ENCUENTRO LATINOAMERICANO DE INNOVACIÓN EN EDUCACIÓN SUPERIOR

10 - 11 Octubre 2019 Bogotá D.C.

¿Y tu repositorio institucional está certificado?

Parte 2

Octubre de 2019

Dra. Marisa R. De Giusti

PREBI-SEDICI- UNLP

CESGI-CIC

UNIVERSIDAD NACIONAL DE LA PLATA

CESGI Centro de Servicios en Gestión de Información cesgi.cic.gba.gob.ar

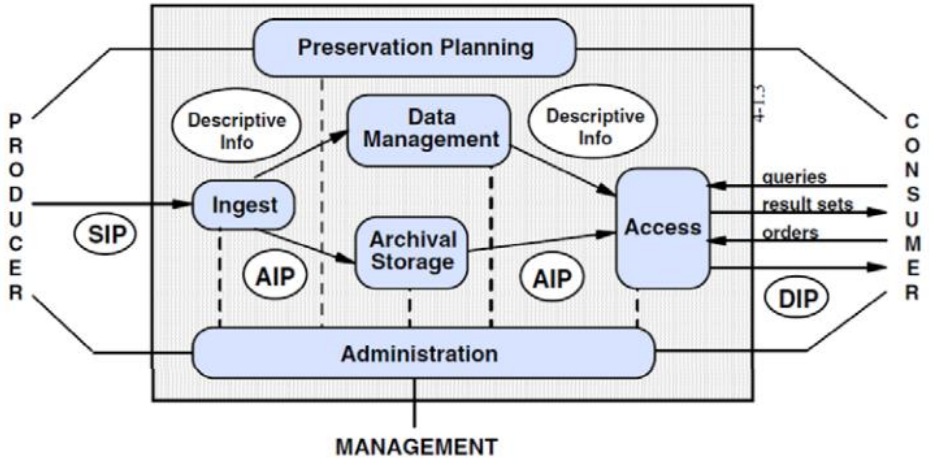
PREBI SEDICI prebi.unlp.edu.ar sedici.unlp.edu.ar

COMISIÓN DE INVESTIGACIONES CIENTÍFICAS Ministerio de Ciencia, Tecnología e Innovación

Marco normativo: ISO 14721

¿La aplicación del modelo OAIS garantiza la creación de repositorios confiables?

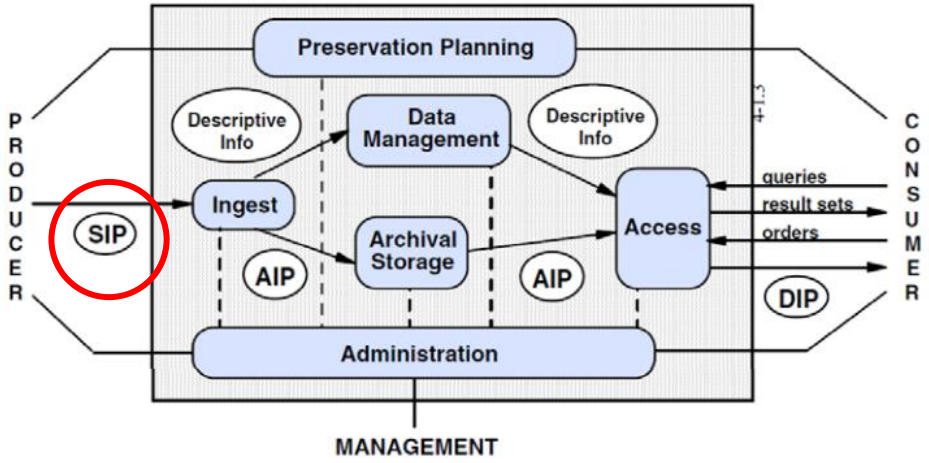
¿Una institución que implementa el modelo OAIS puede asegurar la confiabilidad, integridad, autenticidad y usabilidad de sus documentos digitales en el futuro?



