+

Guía de Verificación de Conformidad con especificación UNE 0087:2025

V1 - 17 de noviembre de 2025

Plan de Recuperación, Transformación y Resiliencia

Comisión Europea

Contenido

1. Objeto y ámbito de aplicación

1.1. Objeto del documento

El presente documento propone una guía de verificación de conformidad de un espacio de datos, cuyo propósito es definir los criterios, requisitos y procedimientos necesarios para determinar si una iniciativa puede ser considerada espacio de datos conforme a la Especificación UNE 0087:2025 "Definición y Caracterización de los Espacios de Datos" [1].

El mecanismo constituye un instrumento de verificación técnica y organizativa, orientado a garantizar que los espacios de datos cumplen las condiciones mínimas en materia de gobernanza, interoperabilidad, solución técnica, seguridad, modelo de negocio y operatividad, de acuerdo con los principios de soberanía digital, confianza y generación de valor establecidos en la citada Especificación.

Su finalidad es asegurar una verificación homogénea, objetiva y trazable de las iniciativas que se presentan como espacios de datos, asegurando su alineamiento con la norma UNE 0087:2025. Asimismo, busca facilitar la identificación y el reconocimiento institucional de los espacios de datos conformes, promoviendo su integración en iniciativas nacionales o europeas.

Además, este mecanismo ofrece una base metodológica común que permite utilizar sus resultados en procesos posteriores de validación, auditoría o evaluación de madurez, contribuyendo a reforzar la coherencia y comparabilidad entre los distintos ecosistemas de datos y a fomentar la confianza en la economía del dato.

1.2. Relación con la Especificación UNE 0087:2025

La Especificación UNE 0087:2025 constituye la base normativa y conceptual sobre la que se construye este mecanismo. Cada una de las dimensiones de verfiicación descritas en el presente documento deriva directamente de dicha especificación.

En consecuencia, la verificación de cumplimiento se realiza en términos de conformidad con la UNE 0087:2025, garantizando la coherencia con su estructura y con los principios de soberanía digital, interoperabilidad, gobernanza, confianza y generación de valor.

1.3. Estructura del documento

El presente documento se organiza en cuatro capítulos principales y tres anexos, que en conjunto describen el marco metodológico, operativo y técnico del mecanismo de verificación de conformidad de los Espacios de Datos.

Cada capítulo cumple una función específica dentro del proceso de verificación:

- **Capítulo 1:** Define el propósito, la finalidad y la relación del mecanismo con la Especificación UNE 0087:2025, que constituye su base normativa y conceptual.
- **Capítulo 2:** Establece los fundamentos metodológicos, los objetivos, los principios de verificación y los valores de trazabilidad y objetividad que guían el proceso de verificación.

- **Capítulo 3:** Describe las dimensiones, los tipos de evidencia y los criterios de elegibilidad que estructuran el mecanismo, determinando las condiciones mínimas necesarias para considerar conforme un espacio de datos.
- **Capítulo 4:** Detalla los criterios asociados a cada dimensión del modelo (modelo de negocio, gobernanza, solución técnica y seguridad, interoperabilidad y verificación funcional). Para cada criterio se incluye una descripción del requisito y una posible evidencia de verificación, que orienta al usuario sobre cómo justificar el cumplimiento durante su verificación.

Finalmente, el documento se complementa con tres anexos de carácter práctico:

- **Anexo A:** Herramienta que agrupa los criterios en formato de tabla para facilitar su cumplimentación y el registro de resultados.
- **Anexo B:** Recoge las definiciones operativas utilizadas en el documento, asegurando la coherencia terminológica con la UNE 0087:2025 y otras normas relacionadas.
- **Anexo C:** Incluye las normas, marcos y fuentes documentales empleadas como referencia en la elaboración del mecanismo.

Esta estructura garantiza una lectura progresiva y modular del documento, permitiendo comprender desde los fundamentos conceptuales hasta la aplicación práctica de la verificación de conformidad, con una trazabilidad directa entre los criterios y las evidencias propuestas.

2. Principios generales del mecanismo de verificación de conformidad

El presente capítulo establece los principios del mecanismo de verificación de conformidad de los espacios de datos, definiendo el enfoque, los objetivos, los fundamentos metodológicos y los roles implicados en su aplicación. Estos principios garantizan que el proceso de verificación se realice con rigurosidad técnica, objetividad y trazabilidad, asegurando resultados consistentes y verificables. Asimismo, se explican las dimensiones de verificación sobre las que se estructura el mecanismo, en coherencia con los criterios definidos en la Especificación UNE 0087:2025.

2.1. Enfoque de la verificación

El mecanismo de verificación se fundamenta en un enfoque basado en evidencias, orientado a comprobar de manera objetiva el grado de conformidad de una iniciativa con los requisitos establecidos. Su propósito no es valorar la madurez, el impacto ni la escala tecnológica de la iniciativa, sino determinar si cumple las condiciones esenciales que definen un espacio de datos según el marco normativo nacional.

Este enfoque permite evaluar tanto la existencia y adecuación de los elementos estructurales del espacio de datos -gobernanza, interoperabilidad, solución técnica, seguridad, modelo de negocio y funcionamiento real – como la consistencia de su aplicación práctica. Para ello, la verificación se apoya exclusivamente en evidencias documentales, técnicas observables, evitando la subjetividad y garantizando la reproductividad del proceso de verificación.

El resultado de la verificación de conformidad es binario: cada criterio se califica como “Cumple” o “No cumple”, esta simplicidad metodológica facilita la trazabilidad, la transparencia [2] y la homogeneidad de los resultados entre distintas evaluaciones o espacios de datos analizados.

2.2. Objetivos del mecanismo de verificación

El mecanismo de verificación de conformidad persigue los siguientes objetivos, definidos en coherencia con los principios de gobernanza y soberanía digital de la especificación [1] :

- Verificar la conformidad de los espacios de datos con los requisitos definidos en la Especificación UNE 0087:2025.
- Proporcionar una metodología común para la verificación de conformidad de proyectos e iniciativas, permitiendo la comparabilidad entre sectores y nieles de desarrollo.
- Asegurar la coherencia normativa y técnica de los espacios de datos en relación con los principios de soberanía digital, interoperabilidad y generación de valor.
- Fomentar la transparencia y la confianza, contribuyendo a la consolidación de un exosistema nacional de espacios de datos sólido, interoperable y ético.

