UNIVERSIDAD DE MURCIA

La preservación digital.
El archivo digital.
Los metadatos de preservación

CONNECT | Conocimiento interconectado y Competencias digitales
Grupo de innovación docente
Universidad de Murcia

Este material es un extracto del libro:

Baños-Moreno, María-José. (2025). Preservación digital: una visión desde la Gestión de la Información. Editum. Ediciones de la Universidad de Murcia.
https://doi.org/10.6018/editum.3176

1. Introducción

Este documento tiene como propósito facilitar la preparación de contenidos para oposiciones en archivos y bibliotecas en relación con la preservación digital. En concreto, se orienta específicamente a la oposición convocada por la *Orden de 20 de octubre de 2025 de la Consejería de Economía, Hacienda, Fondos Europeos y Transformación Digital, por la que se convocan pruebas selectivas de acceso libre para cubrir5 plazas del Cuerpo Técnico, opción Archivos y Bibliotecas de la Administración Pública Regional. (Código BFX01L24-7)* y a su temario, publicado mediante la *Orden de 14 de mayo de 2025 de la Consejería de Economía, Hacienda, Fondos Europeos y Transformación Digital, por la que se aprueba el programa de materias específicas de las pruebas selectivas para ingreso en la Administración Pública Regional en el Cuerpo Técnico, opción Archivos y bibliotecas,* en la Región de Murcia.

Como se indica en la portada, se trata de un extracto del libro **Preservación digital: una visión desde la Gestión de la Información**, publicado en 2025 y disponible en libre abierto para su descarga.

En estas páginas se aborda parte del tema 45 de dicha convocatoria, recogiendo los siguientes aspectos:

- La preservación digital: introducción a la preservación digital y conceptos.
- Archivo digital: planificación de la preservación y el modelo OAIS, esencialmente.
- Metadatos de preservación: introducción, Dublin Core, PREMIS y METS.

Esto no quiere decir que el tema se delimite a las cuestiones aquí tratadas. Al contrario, puede ocurrir que el tribunal de la oposición considere oportunos otros elementos. Puedes ampliar información en la referencia indicada, recurrir a su amplio apartado de bibliografía o mediante búsquedas.

2. La preservación digital

La **preservación digital** se puede definir como *la combinación de políticas, estrategias y acciones que aseguran la integridad y el acceso a los contenidos reformateados* [digitalizados] *o nacidos digitalmente a lo largo del tiempo* (American Library Association (ALA), 2008) y consiste en *procesos destinados a garantizar la accesibilidad permanente de los objetos digitales* (UNESCO, 2003, p. 37). Debe formar parte de la gestión documental de cualquier organización (Castillo Segura, 2018, p. 11).

Ésta se rige por un conjunto de principios, que debe permear en todas y cada una de las acciones que realizamos y de las decisiones que tomamos con respecto a nuestros documentos. (Serra Serra, 2008), citado por (Castillo Segura, 2018) recoge y explica estos seis principios (ver **Tabla 1**).

Tabla 1. Principios de la preservación del patrimonio digital

Principio de integridad	Asegurar que el contenido informativo, la estructura lógica y el contexto no se han modificado ni se ha afectado el grado de fiabilidad ni la autenticidad del documento original.
Principio de equivalencia	Modificar la forma tecnológica sin alterar el valor evidencia de los documentos como medida para enfrentar la obsolescencia tecnológica y para garantizar el acceso a la información.
Principio de economía	Aplicar procesos, procedimientos, métodos y técnicas de preservación viables, prácticos y apropiados para el contexto de los documentos, asegurando la sostenibilidad técnica y económica de la preservación digital.
Principio de actualidad	Evolucionar al ritmo de la tecnología y utilizar los medios disponibles en el momento para garantizar la preservación de los documentos en el futuro. Un sistema de preservación digital debe mantener la capacidad de evolucionar, de ajustarse a los cambios dimensionales y de añadir nuevas prestaciones y servicios.
Principio de cooperación	Reutilizar y compartir soluciones ya existentes y desarrolladas de forma conjunta con otros archivos digitales, especialmente las relacionadas con los procesos que pueden gestionarse de forma centralizada.

Principio de normalización	Generar lineamientos y herramientas basadas en normas, estándares y buenas prácticas como apoyo a la gestión y preservación de los documentos digitales.

Fuente: elaborado por Castillo Segura (2018, p. 17), basado en Serra Serra (2008b)

2.1. Preservación digital como proceso transversal

Cualquier organización que realmente esté interesada en que sus documentos digitales puedan ser utilizados y comprendidos en el futuro debe buscar la forma de que la preservación digital esté presente en todos sus procesos documentales, desde el mismo momento en que se plantea la creación de un objeto digital hasta su destrucción o expurgo, si procede.

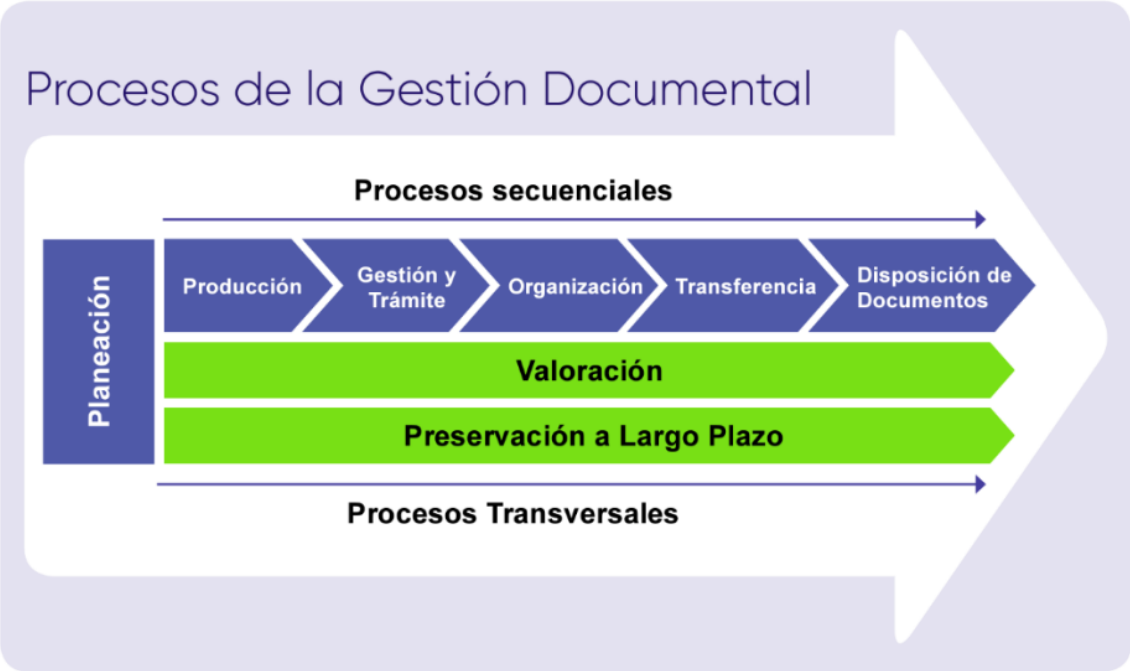

Figura 1. La preservación como proceso de gestión documental

La Figura 1, de (Castillo Segura, 2018, p. 11), muestra precisamente cómo tanto la valoración como la preservación a largo plazo (sea de documentación en papel o digital) son procesos transversales que, en mayor o menor medida, afectan o tienen repercusiones en el resto de los procesos de cualquier organización.