Marco normativo: ISO 14721

Paquete de Información de Transferencia (SIP) (submission information package (SIP)):

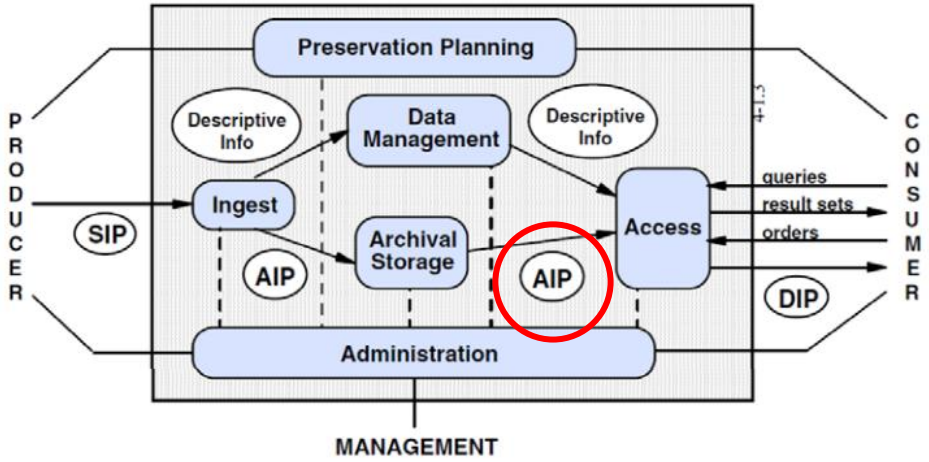
Paquete de Información que se entrega por el Productor al OAIS para usarlo en la construcción o actualización de uno o más AIP y/o la Información de Descripción asociada.



Marco normativo: ISO 14721

Paquete de Información de Archivo (PIA), Archival information package (AIP)

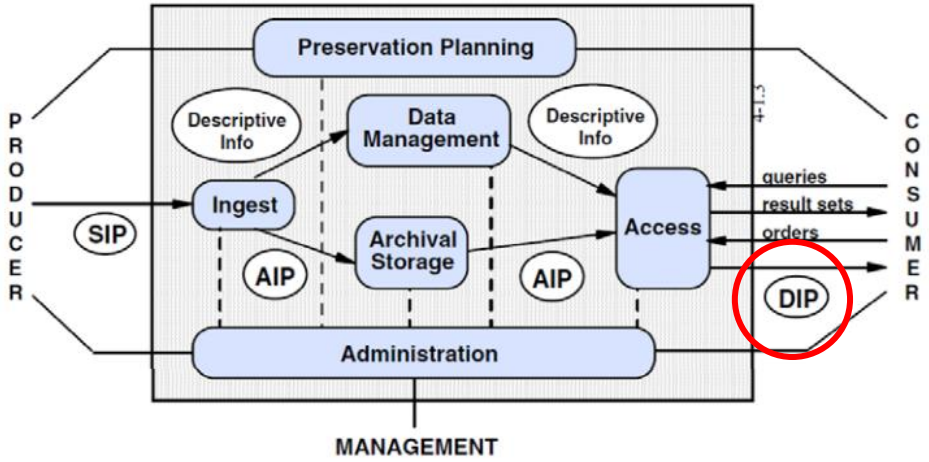
Paquete de Información, que se conserva en un OAIS, y que consta de la Información de Contenido y de la Información de Descripción de Conservación (PDI) asociada.



Marco normativo: ISO 14721

Paquete de Información de Consulta (PIC) (dissemination information package (DIP):

Un Paquete de Información, derivado de uno o más AIP, y enviado por el Archivo al Usuario en respuesta a su solicitud al OAIS.