En conjunto, estos objetivos buscan establecer un sistema de verificación de conformidad que permita distinguir los espacios de datos que cumplen con los estándares nacionales que aún no reúnen las condiciones necesarias para ser reconocidos como tales.

2.3. Principios metodológicos

El mecanismo de verificación se rige por una serie de principios metodológicos fundamentales que garantizan la integridad del proceso y la validez de los resultados obtenidos.

- **Objetividad**: todas las verificaciones deben realizarse sobre la base de hechos comprobables y documentación verificable. La opinión del evaluador no debe sustituir la evidencia técnica o documental.
- **Evidencia verificable**: todo resultado de cumplimiento debe sustentarse en una prueba concreta (documento, demostración técnica, registro o contrato) que confirme el requisito evaluado.
- **Trazabilidad**: cada comprobación debe estar asociada a una fuente de evidencia identificable, con registro de su procedencia, fecha y relación con el criterio evaluado.
- **Transparencia**: el proceso de verificación, los criterios aplicados y las conclusiones obtenidas deben poder ser revisados o auditados por terceros, garantizando la rendición de cuentas.
- **Coherencia**: los criterios deben aplicarse de manera uniforme entre diferentes evaluadores.
- **Proporcionalidad**: la verificación debe adecuarse al grado de desarrollo del espacio de datos, evitando imponer cargas desproporcionadas en fases

tempranas o proyectos piloto, siempre que los requisitos esenciales se encuentren cubiertos.

Estos principios son de aplicación transversal a todas las fases del mecanismo y constituyen el marco ético y técnico que asegura su credibilidad y validez.

Los principios metodológicos definidos en el presente mecanismo se fundamentan en los principios internacionales de verificación de la conformidad establecidos por la Organización Internacional de Normalización (ISO). En particular, el mecanismo se alinea con la ISO/IEC 17029:2019 [3], que establece los principios generales y requisitos aplicables a los procesos de validación y verificación, garantizando la objetividad, la competencia técnica, la independencia y la trazabilidad de las decisiones de verificación.

Asimismo, el documento toma como referencia la ISO 19011:2018 [4], que define los principios de auditoría y evaluación basados en evidencias, y la ISO/IEC 17000:2020 [5], que describe los principios y terminología fundamentales para los procesos de verificación de conformidad. En el ámbito nacional, estos principios se refuerzan mediante la UNE 0080:2023 [6], que proporciona el marco metodológico específico para la evaluación de capacidades en materia de datos, asegurando la coherencia con la UNE 0087:2025.

3. Estructura general del mecanismo de verificación

El presente capítulo describe la estructura y organización del mecanismo de verificación de conformidad de espacios de datos, estableciendo las dimensiones que lo componen, los tipos de evidencias requeridas y las condiciones mínimas necesarias para determinar la conformidad de una iniciativa con la Especificación UNE 0087:2025. Esta estructura proporciona un marco homogéneo para la verificación, asegurando que todas las evaluaciones se desarrollen bajo los mismos criterios, niveles de evidencia y procedimientos de revisión.

El mecanismo se concibe como un proceso de verificación integral, orientado a la comprobación de requisitos objetivos mediante evidencias verificables. No tiene carácter comparativo, sino verificativo y certificativo, permitiendo confirmar la existencia y adecuación de los elementos esenciales de un espacio de datos conforme a los principios de gobernanza, interoperabilidad, seguridad, confianza y generación de valor definidos en la norma UNE.

3.1. Dimensiones de verificación

La estructura del mecanismo se articula en cinco dimensiones principales, que agrupan los criterios de verificación y los requisitos mínimos que debe cumplir un espacio de datos para ser considerado conforme. Cada dimensión representa un área funcional clave descrita en el Anexo C de UNE 0087:2025 [1], y su evaluación conjunta garantiza una visión completa del ecosistema.

1. **Modelo de negocio:** Evalúa la existencia de un modelo económico y operativo sostenible, con identificación de fuentes de valor, participantes, mecanismos de colaboración y estrategias de escalabilidad. El objetivo es garantizar la viabilidad a largo plazo del ecosistema de compartición de datos.
2. **Sistema de gobernanza:** Comprueba la existencia de una autoridad formal de gobierno, un marco documentado de reglas, roles y procedimientos, y los mecanismos de adhesión, gestión y rendición de cuentas. Esta dimensión asegura

la aplicación de los principios de transparencia, responsabilidad y soberanía digital.

3. **Solución técnica y seguridad:** Examina la arquitectura del espacio de datos, la gestión de identidades, los servicios de confianza, la trazabilidad de las transacciones y las medidas de seguridad y privacidad aplicadas. Incluye la validación de los conectores, catálogos y mecanismos de control definidos en la norma.
4. **Interoperabilidad:** Verifica la adopción de estándares, protocolos y modelos semánticos que permitan la conexión fluida entre sistemas y participantes. Abarca las cuatro capas de interoperabilidad (legal, organizativa, semántica y técnica).
5. **Verificación funcional**: Confirma el funcionamiento real del espacio de datos mediante evidencias prácticas de adhesión de participantes, publicación en catálogos y transacciones efectivas de datos o servicios. Esta dimensión valida la operatividad y la capacidad de ejecución del ecosistema.

Cada dimensión se evalúa de manera independiente, pero los resultados deben analizarse de forma integral, dado que el incumplimiento de una de ellas puede comprometer la conformidad global del espacio de datos evaluado.

3.2. Fuentes de información y tipos de evidencia

El mecanismo se fundamenta en un sistema de verificación basado en evidencias, conforme a los principios definidos en la ISO/IEC 17029:2019 y la UNE 0080:2023. Cada criterio de verificación deberá sustentarse en pruebas documentales, técnicas u observables que permitan demostrar el cumplimiento de los requisitos evaluados.