2.2. Riesgos y acciones de preservación digital

Los **riesgos** son situaciones potenciales a las que se enfrentan los contenidos y la información digital por su mera existencia, poniendo en cuestión su uso y acceso en cualquier momento. Ningún contenido digital,

por controlado y analizado que esté, está exento de riesgos. Se pueden destacar como riesgos la **obsolescencia tecnológica**, ya sea de los formatos, de los medios de representación (software) o del hardware: la **fragilidad de los soportes de almacenamiento**; la **pérdida de la integridad de los objetos digitales**; los **desastres naturales**; los **errores humanos**, incluyendo la falta de visión de la dirección de cualquier organización; el **exceso de información**; los **derechos de autoría**; los **ataques informáticos**; y la **falta de contexto** (metadatos).

Para hacer frente a estos riesgos, las organizaciones que apuestan por la preservación digital llevarán a cabo **acciones de preservación**, esto es, procedimientos que, aplicados sobre la información que preservar, intentan reducir o minimizar los riesgos a los que se exponen para asegurar que sigan siendo usables y accesibles. La propia gestión de la preservación, de hecho, también conlleva riesgos, ya que se pueden obviar riesgos, no detectarlos a tiempo, no realizar una buena planificación, etc.

Son acciones o medidas de preservación digital la migración de un formato de archivo a otro, incluyendo la normalización, que se utiliza al describir el proceso de migrar objetos digitales a un número limitado de formatos estándar; la preservación tecnológica, esto es, cuando se preserva el entorno tecnológico completo; la emulación, que implica que un sistema informático imite a otro sistema; la virtualización; la simulación; la traducción, la portabilidad; la preservación mediante el uso; las comunidades de prácticas; y las copias de seguridad que, si bien no operan directamente sobre los objetos digitales, tienen implicaciones directas sobre su preservación.

Tanto riesgos como acciones de preservación deben identificarse, analizarse y recogerse en el plan de preservación de la organización.

2.3. Otros conceptos importantes

2.3.1. Integridad, autenticidad y fiabilidad

Para la (UNESCO, 2015), la integridad, la autenticidad y la fiabilidad son los tres principios rectores de la preservación digital.

La **integridad** tiene que ver con que los documentos almacenados y gestionados en un sistema permanezcan intactos e inalterados en el tiempo. Es decir, que no se han modificado ni corrompido. La forma más común de asegurar la integridad de los ficheros es mediante el **hash** (también llamado huella digital, *checksum* o suma de verificación). Se trata de una *sucesión alfanumérica (letras y números) de longitud fija, que identifica o representa a un conjunto de datos determinados* (Signaturit Group, 2024) de tal forma que, si se comparan dos hashes que representan el mismo documento y son distintos es porque uno de los documentos se ha modificado o bien se ha producido un error, por ejemplo, durante su transmisión o almacenamiento.

La **autenticidad** tiene que ver con que los documentos almacenados y gestionados en un sistema son lo que pretenden ser, han sido creados o enviados por la persona que se presume y se han creado o enviados en el tiempo presumido (Cruz-Mundet, 2009). Las firmas electrónicas son uno de los componentes básicos de un documento digital en relación con su autenticidad, porque identifican al firmante de forma inequívoca. Por otro lado, en algunas administraciones se utiliza el CSV (Código Seguro de Verificación) como sistema que asegura la autenticidad de los documentos, aunque **sólo durante el tiempo que la resolución de conservación de CSV de la administración competente indique**, que puede ser 1, 3 o más años, o de forma indefinida.

En cuanto a la **fiabilidad**, es la propiedad o característica que indica que el contenido de un documento es una *representación completa y precisa de las actuaciones, las actividades o los hechos de los que da testimonio y al que se puede recurrir en el curso de posteriores actuaciones o actividades* (Ministerio de Hacienda y Administraciones Públicas, 2016, p. 36).

2.3.2. Copia máster y copia de difusión

Habitualmente, un objeto digital tendrá una o más copias y puede llegar a ser difícil saber cuál es el archivo original. En cualquier caso*, se debe seleccionar la mejor antes de transferir su contenido a otro formato* (Bradley et al., 2020, p. 13) con el objetivo de la preservación digital

siempre en mente. Es importante distinguir qué objetos se orientan a la preservación y cuáles a la difusión o a la distribución:

- La **copia máster o copia de preservación** es el objeto digital de mayor peso, con todos los metadatos posibles, sin recortes, orientada a su conservación a largo plazo.
- La **copia de difusión** se genera para compartir el objeto a través de las herramientas de difusión de que disponga el archivo. Es la reducción de datos común en la difusión de contenidos. Su uso para la preservación es contrario al principio ético de conservar la mayor cantidad posible de información primaria (2020, p. 20).

2.3. Las normas ISO relacionadas con la preservación digital

Existen varias normas ISO relacionadas con la preservación digital, entre las que se pueden destacar.

ISO 15489:2016. Información y documentación. Gestión de documentos (partes 1 y 2). Proporciona directrices respecto de la política de gestión documental, explica responsabilidades y resalta la importancia de la supervisión y auditoría («ISO/IEC 15489», 2021). Para (Potter, 2025a) recoge los fundamentos para identificar qué necesita preservarse.

ISO 14721:2025. Sistemas de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS). Modelo de referencia. Refleja un modelo conceptual para sistemas de preservación digital, incluyendo roles, funciones y flujos de trabajo (Potter, 2025a). La veremos en el último capítulo, dedicado a la planificación.

ISO 30301:2019. **Información y documentación. Sistemas de gestión para los documentos.** *Contempla la gobernanza organizacional de la gestión de documentos, integrando la preservación digital en la estrategia empresarial* (Potter, 2025a). En 2024 se modificó para incluir acciones relativas al cambio climático.

UNE-EN ISO/IEC 27001:2023. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la

seguridad de la información. Requisitos. *Especifica los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información en el contexto de la organización. También incluye los requisitos para la apreciación y el tratamiento de los riesgos de seguridad de información a la medida de las necesidades de la organización* (AENOR, 2023).