Guía de normas para evaluar la confiabilidad de un repositorio

2002: Trusted Repositories Attributes & Responsibilities. TRAC.
TRAC hoy: https://www.crl.edu/sites/default/files/d6/attachments/pages/trac_0.pdf
2005: RLG/NARA Draft Audit Check-list for Repository Certification.
2006-2007: CRL and DCC Pilot Repository Audits. Después Drambora.
Dec 2006: Catalogue of Criteria for Trusted Digital Repositories published (in English) by Nestor
Feb 2007: Digital Repository Audit Method Based on Risk Assessment (DRAMBORA) published by CRL and OCLC. Glasgow, 2009.
2007: Birds of a Feather group of audit checklist standardisation. Sección 5 del Modelo OAIS
Mar 2008: DRAMBORA Interactive released
May 2008: Data Seal of Approval by DANS
Nov 2008: Version 2 of the Nestor repository criteria
Oct 2009: CCSDS draft standard on Repository Certification. De aquí se desprende la ISO 16363.
Jan 2010: CRL. Certification and assessment of digital repositories
DINI Certificate for Open Access Repositories and Publication Services 2016.
2017: UNE - ISO 16363. Versiones previas.
RDA: RDA/WDS Certification of Digital Repositories IG
Certification and Assessment of Digital Repositories 6 repositorios certificados
2017: CORE TRUST SEAL: https://www.coretrustseal.org/why-certification/requirements/

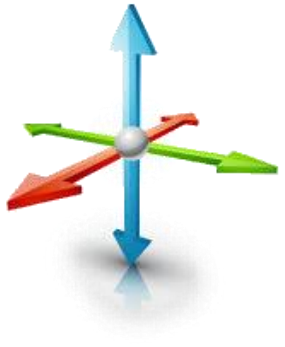
A destacar

Las normas que permiten auditar y certificar un repositorio se basan en la definición de repositorio dada por la ISO 14721, esto no sólo significa que adhieren a la misma definición de OD, sino que, fundamentalmente para esta presentación que asumen que un repositorio es una organización (constituída por personas y tecnología) que se define por su capacidad para asegurar la preservación y el acceso y uso a largo plazo de los objetos digitales.

A destacar: ejes

Parece claro entonces que se tienen que revisar elementos que están vinculados a la organización en sí misma (personas y tecnología) y funciones/procesos/procedimientos que aseguren que el repositorio cumpla con su objetivo más allá de los cambios tecnológicos y los cambios en la comunidad designada.

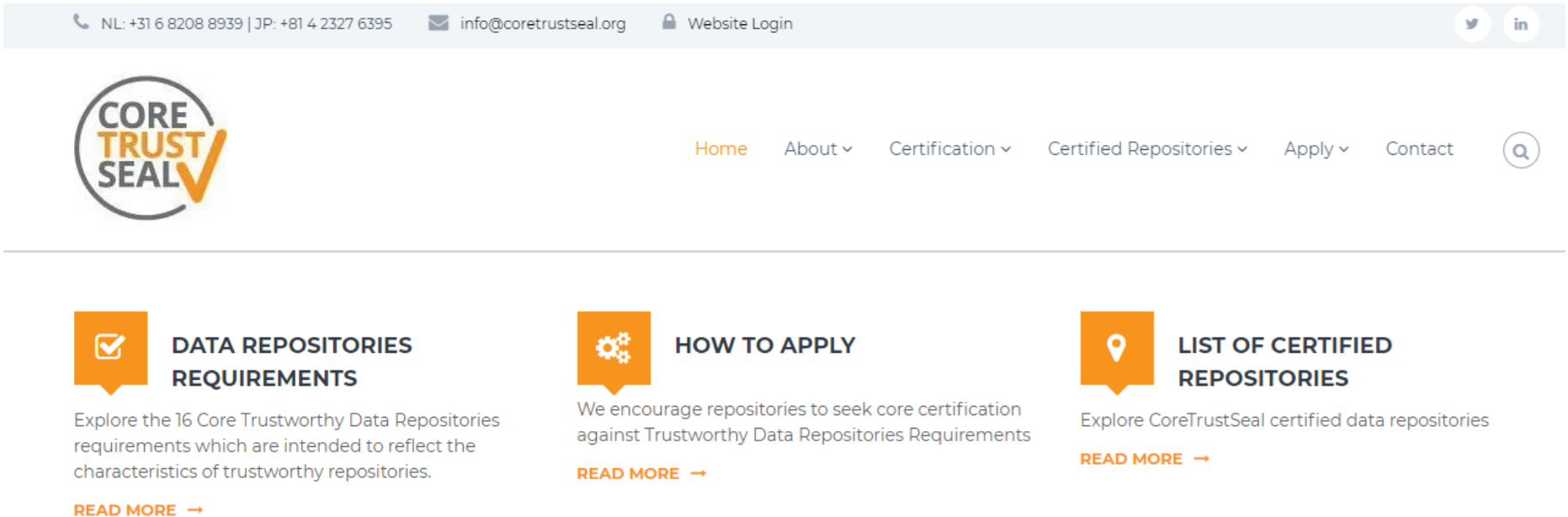
Lo importante en este camino es ir de un modelo de menor a mayor pero que contemple con complejidad creciente los tres aspectos.