Las fuentes de evidencia pueden clasificarse en tres categorías:

- **Evidencias documentales**: informes, memorias, planes, contratos, estatutos o documentos que describan el modelo de gobernanza, la arquitectura técnica, las políticas de seguridad o los procedimientos internos.
- **Evidencias técnicas**: capturas del sistema, demostraciones, logs de actividad, catálogos de datos, metadatos o resultados de pruebas funcionales.
- **Evidencias observables**: demostraciones en entorno real, simulaciones o verificaciones presenciales que confirmen la operatividad del espacio de datos.

Toda evidencia debe ser verificable, actualizada y trazable, y conservarse conforme a las buenas prácticas. En caso de evidencias parciales o no concluyentes, el evaluador podrá solicitar aclaraciones o información complementaria al promotor.

3.3. Criterio de cumplimiento y elegibilidad

El mecanismo de verificación se basa en un criterio binario de cumplimiento, mediante el cual cada requisito o indicador se califica como “Cumple” o “No cumple”, de acuerdo con la evidencia presentada y validada durante el proceso de verificación.

El objetivo de este criterio es garantizar una interpretación homogénea y objetiva de los resultados, facilitando la trazabilidad de las decisiones y la transparencia del proceso.

Un requisito se considerará cumplido cuando la evidencia aportada demuestre de forma inequívoca que el espacio de datos dispone del elemento o capacidad exigida en la Especificación UNE 0087:2025.

Por el contrario, se considerará no cumplido cuando:

- No exista evidencia suficiente o actualizada.
- La evidencia presentada no guarde correspondencia con el requisito evaluado.
- Se detecten contradicciones o inconsistencias entre los documentos, las demostraciones técnicas o los registros verificados.

Un espacio de datos se considerará conforme a la Especificación UNE 0087:2025 cuando se verifique el cumplimiento total de los criterios establecidos en las cinco dimensiones de verificación:

1. Modelo de negocio.
2. Sistema de gobernanza.
3. Solución técnica y seguridad.
4. Interoperabilidad.
5. Verificación funcional.

3.4. Condiciones mínimas para la consideración como espacio de datos

Para que una iniciativa sea considerada espacio de datos conforme a la UNE 0087:2025, deberá cumplir todas las dimensiones de verificación descritas en la presente guía. El cumplimiento parcial o la ausencia de evidencia en una o más dimensiones impedirá emitir un resultado positivo de conformidad.

Se entenderá que un espacio de datos cumple las condiciones mínimas cuando:

- Existe un marco de gobernanza formalizado y operativo.
- Dispone de una arquitectura técnica y de seguridad documentada y en funcionamiento.
- Acredita la interoperabilidad funcional entre participantes mediante estándares o protocolos reconocidos.
- Demuestra actividad real de intercambio de datos o servicios entre los miembros del ecosistema.
- Presenta un modelo de negocio documentado y sostenible, que garantice su continuidad y viabilidad a medio plazo.

El cumplimiento de estas condiciones permitirá emitir el dictamen de conformidad, que acreditará que el espacio de datos evaluado cumple los principios, características y requisitos establecidos por la Especificación UNE 0087:225

4. Criterios e indicadores de verificación

El presente capítulo establece los criterios e indicadores que conforman el mecanismo de verificación de espacios de datos, organizados en función de las dimensiones definidas en el capítulo anterior. Cada criterio representa un requisito verificable de cumplimiento obligatorio, cuya conformidad se determina mediante la presentación y validación de evidencias documentales, técnicas u observables.

El sistema de verificación se basa en un modelo binario de verificación:

- Cumple, cuando la evidencia presentada demuestra que el requisito está implantado y operativo.
- No cumple, cuando no existe evidencia suficiente o cuando esta no se ajusta a lo establecido en el criterio evaluado.

La relación de criterios que se recoge a continuación se aplica de forma homogénea a todos los espacios de datos, independientemente de su ámbito sectorial o tecnológico, permitiendo una verificación uniforme y trazable.

A efectos prácticos, en cada criterio se proporciona:

- Una descripción, que explica el contenido y alcance del requisito.
- Una posible evidencia de verificación, que orienta al evaluador o al promotor sobre los elementos que puede revisar o aportar para justificar el cumplimiento.

4.1. Modelo de negocio

El modelo de negocio constituye la base de sostenibilidad y viabilidad del espacio de datos. Su evaluación tiene por objeto verificar la existencia de una planificación estratégica que garantice su continuidad operativa, la participación equilibrada de los actores y la generación de valor a partir del intercambio de datos.

1. **Existencia de un modelo de negocio documentado**

Descripción:

Se evalúa la existencia de un documento formal que defina los objetivos estratégicos del espacio de datos, la propuesta de valor para los participantes, los servicios ofrecidos, los flujos de ingresos (si los hubiera) y el modelo de sostenibilidad.

El modelo debe describir cómo el espacio de datos crea valor económico, social y cómo ese valor se distribuye entre los miembros del ecosistema.

Posible evidencia de verificación:

Plan de negocio, memoria estratégica, documento de sostenibilidad o equivalente que detalle los objetivos, propuesta de valor, fuentes de ingresos, modelo de gobernanza económica o indicadores de impacto.

2. **Identificación de los participantes y sus roles**

Descripción:

Verifica que el espacio de datos ha identificado a los actores que forman parte del ecosistema y ha definido sus funciones: promotor, autoridad de gobierno, consumidor, proveedor, productor de datos y operador.

Una definición clara de roles es esencial para garantizar la trazabilidad de responsabilidades, el equilibrio de intereses y la interoperabilidad organizativa.

Posible evidencia de verificación:

Organigrama funcional del espacio de datos, estatutos de gobernanza, registro de participantes, contratos o acuerdos de adhesión que especifiquen responsabilidades y derechos.

3. **Plan de sostenibilidad o estrategia de escalado**

Descripción:

Evalúa la existencia de un plan que garantice la continuidad del espacio de datos más allá de su fase inicial o de financiación pública.

El plan debe contemplar aspectos económicos, técnicos y organizativos: fuentes de financiación, mantenimiento de la infraestructura, evolución del modelo de servicios y estrategias de expansión o federación con otros espacios de datos.