UNE-ISO/TR 15801:2019 IN. Gestión de documentos. Información almacenada electrónicamente. Recomendaciones sobre confiabilidad y fiabilidad. *Describe la implementación y manejo de los sistemas de gestión de información que almacenan y ponen a disposición para su uso información almacenada electrónicamente (IAE) de forma íntegra y fiable* (AENOR, 2019).

UNE-ISO 17068:2020. Información y documentación. Repositorio de tercero de confianza para documentos electrónicos. *Especifica requisitos de los RTC (repositorios de terceros de confianza) para apoyar el servicio de custodia autorizada, para salvaguardar la probable integridad y la autenticidad de los documentos electrónicos de los clientes y para servir como una fuente de* prueba *confiable* (AENOR, 2020).

ISO 16363:2025. **Space data and information transfer systems — Audit and certification of trustworthy digital repositories)** (ISO, 2025) es una norma internacional que define una *práctica recomendada para evaluar la confianza de los repositorios digitales. Es aplicable a la gama completa de repositorios digitales* (AENOR, 2017) y actúa sobre tres áreas: infraestructura organizacional, gestión de objetos digitales y tecnologías, infraestructura técnica y seguridad. La actualización de 2025 reemplaza a la de 2012, traducida al español mediante la UNE-ISO 16363: 2017. Los repositorios pueden certificarse por su cumplimiento.

UNE-ISO 16175:2021. Información y documentación. Procesos y requisitos funcionales para software para la gestión de documentos. Consta de dos partes: la **Parte 1: Requisitos funcionales y directrices asociadas para cualquier aplicación que gestione documentos electrónicos** *proporciona modelos, requisitos funcionales de alto nivel y directrices asociadas para aplicaciones de software destinadas a la gestión*

de documentos electrónicos (incluidas las copias digitales de documentos analógicos) (AENOR, 2021a); La **Parte 2. Guía para la selección, diseño, implementación y mantenimiento de software para la gestión de documentos**, *proporciona unas directrices para la toma de decisiones y los procesos asociados con la selección del diseño, implementación y mantenimiento del software de gestión de documentos, de acuerdo con los principios especificados en la Norma ISO 15489-1* (AENOR, 2021b).

ISO/TS 7538:2024. Requisitos funcionales para la disposición de documentos. Identifica el propósito y los beneficios de la disposición de documentos y proporciona a las organizaciones orientación sobre cómo gestionar los procesos relacionados (ISO, 2024).

UNE-CEN/TS 18170/2025. Requisitos funcionales para los servicios de archivo electrónico. Ratificada por AENOR en junio de 2025, especificará requisitos adicionales para servicios de confianza calificados o no calificados que implementen un servicio de archivo electrónico (AENOR, 2025; Comité Europeo de Normalización (CEN), 2025).

3. Archivo digital: planificación de la preservación y el modelo OAIS

La preservación digital no puede llevarse a cabo sin una correcta planificación que, según (Leija Román, 2023) tiene como referencia las políticas y los planes de preservación digital.

Las **políticas de preservación digital** especifican de forma general qué se va a preservar, quién es su responsable, dónde y por qué. En ellos, las instituciones declaran su compromiso con la preservación digital de sus contenidos y hacen explícitas las pautas básicas de actuación (REBIUN. Grupo de Trabajo de Repositorios, 2019).

Los **planes de preservación digital** describen los principios tecnológicos y las actuaciones técnicas en los que se basa la estrategia de preservación digital de la organización (REBIUN. Grupo de Trabajo de Repositorios, 2019). Según (Castillo Segura, 2018) *es una declaración escrita y autorizada por la alta dirección de la entidad. Establece el conjunto de acciones a corto, mediano y largo plazo que tienen como fin implementar los programas, estrategias, procesos y procedimientos tendentes a asegurar la preservación a largo plazo de los documentos electrónicos del archivo. Este plan se formula de conformidad con la política de preservación digital de la entidad y con instrumentos archivísticos como el diagnóstico integral*.

Para llevar a cabo la planificación de la preservación digital, podemos apoyarnos en modelos de gestión, como el modelo OAIS.

3.1. Modelos de gestión de documentos digitales. El modelo OAIS

El modelo OAIS es probablemente el modelo de gestión de documentos digitales más conocido. Tiene su origen en el *Consultative Committee for Space Data Systems* (CCSDS) y en sus recomendaciones para sistemas de información de archivos abiertos (*Open Archival Information System* en inglés). Éste *define los procesos necesarios para preservar y acceder a los objetos de información de forma efectiva y a largo plazo*, pero no especifica cómo hacerlo.

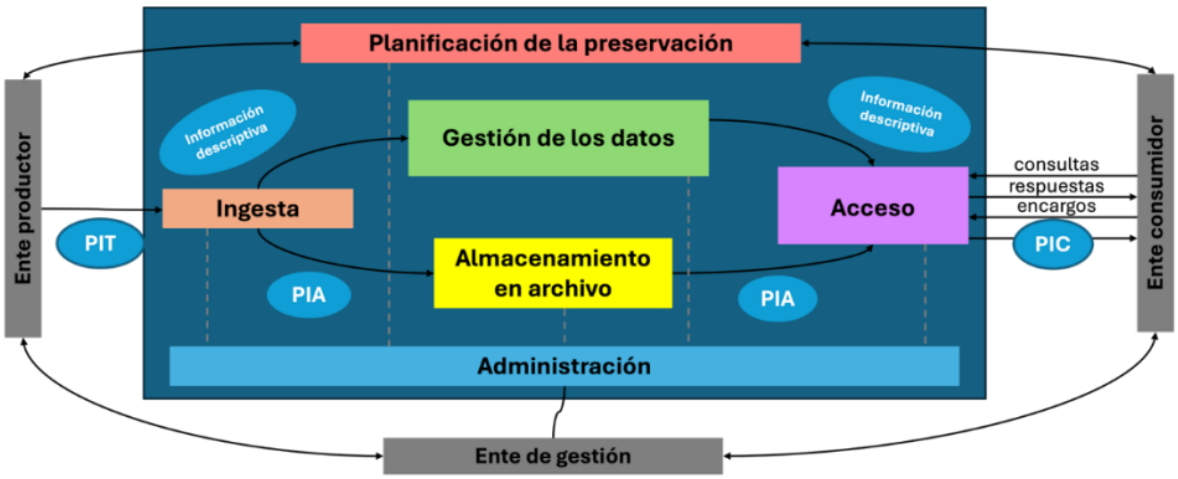

Figura 2. Modelo de entorno OAIS

Lo que hace es describir las funcionalidades básicas, los tipos de información requeridos para el entorno de preservación (Cruz-Mundet & Díez-Carrera, 2016), y quién interactúa en el mismo. La Figura 2, muestra el modelo OAIS, que aparece en las normas ISO 14721 y se mantiene en la recomendación práctica del CCSDS 650.0-M-3 (Consultative Committee for Space Data Systems (CCSDS), 2024, pp. 4-1).