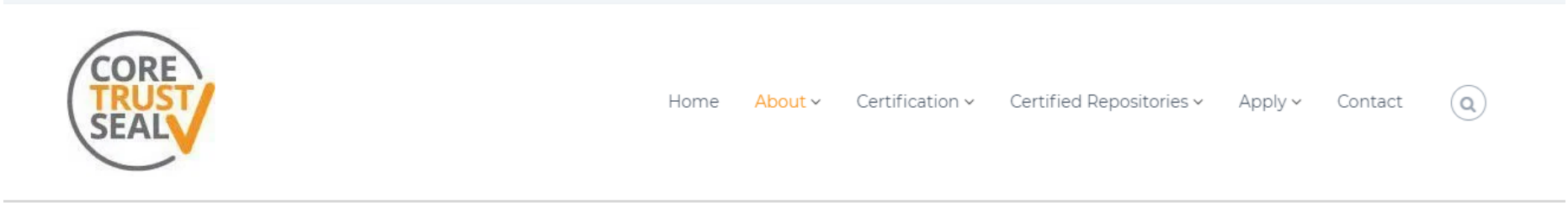


Auditoría

Sin importar el tamaño o propósito del repositorio, se debe alentar la utilización de una lista de verificación como una herramienta para la evaluación objetiva, interna o externa, y sin importar si se cumple para reunir información local, evaluación o como parte de un proceso de certificación. La auditoría es la base para comparar las capacidades con un conjunto de criterios centrales para un repositorio digital confiable. La certificación es un paso adicional que algunos repositorios tomarán y / o deberán tomar para el reconocimiento formal y objetivo.El resultado de cualquier auditoría debe verse en el contexto en el que se realizó.

Auditoría y certificación


NL: +31 6 8208 8939 | JP: +81 4 2327 6395
info@coretrustseal.org
Website Login
CORE TRUST SEAL
Home
About
Certification
Certified Repositories
Apply
Contact
DATA REPOSITORIES REQUIREMENTS
Explore the 16 Core Trustworthy Data Repositories requirements which are intended to reflect the characteristics of trustworthy repositories.
READ MORE
HOW TO APPLY
We encourage repositories to seek core certification against Trustworthy Data Repositories Requirements
READ MORE
LIST OF CERTIFIED REPOSITORIES
Explore CoreTrustSeal certified data repositories
READ MORE



La certificación CoreTrustSeal se visualiza como el primer paso en un marco global para la certificación de repositorio que incluye la certificación de nivel extendido (Nestor-Seal DIN 31644) y la certificación de nivel formal (ISO 16363). CoreTrustSeal también certifica nivel básico para otras entidades de investigación, como servicios de datos y software.

No hay visita y toda la evidencia debe ser pública.

Los requisitos básicos de los repositorios de datos confiables están destinados a reflejar lo que caracteriza a los repositorios confiables, por lo tanto todos los requisitos son obligatorios y son elementos independientes igualmente ponderados.

Hay diferentes niveles de cumplimiento: 0 – Not applicable 1 – The repository has not considered this yet 2 – The repository has a theoretical concept 3 – The repository is in the implementation phase 4 – The guideline has been fully implemented in the repository.

Aspectos

Infraestructura organizacional: misión, licencias, accesos, confidencialidad, infraestructura, orientación experta.