Posible evidencia de verificación:

Documento de planificación estratégica o plan de sostenibilidad, informes financieros o de continuidad, estrategias de federación o colaboración intersectorial.

4.2. Sistema de gobernanza

La gobernanza asegura la correcta gestión del espacio de datos y la aplicación de los principios de soberanía digital, transparencia y rendición de cuentas. Su evaluación se centra en verificar la existencia y funcionamiento de las estructuras y mecanismos definidos en la norma UNE 0087:2025, capítulo 6.

1. **Constitución formal de la autoridad de gobierno**

Descripción:

Se evalúa la existencia de una entidad, comité o figura responsable de la dirección y supervisión del espacio de datos.

La autoridad de gobierno debe contar con competencias formales para definir políticas, aprobar normas de participación, velar por el cumplimiento de los principios de confianza y resolver incidencias o disputas.

Su creación debe ser transparente y documentada, asegurando la representación equilibrada de los distintos grupos de interés.

Posible evidencia de verificación:

Acta de constitución de autoridad de gobierno, estatutos del espacio de datos, documento de roles y responsabilidades, resolución o registro institucional que acredite su existencia.

2. **Existencia de un marco de gobernanza documentado**

Descripción:

Verifica que el espacio de datos dispone de un marco normativo y organizativo formal que regule su funcionamiento.

El marco de gobernanza debe incluir reglas de participación, derechos y obligaciones de los miembros, procedimientos de decisión, mecanismos de supervisión, medidas disciplinarias y políticas de transparencia.

Este documento constituye el núcleo organizativo del ecosistema y debe estar accesible para todos los participantes

Posible evidencia de verificación:

Libro de reglas del espacio de datos, reglamento interno de gobernanza, manual de operaciones, documentos de políticas o conjunto de normas internas aprobadas por la autoridad de gobierno.

3. **Procedimientos de adhesión, permanencia y salida de participantes**

Descripción:

Evalúa si existen procesos formales que regulen cómo las entidades pueden incorporarse al espacio de datos, mantener su pertenencia o darse de baja.

Estos procedimientos deben ser públicos, transparentes y basados en criterios objetivos, garantizando igualdad de oportunidades de acceso y continuidad.

Su existencia asegura la sostenibilidad del ecosistema y evita la discriminación.

Posible evidencia de verificación:

Procedimientos de adhesión y salida publicados, formularios de solicitud, contratos o acuerdos de adhesión, manuales de participación o actas de revisión de nuevas altas/bajas.

4. **Mecanismos de resolución de conflictos y rendición de cuentas**

Descripción:

Se analiza la existencia de mecanismos internos para la gestión de disputas, reclamaciones o incumplimientos de las normas de gobernanza.

También se valora la rendición de cuentas de la autoridad de gobierno y de los operadores ante los participantes y las autoridades regulatorias competentes.

La presencia de mecanismos de revisión y control fortalece la confianza, reduce riesgos y mejora la transparencia operativa.

Posible evidencia de verificación:

Protocolo de gestión de incidencias, reglamento de reclamaciones, comités de arbitraje, informes de auditoría, documentación de procesos disciplinarios o de control.

5. **Portal o repositorio de transparencia**

Descripción:

Verifica si el espacio de datos dispone de un espacio público (portal web, repositorio o plataforma digital) donde se publiquen las políticas, reglas, informes de actividades y resultados de las evaluaciones.

El objetivo es garantizar la transparencia y facilitar la comunicación con los participantes y con la ciudadanía. Un portal de transparencia operativo constituye un indicador de madurez y confianza del ecosistema.

Posible evidencia de verificación:

Portal web institucional o repositorio digital con información pública actualizada (estatutos, actas, informes de cumplimiento, políticas de privacidad, listado de miembros).

4.3. Solución técnica y seguridad

Esta dimensión analiza la infraestructura técnica que sustenta el espacio de datos, los mecanismos de autenticación y control de acceso, la gestión de seguridad y privacidad, la capacidad de trazabilidad y auditoría. Se apoya en lo dispuesto en los capítulos 5 y 6 de la UNE 0087:2025.

Su propósito es asegurar la operación confiable, interoperable y segura del ecosistema, preservando la integridad de los datos, la autenticidad de los participantes y la trazabilidad de las transacciones.

La verificación de esta dimensión permite verificar que el espacio de datos cuenta con los recursos tecnológicos necesarios para prestar servicios de compartición de información bajo principios de soberanía, protección y control.

1. **Existencia de una arquitectura técnica definida y documentada**

Descripción:

Se evalúa si el espacio de datos dispone de una arquitectura técnica formalmente definida, que describa los componentes principales, los servicios habilitadores, las relaciones entre actores y los flujos de información.

La arquitectura debe reflejar cómo se soportan las funciones esenciales del ecosistema: gestión de identidades, catálogos, conectores, auditoría, trazabilidad y seguridad.

Debe incluir también las dependencias tecnológicas, protocolos de comunicación y estándares empleados.

Posible evidencia de verificación:

Documento técnico de arquitectura, diagramas de componentes y flujos de datos, fichas de diseño, plan de infraestructura o modelo de referencia técnico aprobado por la autoridad de gobierno.

2. **Mecanismos de identificación y autenticación de participantes y servicios**

Descripción:

Verifica la existencia de mecanismos que permitan identificar de forma unívoca y segura a los participantes (personas físicas, jurídicas o sistemas) y a los servicios digitales que operan en el espacio de datos.

La autenticación debe basarse en credenciales verificables, certificados digitales o mecanismos equivalentes, alineados con los estándares europeos de identidad digital (eIDAS 2.0, SSI).

El sistema debe garantizar la integridad, la no suplantación y la trazabilidad de todas las operaciones.

Posible evidencia de verificación:

Esquema de gestión de identidades, políticas de autenticación, registros de acceso, certificados o credenciales digitales, logs de verificación de usuarios y servicios.

3. **Catálogo estructurado de productos y servicios de datos**

Descripción:

Evalúa la existencia de un catálogo digital que permita registrar, describir y descubrir los productos de datos y servicios ofrecidos dentro del espacio de datos.

