocol.org/corporate-standard.