Gestión del objeto digital: gestión de los datos y autenticidad, evaluación de los datos, procedimientos de almacenamiento documentados, plan de preservación, calidad de los datos, flujos de trabajo, descubrimiento e identificación de los datos.

Tecnología: infraestructura tecnológica y seguridad.

Directrices seleccionadas para la evaluación

- TRAC Base de ISO 16363
- DINI
- NESTOR
- ISO 16363

Center for Research Libraries
GLOBAL RESOURCES NETWORK

Search CRL catalog

catalog website browse catalog

About | Membership | Collections | Electronic Resources | Services | Archiving & Preservation | Collaborations

Archiving & Preservation

- Overview
- **Digital Preservation**
  - Certification & Assessment of Digital Repositories
  - **Metrics**
  - Other Reports and White Papers
- Print Preservation

TRAC Metrics

The *Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC)*, is the principle tool used by CRL in its auditing and certification of digital repositories. TRAC criteria measure the ability of a given repository to preserve digital content in a way that serves the repository's stakeholder community.

TRAC metrics are based on the **OAIS** reference model/ **ISO 14721:2012 standard**. This standard was developed through the Consultative Committee for Space Data Systems (CCSDS) and a task force under the auspices of OCLC's Research Libraries Group (RLG) and the National Archives and Records Administration (NARA). The final version of TRAC was revised by the Center for Research Libraries and the Research Libraries Group (RLG) after jointly conducting test audits of several digital repositories in 2005-2006. The final version of the TRAC checklist was published in 2007 by CRL and RLG. The full **TRAC** document in PDF format is available on the CRL website.

A list of the TRAC metrics, with examples of the types of evidence of compliance with those metrics, is found below. Many of the concepts and terms used in TRAC are defined in the **OAIS Reference Manual** (ISO 14721:2012).

TRAC: AUDIT & CERTIFICATION CRITERIA

A. Organizational Infrastructure

A1. Governance & organizational viability
A2. Organizational structure & staffing
A3. Procedural accountability & policy framework
A4. Financial sustainability
A5. Contracts, licenses, & liabilities

B. Digital Object Management

B1. Ingest: acquisition of content
B2. Ingest: creation of the archivable package
B3. Preservation planning
B4. Archival storage & preservation/maintenance of AIPs
B5. Information management
B6. Access management

C. Technologies, Technical Infrastructure, & Security

C1. System infrastructure
C2. Appropriate technologies
C3. Security

La lista de verificación se divide en tres secciones:

A. Infraestructura organizacional.

B. Gestión de objetos digitales

C. Tecnologías, infraestructura técnica y seguridad.

Certificado DINI

DEUTSCHE INITIATIVE
FÜR NETZWERKINFORMATION E.V.

DINI (2006) se funda en las universidades alemanas con el fin de mejorar los servicios de información. Crean un certificado que es aplicable sobre repositorios de AA con 8 dimensiones y dentro de cada una aspectos obligatorios (M) y otros recomendados (R):

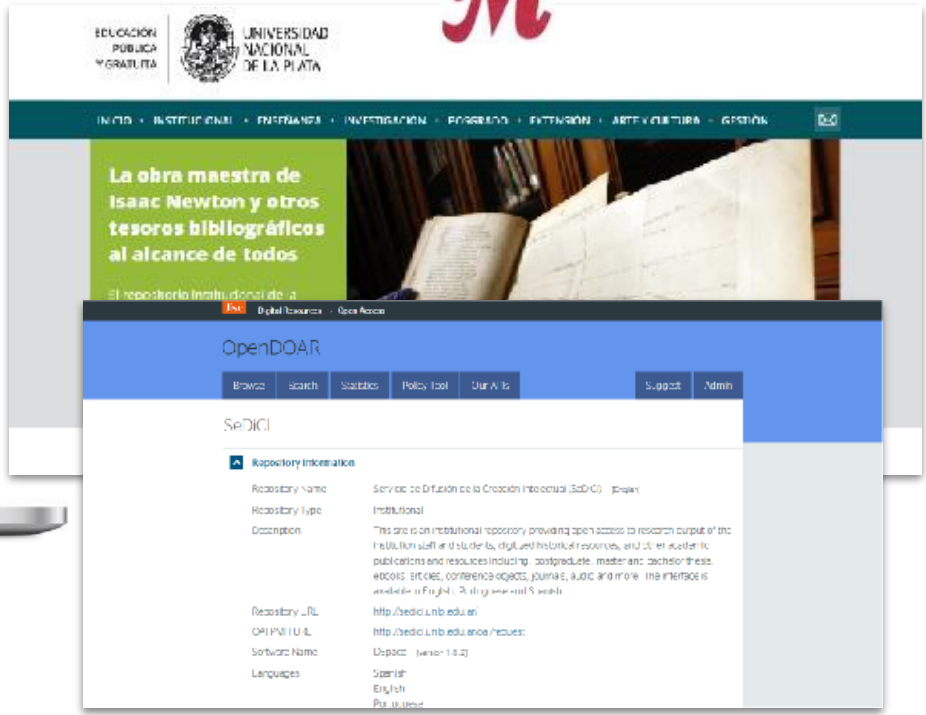
- Visibilidad del servicio,
- políticas,
- soporte para autores y editores,
- aspectos legales,
- seguridad de la información,
- indexación e interfases,
- acceso a estadísticas y
- disponibilidad a largo plazo.