El catálogo debe estructurarse siguiendo estándares reconocidos (como DCAT o DCAT-AP), garantizando la interoperabilidad semántica y la reutilización de la información.

Además, debe permitir búsquedas, gestión de metadatos, control de acceso y trazabilidad de las operaciones.

Posible evidencia de verificación:

Catálogo operativo o documentación de su diseño, perfiles de metadatos, registros de productos o servicios publicados, descripciones DCAT o equivalentes, interfaces de búsqueda o APIs.

4. **Mecanismos de transferencia y control de datos**

Descripción:

Se analiza si el espacio de datos dispone de conectores, protocolos o servicios que permitan la transferencia controlada de datos entre participantes.

Estos mecanismos deben asegurar la integridad, trazabilidad y no repudio de las transacciones, así como el cumplimiento de las políticas de uso y licencias asociadas a cada intercambio.

También se evalúa la existencia de herramientas de supervisión o control que validen las condiciones antes, durante y después de la transferencia.

Posible evidencia de verificación:

Documentación de los conectores o APIs utilizados, logs de transferencia, mecanismos de validación, auditorías automáticas, pruebas de intercambio o contratos digitales asociados.

5. **Medidas de seguridad y privacidad implementadas**

Descripción:

Evalúa las medidas aplicadas para proteger la infraestructura, los datos y las operaciones del espacio de datos frente a riesgos de seguridad o violaciones de privacidad.

Incluye la aplicación de políticas de control de acceso, cifrado de datos, aislamiento de entornos, gestión de vulnerabilidades y cumplimiento del Reglamento General de Protección de Datos (RGPD).

La seguridad debe integrarse desde el diseño (“security & privacy by design”) y cubrir tanto los componentes técnicos como los procesos organizativos.

Posible evidencia de verificación:

Política de seguridad del espacio de datos, certificaciones, medidas de cifrado, informes de auditoría, registro de consentimientos y análisis de riesgos o DPIA.

6. **Mecanismos de cumplimiento y auditoría**

Descripción:

Se verifica la existencia de procesos y herramientas que permitan auditar el cumplimiento normativo, contractual y técnico del espacio de datos.

Incluye la trazabilidad de las operaciones, el registro de logs, la monitorización continua y la generación de informes de cumplimiento o alertas ante desviaciones.

Estos mecanismos son fundamentales para la transparencia, la rendición de cuentas y la mejora continua del ecosistema.

Posible evidencia de verificación:

Logs de auditoría, informes técnicos de verificación, reportes de cumplimiento RGPD, evidencias de auditorías internas o externas, herramientas de observabilidad o paneles de control.

4.4. Interoperabilidad

La interoperabilidad constituye el eje fundamental para la integración, cooperación y comunicación entre los participantes del espacio de datos y entre diferentes espacios o ecosistemas.

Su propósito es garantizar que las organizaciones puedan intercambiar información, comprenderla y utilizarla de forma efectiva, sin necesidad de adaptaciones específicas.

El concepto se aplica de manera transversal en cuatro niveles complementarios: legal, organizativo, semántico y técnico, según la norma UNE 0087:2025.

La verificación de esta dimensión permite determinar si el espacio de datos es capaz de operar de forma federada y sostenible dentro de un ecosistema digital más amplio.

Nota metodológica
Los criterios de interoperabilidad no deben evaluarse de forma aislada, sino en conjunto con las dimensiones solución técnica y gobernanza, ya que la interoperabilidad depende tanto de la infraestructura tecnológica como del marco normativo y organizativo que la regula. El cumplimiento de esta dimensión implica que el espacio de datos es capaz de interconectarse, integrarse y colaborar con otros espacios o ecosistemas europeos bajo un modelo federado.

1. Capacidades digitales para la transferencia de datos

Descripción:

Evalúa si el espacio de datos dispone de los medios digitales necesarios para realizar transferencias seguras, trazables y controladas de datos entre sistemas y participantes.

Las capacidades digitales deben permitir el transporte de información entre dominios de confianza, garantizando la disponibilidad, integridad y control de los intercambios.

Se consideran tanto los mecanismos de comunicación directa (APIs, conectores) como los servicios federados que faciliten la interoperabilidad técnica entre distintas plataformas.

Posible evidencia de verificación:

Documentación técnica de los conectores o servicios de intercambio, descripciones de APIs o interfaces de comunicación, evidencias de pruebas de interoperabilidad entre participantes o catálogos de servicios conectados.

2. **Mecanismos de autenticación, autorización y registro de acceso**

Descripción:

Se verifica la existencia de mecanismos de autenticación y control de acceso que aseguren que solo los participantes acreditados y autorizados pueden acceder a los datos o servicios del espacio.

Estos mecanismos deben estar integrados con los sistemas de identidad digital y respetar los principios de confianza mutua entre dominios federados.

También se evalúa la capacidad del sistema para mantener registros de auditoría y trazabilidad de los accesos realizados.

Posible evidencia de verificación:

Políticas de control de acceso, logs de autenticación, descripción de flujos de autorización, documentación del sistema de identidad digital o credenciales verificables utilizadas (eIDAS2, SSI u otros).

3. **Instrumentos de control y validación de políticas**

Descripción:

Se analiza si el espacio de datos dispone de mecanismos automáticos o manuales que verifiquen el cumplimiento de las reglas del ecosistema antes de autorizar una transferencia de datos, asegurando el cumplimiento de las políticas de acceso y uso a los datos.

Estos instrumentos deben validar que los intercambios respetan las condiciones contractuales, las licencias de uso, los derechos de los participantes y las restricciones de privacidad.

Su implementación es esencial para asegurar la soberanía digital y la aplicación coherente de las políticas de uso y gobernanza.

Posible evidencia de verificación:

Procedimientos de validación de licencias, contratos digitales, logs de control, mecanismos de definición y verificación de políticas de uso, registros de denegación o autorización de transacciones.

4. **Protocolos y especificaciones técnicas interoperables**

Descripción:

Verifica la adopción de protocolos, formatos y modelos de datos estándar que garanticen la interoperabilidad entre los distintos componentes y actores del espacio de datos.