En OAIS, se contemplan relaciones entre tres elementos:

- **Ente Productor**: personas o sistemas clientes que proporcionan información que conservar. Entre este ente y el órgano responsable del entorno OAIS existirá un Acuerdo de Envío.
- **Ente de Gestión**: papel desempeñado por quien establece la política general del OAIS como componente de una esfera política más amplia, esto es, la Dirección de una organización. Este rol es distinto de quien administra el día a día del OAIS, que está contemplado en la entidad funcional Administración.
- **Ente Consumidor**: personas o sistemas clientes que interactúan con los servicios OAIS para encontrar y recuperar aquella información conservada que le resulta de interés, ya sea mediante solicitudes ad hoc o basadas en eventos. Un tipo de ente consumidor es la

comunidad designada[1]. Entre este Ente y el órgano responsable del OAIS existirá un Acuerdo de Solicitud.

Sobre las **funciones**, para cumplir de forma fiable y sostenible con su propósito, un archivo digital debe atender seis entidades funcionales:

- **Ingesta o ingreso** (a veces también denominada "Captura de Datos"): proporciona los servicios y funciones necesarios para aceptar los PITs en el entorno OAIS desde un Ente Productor.
- **Almacenamiento en archivo**: proporciona los servicios y funciones necesarios para el almacenamiento, mantenimiento y recuperación de los PIAs, asegurando que sea un archivo fiable y seguro.
- **Acceso**: aporta los servicios y funciones necesarios para que los Entes Consumidores puedan determinar la existencia, descripción, ubicación y disponibilidad de la información almacenada en un OAIS y les permite solicitar y recibir PICs.
- **Administración**: proporciona los servicios y funciones necesarios para el funcionamiento general del entorno.
- **Gestión de datos**: proporciona los servicios y funciones requeridos para completar, mantener y acceder a la Información Descriptiva (que identifica y documenta los fondos del Archivo), así como a los datos administrativos empleados para la gestión del Archivo.
- **Planificación de la preservación**: aporta los servicios y funciones necesarios para supervisar el entorno OAIS, identificar riesgos, formular recomendaciones y proveer planes de preservación digital.

Ahora que entendemos la estructura básica y las relaciones de un PI, podemos ver las **variantes que admite el modelo OAIS**, que reflejan tres estados de la información:

---

[1] La comunidad designada también se ha denominado comunidad específica o comunidad de usuarios. En este documento se prefiere utilizar el término comunidad designada, por haberse generalizado más el término y ser inclusivo en cuanto al género de sus participantes.

- **PIT (Paquete de Información de Transferencia)** / SIP (*Submission Information Package*): es el paquete que transfiere el Ente Productor a un entorno OAIS. La mayoría de estos paquetes contienen alguna Información de Contenido y alguna Información Descriptiva del Paquete, dependiendo del acuerdo de envío entre el Ente Productor y el órgano responsable del entorno OAIS. Cuando un PIT ingresan en un entorno OAIS debe pasar por una serie de validaciones que aseguran su integridad, autenticidad e idoneidad con los requerimientos del modelo OAIS.

- **PIA (Paquete de Información de Archivo)** / AIP (*Archival Information Package*): se trata de un PI que está preservado en un entorno OAIS y que se compone de Información de Contenido e Información de Descripción de Preservación (IDP) (*Preservation Description Information*) (PDI). Al entrar en el entorno OAIS, uno o más PITs pueden transformarse en uno o varios PIAs para su preservación.

  Sólo cuando un Objeto de Datos es claramente definido, se puede evaluar la Información de Descripción de Preservación (IDP). Este tipo de información se debe proporcionar para preservar adecuadamente el Objeto de Datos y se orienta específicamente a la descripción del estado pasado y presente de la Información de Contenido, asegurando su identificación única y garantizando que no se haya alterado inconscientemente. Sólo aparece en los PIAs. Puede registrar información de cinco tipos:

  - **De Procedencia** (*Provenance*): describe la fuente del Objeto de Información, quién tiene su custodia desde su origen y su historia.
  - **De Contexto** (*Context*): describe cómo se relaciona el Objeto de Información con otra información externa al PI (por ejemplo, por qué se produjo) o con otros Objetos de Datos.
  - **De Referencia** (*Reference*): proporciona uno o más identificadores o sistemas de identificación, como un ISBN.
  - **De Integridad** (*Fixity*): recoge información sobre

mecanismos que aseguran que el Objeto de Información no haya sufrido cambios no documentados, como hashes, firmas electrónicas.

- **De Derechos de Acceso** (*Access Right*): establece las condiciones de acceso, incluyendo preservación, distribución y uso del Objeto de Información. Por ejemplo, contendría las declaraciones para otorgar permisos a OAIS para operaciones de preservación, ofertas de licencias (para distribución), especificaciones para medidas de cumplimiento de derechos, así como especificaciones de control de acceso.

Por otro lado, de los PIA pueden existir distintas versiones, como resultado de la modificación de la Información de Contenido o de la Información de Descripción de la Preservación (por la aplicación de estrategias de preservación).

- **PIC (Paquete de Información de Consulta)** / DIP (*Dissemination Information Package*): como respuesta a una solicitud de información, el entorno OAIS proporciona uno o más PICs, que se derivan de uno o más PIAs, con las restricciones necesarias de acuerdo con las condiciones de acceso definidas.

4. Metadatos de preservación digital

Son metadatos de preservación aquellos que incluyen *información sobre cualquier soporte no digital en el que se haya guardado el contenido, incluyendo su condición; el equipo de reproducción utilizado en el proceso de transferencia y sus parámetros; el equipo de captura utilizado, incluyendo el programa de reproducción conocido; información sobre el formato del fichero resultante, incluyendo la resolución digital; los operadores que participan en el proceso;* el checksum*, que permite la autentificación del fichero; detalles de cualquier fuente de información secundaria* y todos aquellos que proporcionan cualquier información contextual necesaria para proporcionar un acceso sostenible al contenido (Bradley et al., 2020, p. 24). Por supuesto, también son metadatos de preservación aquellos que recogen información de soportes digitales.

Si nos ceñimos a los metadatos más técnicos como, por ejemplo, aquellos que permiten *evaluar los parámetros técnicos de una grabación y sacar conclusiones adecuadas para el tratamiento de la preservación* (Bradley et al., 2020, p. 24) vemos que sólo con ellos podemos asegurar la reproducción fiel de la información contenida en los ficheros. Algunos metadatos son imprescindibles para hacer uso de un recurso digital, desde su lectura, con la mediación de un software y un hardware concretos, hasta su comprensión.