Aunque sólo sirve para Alemania resulta muy útil

1 Visibilidad del servicio

Una mayor **visibilidad** y potencialmente un mayor reconocimiento son ventajas características de las publicaciones electrónicas, en especial las que están en acceso abierto. Para extraer el máximo beneficio de este potencial, debe difundirse ampliamente el rango completo de ofertas de un repositorio. Debe ser visible no sólo para el usuario inmediato e individual –con independencia de si uno quiere leer una publicación concreta o emplearla de alguna otra manera, o si uno quiere publicar un documento– sino también para servicios externos tales como motores de búsqueda u otros servicios referenciales. Además de las interfaces técnicas necesarias es fundamental el registro de un servicio local con las pertinentes agencias.

1 Visibilidad del servicio



http://sedici.unlp.edu.ar/handle/10915/66517

20

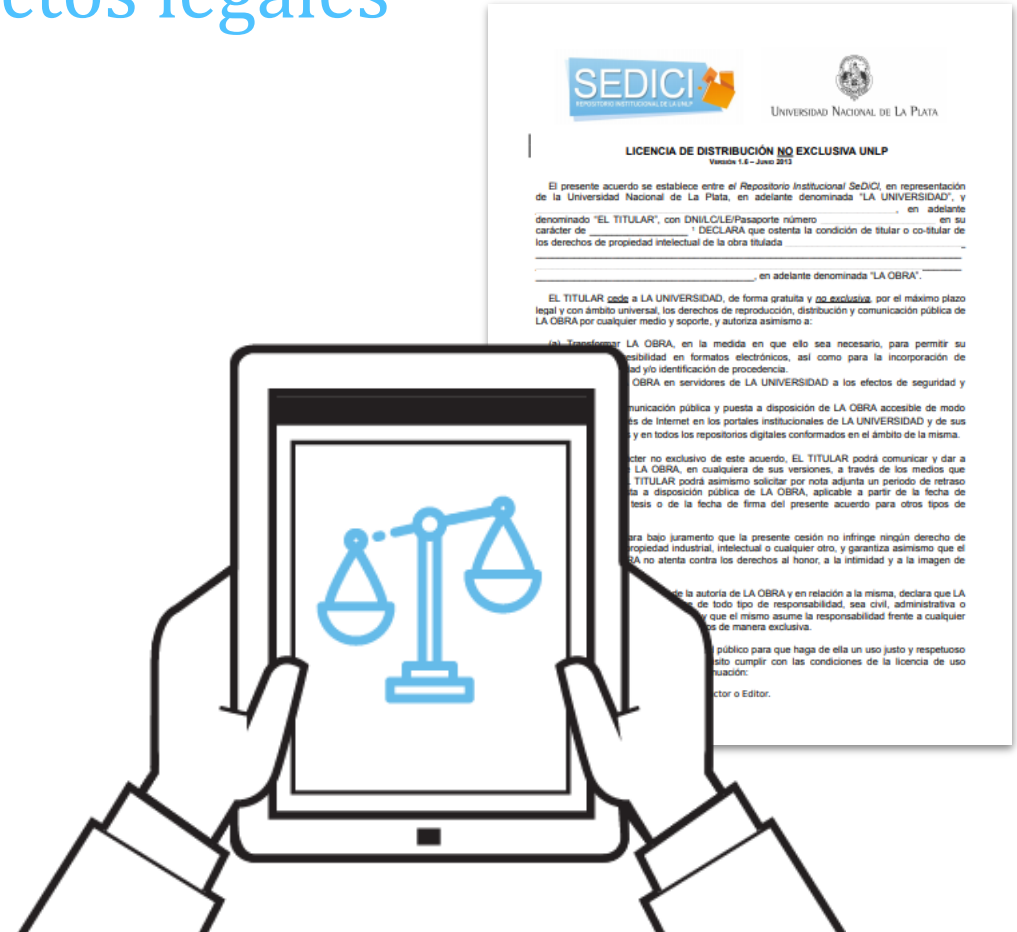
2 Políticas

La **fiabilidad** y la **transparencia** juegan un papel primordial en la provisión de Servicios de Documentación y Publicaciones. Es crucial para el respectivo proveedor de servicios **describir claramente los servicios ofertados y realizar declaraciones sobre los criterios relacionados con los contenidos** y sobre las **operaciones técnicas** (por ejemplo sobre tipos de documentos, usuarios a los que se dirige, sostenibilidad del servicio) a través de una política públicamente disponible.

3 Asesoramiento a autores y editoriales

El objetivo es **apoyar el proceso completo de publicación** en el marco del Servicio de Documentación y Publicaciones. Para aquellos que hagan uso de los servicios para publicar (i. e. autores y editoriales allí donde sea aplicable) es importante facilitar información visible y bien estructurada, que dé respuesta a las preguntas más relevantes sobre publicación electrónica. Las páginas importantes deben estar accesibles desde la web del Servicio de Documentación y Publicaciones y pueden adicionalmente estar disponibles en otros formatos (p. ej. tarjetas o folletos). La información puede incluir recursos externos.