La verificación incluye el uso de estándares internacionales (como DCAT-AP, RDF, JSON-LD, OpenAPI, IDS-RAM o equivalentes), así como la alineación con las especificaciones nacionales y europeas.

La aplicación de estos estándares permite el intercambio fluido de datos y servicios, reduciendo costes de integración y favoreciendo la escalabilidad del

Posible evidencia de verificación:

Especificaciones técnicas adoptadas, documentación de APIs y ontologías, catálogos o repositorios DCAT-AP, documentación de conformidad con el marco IDS-RAM o reportes de compatibilidad con estándares de interoperabilidad.

5. **Registro trazable de transacciones y operaciones**

Descripción:

Evalúa si el espacio de datos mantiene un registro completo, verificable y auditable de todas las transacciones realizadas entre participantes.

El registro debe permitir la trazabilidad de los intercambios, la detección de anomalías, la generación de métricas de uso y la reconstrucción de eventos en caso de incidentes.

Este requisito refuerza la transparencia, la confianza y la rendición de cuentas del ecosistema, siendo un componente esencial de la gobernanza técnica.

Posible evidencia de verificación:

Logs de transacciones, informes de actividad, paneles de observabilidad, mecanismos de seguimiento de eventos, herramientas de monitorización o auditorías automáticas de integridad.

4.5. Verificación funcional

La verificación funcional permite constatar el nivel operativo real del espacio de datos y confirmar que sus procesos esenciales —adhesión, publicación, consulta y transacción de datos— se encuentran implementados y activos.

Esta dimensión valida la madurez práctica del ecosistema y su capacidad para generar valor a través de la colaboración, la interoperabilidad y la compartición segura de información.

El cumplimiento de los criterios de este apartado es condición necesaria para que un espacio de datos pueda considerarse plenamente conforme con la Especificación UNE 0087:2025.

Nota metodológica
La verificación funcional representa la fase final y decisiva del proceso de evaluación. Un espacio de datos puede disponer de una gobernanza sólida y una arquitectura técnica avanzada, pero solo se considerará plenamente conforme si demuestra actividad real y sostenida. La evidencia de transacciones y operaciones activas constituye el indicador principal de madurez y éxito operativo del ecosistema.

1. **Evidencia del proceso de adhesión de participantes**

Descripción:

Evalúa si el espacio de datos dispone de un proceso formal y operativo que permita a nuevas entidades adherirse al ecosistema.

El proceso debe incluir la verificación de requisitos de entrada, la aceptación de las condiciones de participación y la asignación de credenciales o identidades digitales.

Este criterio refleja la apertura y la capacidad de crecimiento sostenible del espacio, garantizando que el acceso sea transparente, trazable y no discriminatorio.

Posible evidencia de verificación:

Registro de adhesiones, formularios o contratos de participación, guías de incorporación de miembros, evidencias de altas recientes, logs de creación de cuentas o credenciales verificables.

2. **Evidencia del proceso de publicación de productos o servicios de datos**

Descripción:

Verifica que los proveedores del espacio de datos pueden publicar productos, servicios o conjuntos de datos en el catálogo del ecosistema.

El proceso de publicación debe estar automatizado o documentado, e incluir validaciones de metadatos, asignación de políticas de uso y control de acceso.

La existencia de publicaciones activas demuestra la utilidad y el dinamismo del espacio de datos, así como la capacidad de los participantes para compartir recursos de manera estructurada y gobernada.

Posible evidencia de verificación:

Capturas o registros del catálogo de productos, evidencias de publicación o actualización de datos, informes de actividad de proveedores, logs de validación de metadatos, interfaces o APIs de publicación.

3. **Evidencia del proceso de consulta o descubrimiento de información**

Descripción:

Se evalúa si los usuarios o consumidores del espacio de datos pueden buscar, descubrir y acceder a los productos o servicios disponibles.

El proceso de consulta debe permitir la localización de los datos mediante metadatos estructurados y garantizar la disponibilidad y rendimiento del sistema.

Este criterio demuestra la funcionalidad del catálogo y la experiencia de uso dentro del ecosistema.

Posible evidencia de verificación:

Capturas del buscador del catálogo, consultas realizadas, logs de acceso a productos o servicios, resultados de búsquedas o pruebas de rendimiento de la interfaz de consulta.

4. **Evidencia de transacciones efectivas de datos o servicios**

Descripción:

Verifica la existencia de intercambios reales de datos o servicios entre los participantes del espacio, realizados bajo los principios de seguridad, confianza y soberanía.

Estas transacciones pueden consistir en transferencias, consultas federadas, ejecuciones de algoritmos sobre datos compartidos o prestación de servicios derivados.

Su validación confirma que el ecosistema no solo está implementado, sino que opera activamente y genera valor tangible para sus miembros.

Posible evidencia de verificación:

Logs de transacciones, reportes de intercambio, registros de auditoría, contratos digitales ejecutados, trazas de ejecución de servicios, informes de casos de uso o resultados de validación de transacciones.

5. Anexo A. Lista de criterios de verificación

5.1. Modelo de negocio

Criterio de verificación	Descripción del requisito	Posible evidencia de verificación	Resultado
Neg.1	Existencia de un documento de modelo de negocio que describa objetivos, propuesta de valor, participantes y fuentes de ingresos	Plan de negocio, memoria estratégica o documento equivalente	☐ Cumple ☐ No cumple
Neg.2	Identificación de los participantes y sus roles en el ecosistema (proveedores, consumidores, operadores, autoridad de gobierno)	Organigrama funcional, estatutos o documentación de gobernanza	☐ Cumple ☐ No cumple
Neg.3	Definición de un plan de sostenibilidad o estrategia de escalado que garantice la continuidad económica y la participación de nuevos actores	Documento de planificación o estrategia de crecimiento	☐ Cumple ☐ No cumple