En preservación digital suelen utilizarse los siguientes, destacados entre otros por (Potter, 2025b) cita:

- **Dublin Core**[2]: es un esquema de metadatos empleado para la descripción de recursos desde hace más de 20 años. Consta de dos niveles: el simple (ver sección 3 de DCMI Metadata Terms), con 15 metadatos básicos para esa descripción; y el calificado, que amplía ese esquema con 40 nuevos elementos que refinan los anteriores. La siguiente tabla muestra los 55 elementos de DC calificado,

[2] DCMI Metadata Terms: http://purl.org/dc/elements/1.1/ The /elements/1.1/ (consulta: 23/07/2025).

indicando en negrita los que también forman parte del simple. La guía elaborada por (Alcaraz Martínez, 2023) explica perfectamente cómo funcionan tanto uno como el otro. También son relevantes ESE y EDM, que son esquemas utilizados para la agregación de contenido en Europeana.

Tabla 2. Metadatos del esquema Dublin Core calificado

abstract	**date**	isPartOf	references
accessRights	dateAccepted	isReferencedBy	**relation**
accrualMethod	dateCopyrighted	isReplacedBy	replaces
accrualPeriodicity	dateSubmitted	isRequiredBy	requires
accrualPolicy	**description**	issued	**rights**
alternative	educationLevel	isVersionOf	rightsHolder
audience	extent	**language**	**source**
available	**format**	license	spatial
bibliographicCitation	hasFormat	mediator	**subject**
conformsTo	hasPart	medium	tableOfContents
contributor	hasVersion	modified	temporal
coverage	**identifier**	provenance	**title**
created	instructionalMethod	**publisher**	**type**
creator	isFormatOf		

Fuente: (DCMI, 2020)

- **PREMIS** (*PReservation Metadata Implementation Strategies*): este estándar está ampliamente extendido como medio para dejar constancia de las actividades de preservación digital llevadas a cabo por una entidad. Incidiremos en el mismo en el siguiente apartado.

- **METS** (*Metadata Encoding and Transmission Standard*): es un marco estructural de metadatos para objetos digitales complejos. Sobre éste también dedicaremos un apartado específico en el último capítulo de la guía, ya que es utilizado en e-Arquiving.

Por supuesto, existen muchos otros esquemas de metadatos que pueden servir al fin de la preservación digital. De hecho, cualquier esquema que facilite la recogida de metadatos técnicos, administrativos y descriptivos, es útil para ello. Tanto es así que lo habitual es que las

organizaciones, sean las GLAM o las de cualquier otro tipo, utilicen conjuntos de metadatos, ya sean propios o no, estandarizados o no.

4.1. El esquema de metadatos PREMIS

El Diccionario de datos PREMIS indica que los metadatos de preservación *representan la información que la mayoría de los repositorios necesitan conocer para preservar materiales digitales a largo plazo* (BNE, 2015, p. 6). Lo cierto es que *la articulación más completa de los metadatos de preservación está representada por PREMIS* (PREservation Metadata: Implementation Strategies)*, producto de un grupo de trabajo internacional activo entre 2003 y 2005 y posteriormente actualizado y revisado por miembros de la comunidad de bibliotecas digitales* (Bradley et al., 2020, p. 24).

Los metadatos PREMIS son necesarios para asegurar la accesibilidad a largo plazo de los recursos digitales de cualquier repositorio, en la medida de lo posible. Además, permiten que los objetos sean autodescriptivos e interoperables con otros sistemas. Para ello, deben existir de manera independiente del sistema que los creó (Cabral Vargas, s.f.).

PREMIS representa información sobre 4 entidades, relacionadas entre sí, además de con las entidades intelectuales, para quien no define metadatos, pues ya existen otros metadatos descriptivos que se pueden emplear para esta cuestión (ver Figura 3, de (Caplan, 2009, p. 10)):

- **Objetos**: lo que se almacena y gestiona en el archivo. Pueden hacer referencia a otros Objetos o a Entidades Intelectuales (por ejemplo, un libro).
- **Eventos**: acontecimientos que afectan a los objetos. *Un registro preciso y fiable de los acontecimientos es crítico para el mantenimiento de la procedencia digital de un objeto lo que, a su vez, es importante para demostrar* [su] *autenticidad* (Caplan, 2009, p. 12). Se recomienda recoger al menos aquellas acciones que impliquen la modificación de un Objeto.

- **Agentes**: elementos que tienen un papel en estos acontecimientos y/o en las declaraciones de derechos. El Diccionario de Datos recoge únicamente tres unidades semánticas: identificador del agente, nombre y tipo (personas, organizaciones o aplicaciones informáticas).

- **Derechos y otras restricciones**: declaraciones de uno o de varios derechos pertenecientes a un Objeto o Agente. Cubren aspectos como el acceso al contenido (incluso al preservarlo, ya que esto puede implicar la realización de copias idénticas y versiones de objetos digitales), derechos de autoría u otro tipo de restricciones.

Los metadatos PREMIS muestran las relaciones entre las entidades que pueden representarse a través de este esquema, como puedes ver en la Figura 3.

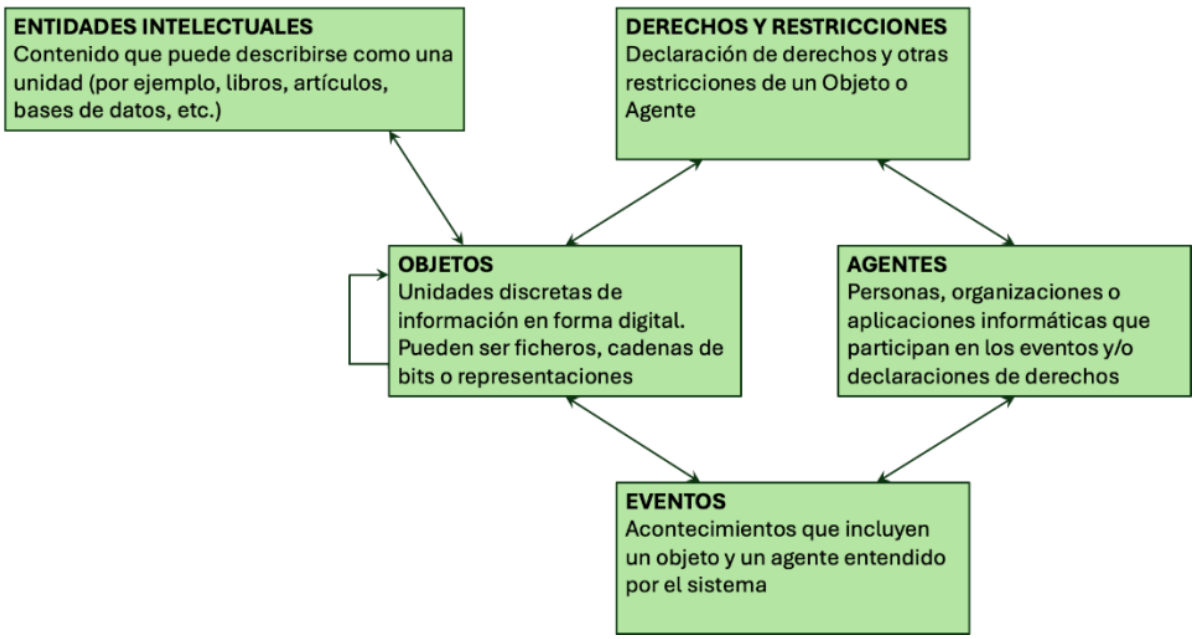

Figura 3. Elementos representados por PREMIS

En cuanto a los Objetos, en PREMIS pueden ser de tres tipos (BNE, 2015, p. 14): fichero, representación o cadena de bits.