4 Aspectos legales



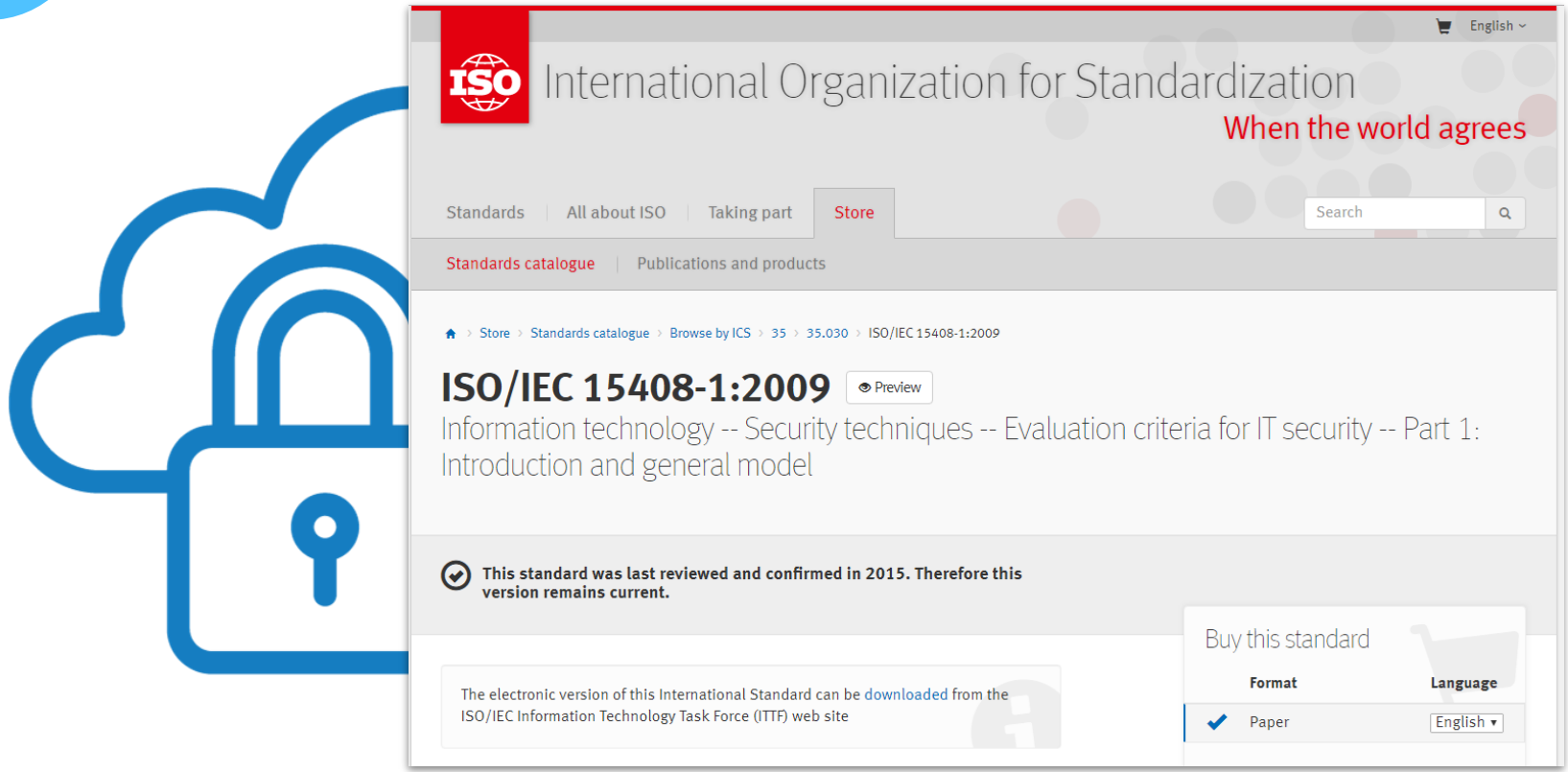
4 Aspectos legales

El proveedor de un Servicio de Documentación y Publicaciones precisa de ciertos derechos de uso para ofrecer documentos al público y para facilitar su archivo a largo plazo. Estos derechos deben ser concedidos por el/los autor/es y el/los editor/es. Esto se realiza a través de un acuerdo formal, la llamada **licencia de depósito.** En este acuerdo debe regularse asimismo que *no se infringen los derechos de tercera parte alguna y que el proveedor del servicio está exento de cualquier responsabilidad en el caso de que se infringieran tales derechos de terceras partes*. Se recomienda a todos los proveedores de un Servicio de Documentación y Publicaciones colaborar con el