5.2. Sistema de gobernanza

Criterio de verificación	Descripción del requisito	Posible evidencia de verificación	Resultado
Gob.1	Constitución formal de la autoridad de gobierno del espacio de datos.	Estatuto, acta constitutiva o documentación de constitución	☐ Cumple
			☐ No cumple
Gob.2	Existencia de un marco de gobernanza documentado que incluya reglas, roles y responsabilidades.	Libro de reglas y roles, reglamento interno o equivalente	☐ Cumple
			☐ No cumple
Gob.3	Definición y documentación de los procedimientos de adhesión, permanencia y salida de participantes.	Formularios o contratos de adhesión, procesos publicados o registros	☐ Cumple
			☐ No cumple
Gob.4	Existencia de mecanismos de resolución de conflictos y rendición de cuentas.	Protocolo de gestión de incidencias	☐ Cumple
			☐ No cumple
Gob.5	Disponibilidad de un repositorio o portal de	URL, portal de transparencia o	☐ Cumple

Criterio de verificación	Descripción del requisito	Posible evidencia de verificación	Resultado
	transparencia accesible para los participantes	repositorio de políticas	☐ No cumple

5.3. Solución técnica y seguridad

Criterio de verificación	Descripción del requisito	Posible evidencia de verificación	Resultado
Tec.1	Existencia de una arquitectura técnica definida y documentada.	Diagrama de arquitectura, documentación técnica o ficha de diseño	☐ Cumple
			☐ No cumple
Tec.2	Implementación de mecanismos de identificación y autenticación de participantes y servicios.	Sistema de identidad digital, credenciales verificables, logs de acceso	☐ Cumple
			☐ No cumple
Tec.3	Existencia de un catálogo estructurado que permita la publicación y descubrimiento de datos y servicios	Catalogo DCAT o plataforma de servicios registrada	☐ Cumple
			☐ No cumple
Tec.4	Disponibilidad de mecanismos de transferencia y control que aseguren la integridad y trazabilidad d ellos intercambios.	Registros de transacción, conectores o logs de validación	☐ Cumple
			☐ No cumple

Criterio de verificación	Descripción del requisito	Posible evidencia de verificación	Resultado
Tec.5	Existen medidas de seguridad y privacidad implementadas para proteger los datos y la infraestructura, incluyendo el uso de cifrado, aislamiento de entornos y control de accesos conforme al RGPD	Políticas de privacidad, medidas de cifrado, registro de consentimiento	☐ Cumple ☐ No cumple
Tec.6	El espacio de datos cuenta con mecanismos de cumplimiento y auditoría, que permiten verificar la conformidad con las normativas aplicables y generar trazabilidad de los procesos.	Logs de auditoría, informes técnicos, reportes de cumplimiento RGPD o certificaciones de seguridad	☐ Cumple ☐ No cumple

5.4. Interoperabilidad

Criterio de verificación	Descripción del requisito	Posible evidencia de verificación	Resultado
Int.1	El espacio de datos dispone de capacidades digitales para la transferencia de datos entre sistemas, que aseguran su disponibilidad y transporte controlado	Capturas o demostraciones que muestren la transferencia de datos mediante descarga, API o conector, documentación técnica de la arquitectura de red y protocolos utilizados	☐ Cumple ☐ No cumple
Int.2	Existen mecanismos de autenticación, autorización y	Descripción del sistema de identidad	☐ Cumple

Criterio de verificación	Descripción del requisito	Posible evidencia de verificación	Resultado
	registro que garantizan que únicamente los participantes acreditados puedan acceder a los datos o servicios	y control de acceso, logs de autenticación, credenciales verificables, políticas de autorización.	☐ No cumple
Int.3	Se implementan instrumentos de control y validación que aseguran el cumplimiento de las reglas del espacio de datos, las políticas de uso y los términos contractuales antes de la transferencia	Capturas o vídeos del proceso de validación de contrato digital, políticas o licencias, evidencias de interrupción de transferencia ante incumplimiento	☐ Cumple ☐ No cumple
Int.4	Se aplican protocolos y especificaciones técnicas interoperables (conectores, APIs, catálogos DCAT, ontologías semánticas o perfiles de intercambio)	Documentación de conectores o APIs implementadas, descripción de estándares aplicados (DCAT-AP, RDF, IDS-RAM, etc.)	☐ Cumple ☐ No cumple
Int.5	Se mantiene un registro trazable de las transacciones de datos que permita su auditoría posterior y garantice la integridad y no repudio de las operaciones	Logs de transacciones, auditorías automáticas, evidencias de observabilidad o paneles de seguimiento.	☐ Cumple ☐ No cumple

5.5. Verificación funcional

Criterio de verificación	Descripción del requisito	Posible evidencia de verificación	Resultado
Fun.1	Evidencia de proceso de adhesión de un participante	Capturas de registro o demostración del proceso de alta	☐ Cumple ☐ No cumple
Fun.2	Evidencia del proceso de publicación de un producto o servicio en el catálogo	Captura o demostración funcional de publicación	☐ Cumple ☐ No cumple
Fun.3	Evidencia de consulta o descubrimiento del catálogo por parte de un usuario	Registro de búsqueda o demostración funcional	☐ Cumple ☐ No cumple
Fun.4	Evidencia de transacción efectiva de datos o servicios entre participantes	Logs o registros de intercambio, contratos digitales o APIs	☐ Cumple ☐ No cumple

6. Anexo B. Glosario de términos

Acuerdo Marco

Contrato general que regula los principios de participación en un espacio de datos, definiendo derechos, obligaciones, reglas de acceso y permanencia de los participantes.

Autoridad de Gobierno del Espacio de Datos

Rol del espacio de datos, responsable de desarrollar, mantener, operar y hacer cumplir el modelo de gobernanza del espacio de datos.

Auditoría Técnica

Proceso de verificación sistemática destinado a evaluar la conformidad de las evidencias presentadas en el mecanismo de verificación, conforme a las directrices de la ISO 19011:2018.

Catálogo de espacio de datos

Servicio que, por una parte, permite a los proveedores describir y registrar en el espacio de datos ofertas de productos de datos, servicios y otros tipos de recursos y, por otra, facilita a consumidores potenciales descubrir, valorar, negociar y contratar dichas ofertas.

Confianza

Pilar fundamental de los espacios de datos. Se refiere a la garantía de un entorno seguro, transparente y verificable para el intercambio de datos entre actores.