- **Fichero**: un archivo de ordenador. Es una secuencia de bytes, con un nombre y orden, reconocida por un sistema operativo y que tiene un formato *y unos permisos de acceso además de las típicas características de sistema como tamaño y fecha de su última modificación*.

- **Representación**: conjunto de todos los objetos ficheros necesarios para reproducir o representar una entidad intelectual. Por ejemplo, un artículo de periódico puede estar compuesto por un único fichero PDF, que por sí solo constituye la representación; otro *puede constar de un fichero SGML y dos ficheros de imagen; estos tres ficheros constituyen la representación*.

- **Cadena de bits**: son subconjuntos de ficheros, datos (bits) dentro de un fichero que a) presenta propiedades comunes para los propósitos de preservación, y b) no puede ser autónomo sin añadir un fichero cabecera u otra estructura.

La relación entre estos tipos de Objetos se muestra en la Figura 4, cuya fuente es (PREMIS Editorial Committee, 2015).

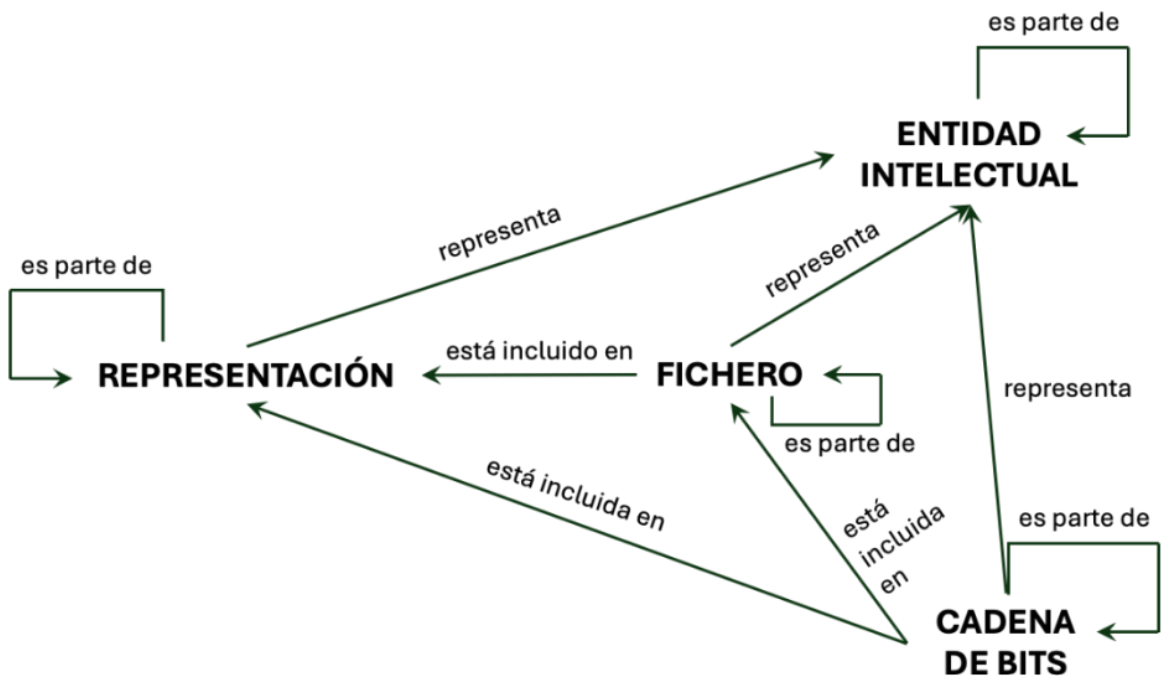

Figura 4. Tipos de objetos que pueden representarse con metadatos PREMIS

4.2. El esquema de metadatos METS

METS (*Metadata Encoding and Transmission Standard*) es un esquema XML utilizado para definir la estructura jerárquica de un objeto de un repositorio digital (AENOR, 2015). Habitualmente, se combina con otros esquemas para proporcionar la mayor cantidad de información posible

sobre dicho objeto. METS puede utilizarse en los paquetes generados siguiendo el modelo OAIS, por ejemplo.

Este estándar es mantenido por la METS Board y la Network Development and MARC Standards Office de la Library of Congress, aunque inicialmente surgió como iniciativa de la Digital Library Federation. En 2025 se liberó la versión 2 del esquema, que también se presentó en iPRESS 2024 (Elkiss et al., 2024).

Un paquete con METS versión 2 está compuesto por:

- Fichero/s de contenido: esto es, el objeto u objetos digitales de los que se generan metadatos en el propio paquete. Si son varios objetos, entre ellos suele existir algún tipo de relación, por ejemplo, entre las páginas de un libro digitalizado, donde cada página es un archivo de contenido y existe una relación de orden.
- Metadatos de diversos tipos, incluyendo metadatos de otros esquemas distintos a METS: estructurales, descriptivos, administrativos. La incorporación de estos tres tipos de metadatos es fundamental, según (Pulido Daza et al., 2024), para la gestión eficaz del patrimonio cultural digital, ya que facilita la recuperación y el acceso a la información y proporcionan un contexto esencial para la interpretación y uso de los documentos.

Cabe destacar que la versión 1 de METS sigue estando vigente y mantenida. De hecho, mucha de la documentación existente sigue apuntando únicamente a dicha versión[3]. Pasado un tiempo, la versión 2 acabará probablemente por imponerse puesto que, según sus creadores/as, *mejora la consistencia de los elementos; reduce la complejidad al eliminar ciertos conceptos que se incluyeron inicialmente, pero que rara vez se usaban; simplifica el esquema al eliminar dependencias*

[3] Merece particularmente la pena el tutorial en español que aloja la propia página oficial de METS para conocer la estructura de este esquema en su versión 1: https://www.loc.gov/standards/mets/METSOverview_spa.html (consulta: 13/08/2025).

externas; aumenta la flexibilidad para los atributos y sus valores (METS Editorial Board, 2025b).