Consumidor de Datos/Servicios

Rol que utiliza los datos y/o servicios que son ofertados en el espacio de datos. Este rol puede ser asumido tanto por una entidad jurídica (organización) como por un usuario vinculado a una organización (usuarios finales que son personas físicas vinculadas con la organización, incluyendo no sólo empleados sino también clientes de la misma, aplicaciones implementadas dentro de la organización, o incluso dispositivos tales como sensores desplegados por la organización).

Datos

Toda representación digital de actos, hechos o información, así como su recopilación, incluso como grabación sonora, visual o audiovisual (*Reglamento (UE) 2022/86*).

Dictamen de Conformidad

Documento emitido por la entidad evaluadora al final del proceso, que acredita si un espacio de datos cumple los criterios establecidos en el mecanismo de verificación y en la UNE 0087:2025.

Evidencia Verificable

Documento, demostración técnica o registro observable que respalda el cumplimiento de un requisito evaluado. Debe ser trazable, objetiva y verificable por terceros.

Espacio de Datos

Ecosistema colaborativo que proporciona un medio para que diversos participantes compartan, utilicen datos y presten servicios de manera segura, confiable y conforme a las normativas, con el fin de impulsar la innovación, el impacto económico y social. Basado

en un marco de gobernanza, los espacios de datos pueden facilitar transacciones de datos seguras, fomentar la confianza y la soberanía. Estos espacios se pueden implementar mediante arquitecturas interoperables, tecnologías semánticas, conectores y tecnologías de identidad digital, y están diseñados para apoyar una amplia variedad de casos de uso y aplicaciones.

Verificación de Conformidad

Proceso mediante el cual se determina si un objeto, proceso o sistema cumple los requisitos especificados en normas o marcos de referencia. (ISO/IEC 17029:2019).

Identidad Digital

Mecanismo o conjunto de credenciales verificables que permite identificar de forma segura a los participantes y servicios en un espacio de datos, garantizando autenticación y autorización conforme al Reglamento eIDAS 2.0.

Indicador de Evaluación (KPI)

Elemento medible utilizado para verificar el cumplimiento de un criterio específico. Cada KPI se asocia a una dimensión de análisis (gobernanza, interoperabilidad, seguridad, etc.).

Infraestructura del Espacio de Datos

Conjunto de componentes técnicos (servicios de identidad, catálogos, conectores, auditoría, trazabilidad, etc.) que permiten la operación y sostenibilidad del ecosistema.

Interoperabilidad

Capacidad de que las organizaciones interactúen con vistas a alcanzar objetivos comunes que sean mutuamente beneficiosos y que hayan sido acordados previa y conjuntamente, recurriendo a la puesta en común de información y conocimientos entre las organizaciones, a través de los procesos empresariales a los que apoyan, mediante el intercambio de datos entre sus sistemas de TIC respectivos (*MEI/EIF 2017*).

Marco de gobernanza

Conjunto de convenios y normas organizativas, funcionales, técnicas, operativas y legales que estructuran los roles de los participantes y sus interacciones dentro y a través de las distintas partes del ecosistema que conforma el espacio de datos. En base a este marco, se implementa el sistema que gobierna el espacio de datos.

Modelo Arquitectónico

Estructura tecnológica que soporta el espacio de datos, compuesta por servicios habilitadores (identidad, catálogos, conectores) y protocolos de interoperabilidad.

No Conformidad

Resultado negativo obtenido durante el proceso de verificación cuando un criterio obligatorio no se cumple o la evidencia es insuficiente. Puede ser mayor o menor, según su impacto en el resultado final.

Operador del Espacio de Datos

Entidad responsable de desplegar y mantener la infraestructura técnica, asegurando el funcionamiento de los servicios habilitadores.

Participante

Entidad sujeta al sistema de gobierno que interactúa con el espacio de datos en calidad de productor, proveedor o consumidor de productos de datos y servicios u otro rol

Productor de Datos

Entidad, dispositivo o software capaz de generar datos.

Promotor

Figura clave que impulsa, coordina y asegura la sostenibilidad de un espacio de datos. Define la propuesta de valor, convoca a los participantes, establece la gobernanza y garantiza el cumplimiento normativo.

Servicios Habilitadores

Conjunto de componentes técnicos que permiten operar el espacio de datos: gestión de identidad, catálogos, conectores, mecanismos de seguridad, observabilidad y auditoría.

Soberanía Digital

Principio que asegura que cada participante conserva control sobre los datos que comparte y sobre las condiciones de su uso.

Trazabilidad

Capacidad de identificar el origen, uso, modificaciones y transferencias de los datos dentro del espacio, garantizando integridad, auditoría y rendición de cuentas.

UNE 0087:2025

Norma española que define los principios, requisitos y orientaciones para la creación y desarrollo de espacios de datos, centrada en interoperabilidad, soberanía y confianza.

Verificación Funcional

Proceso mediante el cual se comprueba la operatividad real de los componentes técnicos y organizativos del espacio de datos (adhesión, publicación, consulta y transacción de datos o servicios).

7. Anexo C. Referencias bibliográficas

[1] Centro de Referencia de Espacios de Datos, «ESPECIFICACION UNE 0087:2025 Definición y caracterización de los espacios de datos». Accedido: 17 de julio de 2025. [En línea]. Disponible en: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0074731

[2] «The European Interoperability Framework in detail». [En línea]. Disponible en: https://interoperable-europe.ec.europa.eu/collection/iopeu-monitoring/european-interoperability-framework-detail

[3] «ISO/IEC 17029:2019», Conformity assessment — General principles and requirements for validation and verification bodies. [En línea]. Disponible en: https://www.iso.org/standard/29352.html

[4] «ISO 19011:2018», Guidelines for auditing management systems. [En línea]. Disponible en: https://www.iso.org/standard/70017.html

[5] «ISO/IEC 17000:2020», Conformity assessment — Vocabulary and general principles. [En línea]. Disponible en: https://www.iso.org/standard/73029.html

[6] «ESPECIFICACION UNE 0080:2023», Guía de evaluación del Gobierno, Gestión y Gestión de la Calidad del Dato. [En línea]. Disponible en: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0071383