4.2.1. Estructura de un fichero con METS versión 2

Un fichero XML hecho con METS versión 2 se estructura de la siguiente forma (Elkiss et al., 2024; METS Editorial Board, 2025a, 2025c) (ver también la Figura 5) en cuatro secciones:

- **<metsHdr>**: inicia la **sección** cabecera del fichero y contiene información sobre el propio documento METS, como su creador/a, editor/a, etc.
- **<mdSec>**: es la sección de metadatos del fichero XML, sobre el objeto METS y componentes fuente de los que procede. Aporta información de tipo descriptivo y técnico del *objeto fuente original del que deriva el objeto digital e información sobre la procedencia de los archivos que componen el objeto digital (es decir, relaciones entre archivos maestros y derivados, e información de migración/transformación)* (METS Editorial Board, 2025a). Es un elemento repetible. Se divide en subsecciones, también repetibles, para distintos tipos de metadatos, como descriptivos, técnicos, sobre derechos de propiedad intelectual, sobre fuentes analógicas/digitales y de procedencia digital.
- **<fileSec>:** sección de ficheros o de archivos de contenido que componen el objeto digital que se describe en el documento METS. Persigue proporcionar un inventario y ubicación de estos.
- **<structSec>**: esta sección permite definir una o más estructuras jerárquicas, de acuerdo con diferentes criterios.

De entre todos los elementos contemplados por METS versión 2, existen 10 obligatorios y 89 opcionales. (Elkiss et al., 2024) muestran la estructura de un documento METS 2, donde el objeto digital incluye un documento de Word, un documento PDF/A derivado del documento de Word y una presentación de PowerPoint; así como metadatos descriptivos

en Dublin Core asociados al contenido y metadatos de preservación (PREMIS) que describen la transformación de DOCX a PDF/A.

La siguiente figura, elaborada por (Elkiss et al., 2024), muestra los componentes de un documento XML elaborado con METS2 de forma gráfica y su relación con los objetos digitales sobre los que trata.

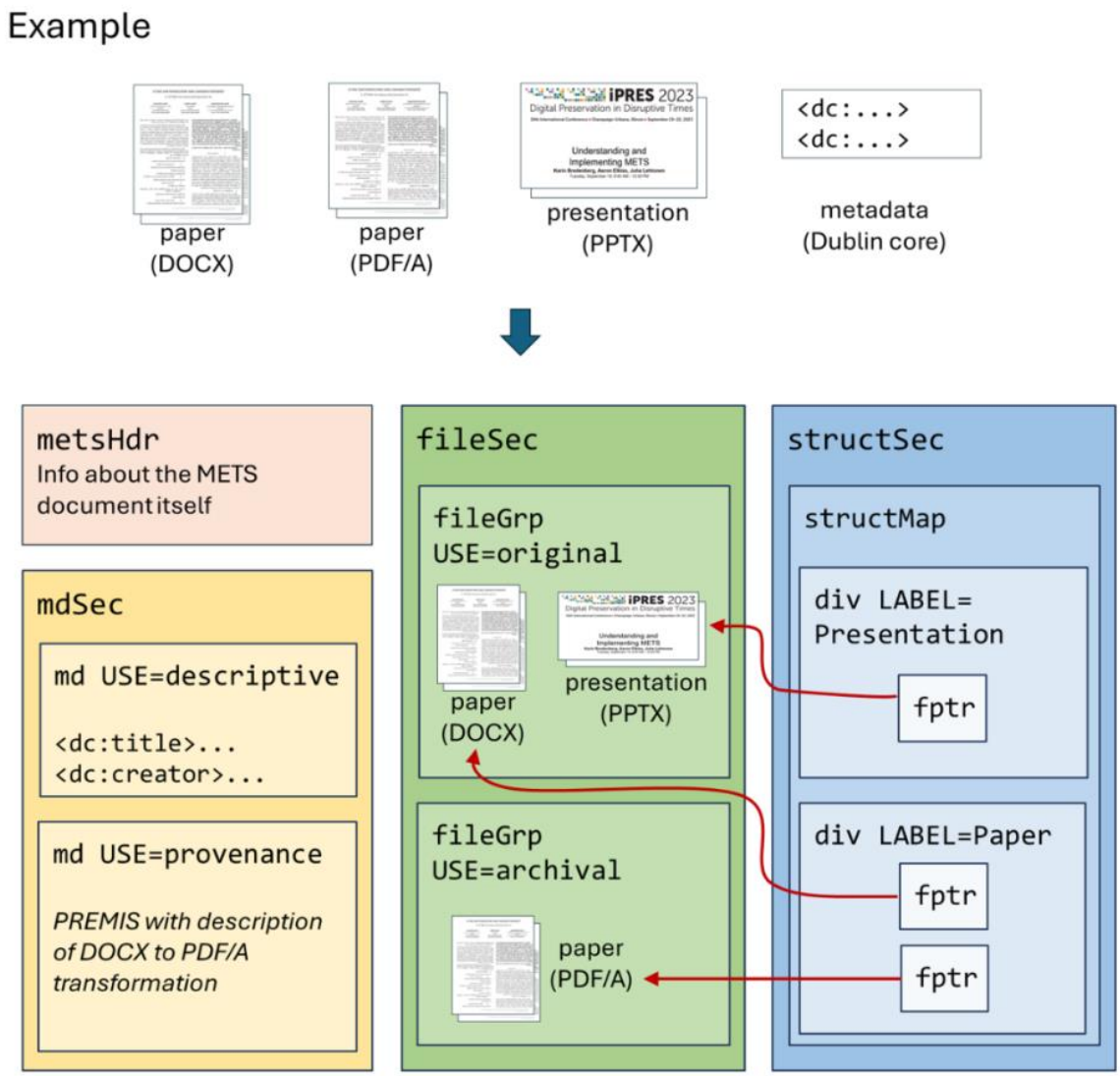

Figura 5. Estructura de un documento METS2

Referencias bibliográficas

AENOR. (2015). UNE-ISO 14721:2015. Sistemas de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS). Modelo de referencia. https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0055413

AENOR. (2017). UNE-ISO 16363:2017. Sistemas de transferencia de información y datos espaciales. Auditoría y certificación de repositorios digitales de confianza. https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0058850

AENOR. (2019). UNE-ISO/TR 15801:2019 IN Gestión de documentos. Información al... https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0062170

AENOR. (2020). UNE-ISO 17068:2020. Información y documentación. Repositorio de tercero de confianza para documentos electrónicos. https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0063117

AENOR. (2021a). UNE-ISO 16175-1:2021. Información y documentación. Procesos y requisitos funcionales para software para la gestión de documentos. Parte 1: Requisitos funcionales y directrices asociadas para cualquier aplicación que gestione documentos electrónicos. https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0067981

AENOR. (2021b). UNE-ISO/TS 16175-2:2021. Nformación y documentación. Procesos y requisitos funcionales para software para la gestión de documentos. Parte 2: Guía para la selección, diseño, implementación y mantenimiento de software para la gestión de documentos. https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0067978

AENOR. (2023). UNE-EN ISO/IEC 27001:2023. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma/?c=N0071764

AENOR. (2025). UNE-CEN/TS 18170:2025. Requisitos funcionales para los servicios de archivo electrónico. https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0074502

Alcaraz Martínez, R. (2023). Dublin Core: Guía de uso. OMADO (Objectes i MAterials DOcents), 20.

American Library Association (ALA). (2008). Definitions of digital preservation. http://hdl.handle.net/11213/1587

BNE. (2015, octubre 16). Diccionario de datos PREMIS. De Metadatos de Preservación. Versión 2.0. https://www.bne.es/es/publicaciones/diccionario-datos-premis

Bradley, K., Fleischhauer, C., Gaustad, L., Gordon, B., Prentice, W., Schüller, D., & Sjøberg, T. (2020). La salvaguarda del patrimonio audiovisual: Ética, principios y estrategia de preservación (IASA-TC 03). IASA-TC 03. https://www.iasa-web.org/sites/default/files/downloads/publications/TC03_4th_edition_Spanish.pdf

Cabral Vargas, B. (s.f.). Metadatos para la Preservación Digital: PREMIS en la versión 3.0. 42.

Caplan, P. (2009). Entender PREMIS. Library of Congress Network Development and MARC Standards Office. https://www.loc.gov/standards/premis/UnderstandingPREMIS_espanol.pdf

Castillo Segura, C. C. (2018). Fundamentos de preservación digital a largo plazo. Archivo General de la Nacional de Colombia. Archivo General de la Nación de Colombia. https://www.archivogeneral.gov.co/caja_de_herramientas/docs/6.%20pr

eservacion/DOCUMENTOS%20TECNICOS/FUNDAMENTOS%20PRESERVACION%20DIGITAL%20LARGO%20PLAZO.pdf

Comité Europeo de Normalización (CEN). (2025). CEN/TS 18170:2025. https://tienda.aenor.com/norma-cen-ts-18170-2025-80628

Consultative Committee for Space Data Systems (CCSDS). (2024). Reference Model for an Open Archival Information System (OAIS). Recommendation for Space Data System Practices (Recommended Practice No. CCSDS 650.0-M-3; Magenta Book, p. 150). CCSDS Secretariat. https://ccsds.org/wp-content/uploads/gravity_forms/5-448e85c647331d9cbaf66c096458bdd5/2025/01//650x0m3.pdf

Cruz-Mundet, J. R. (2009). La gestión de los documentos electrónicos como función archivística. Revista del Archivo Nacional, 73(1-12), 29-56.

Cruz-Mundet, J. R., & Díez-Carrera, C. (2016). Sistema de Información de Archivo Abierto (OAIS): Luces y sombras de un modelo de referencia. Investigación Bibliotecológica: Archivonomía, Bibliotecología e Información, 30(70), 221-247. https://doi.org/10.1016/j.ibbai.2016.10.010

DCMI. (2020, enero 20). DCMI Metadata Terms. Dublin Core. https://www.dublincore.org/specifications/dublin-core/dcmi-terms/

Elkiss, A., Bredenberg, K., Hofsink, I., Lehtonen, J., Nef, A., Steinke, T., & Wendler, R. (2024, septiembre 3). Metadata Encoding and Transmission Standard (METS) Version 2. https://doi.org/10.5281/zenodo.13646107

ISO. (2024). ISO/TS 7538:2024. https://www.iso.org/standard/83150.html

ISO. (2025). ISO 16363:2025. Space data and information transfer systems. Audit and certification of trust-worthy digital repositories. https://tienda.aenor.com/norma-iso-16363-2025-087472

ISO/IEC 15489. (2021). En Wikipedia. https://es.wikipedia.org/w/index.php?title=ISO/IEC_15489&oldid=140440656

Leija Román, D. A. (2023). La política de preservació digital: Models i elements clau per redactar-la. BiD: textos universitaris de biblioteconomia i documentació, 50.

METS Editorial Board. (2025a). METS Version 2: An Overview & Tutorial. METS. https://mets.github.io/metsoverview.html

METS Editorial Board. (2025b, marzo 3). METS 2 Schema Now Available. METS News and Announcements. https://www.loc.gov/standards/mets/news030325.html

METS Editorial Board. (2025c, marzo 10). METS: Metadata Encoding and Transmission Standard, version 2. https://loc.gov/standards/mets/mets2.xsd

Ministerio de Hacienda y Administraciones Públicas. (2016). DOCUMENTO ELECTRÓNICO. Guía de aplicación de la Norma Técnica de Interoperabilidad de Documento electrónico. 2ª edición electrónica. https://www.hacienda.gob.es/SGT/catalogo_sefp/244_guia_aplicacion_nti_accesible.pdf

Potter, A. (2025a, abril 27). Navigating the Archipelago of Digital Preservation Standards [Substack newsletter]. Andrew Potter. https://metaarchivist.substack.com/p/navigating-the-archipelago-of-digital

Potter, A. (2025b, mayo 5). Digital Preservation in 2025 [Substack newsletter]. Andrew Potter. https://metaarchivist.substack.com/p/digital-preservation-in-2025

PREMIS Editorial Committee. (2015). PREMIS Data Dictionary for] Preservation Metadata, Version 3.0. https://www.loc.gov/standards/premis/v3/premis-3-0-final.pdf

Pulido Daza, N. J., Bustos Ríos, M. A., Cabrera Carranza, A. C., & Rengifo Reyes, E. E. (2024). La preservación digital sostenible – PPREDIS como herramienta para garantizar la protección y accesibilidad del patrimonio cultural documental. Culturas. Revista de Gestión Cultural, 11, 85-97. https://doi.org/10.4995/cs.2024.22417

REBIUN. Grupo de Trabajo de Repositorios. (2019). Informe sobre la evaluación del estado de la preservación de los repositorios REBIUN 2018. http://hdl.handle.net/20.500.11967/253

Serra Serra, J. (2008). Los documentos electrónicos: Qué son y cómo se tratan. Trea. https://trea.es/producto/los-documentos-electronicos-que-son-y-como-se-tratan/

Signaturit Group. (2024, febrero 12). ¿Qué es un hash y cómo funciona? https://www.signaturit.com/es/blog/que-es-un-hash/

UNESCO. (2003). Carta para la preservación digital de la UNESCO. Actas de la Conferencia General, 32a reunión, París, 29 de septiembre-17 de octubre de 2003, v. 1: Resoluciones. https://unesdoc.unesco.org/ark:/48223/pf0000133171_spa.page=85

UNESCO. (2015). Recomendación relativa a la preservación del patrimonio documental, comprendido el patrimonio digital, y el acceso al mismo. https://www.unesco.org/es/legal-affairs/recommendation-concerning-preservation-and-access-documentary-heritage-including-digital-form