departamento legal de su institución y recabar asesoramiento profesional adicional cuando haya que tratar con aspectos legales.

5 Seguridad de la información

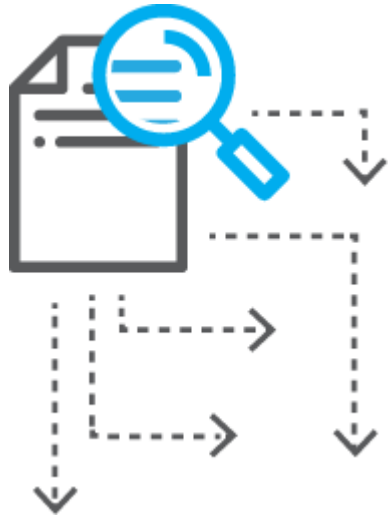
Para garantizar un Servicio de Documentación y Publicaciones fiable que satisfaga los requisitos generales de la publicación científica, el sistema técnico subyacente y la estructura de la organización deben cumplir criterios básicos con respecto a la **seguridad de la información**. Estos criterios se especifican en los *Common Criteria* tal como se publican en la norma internacional ISO/IEC 15408. Los contenidos principales son seguridad ante fallos, seguridad operacional y fiabilidad de la infraestructura técnica, así como disponibilidad, integridad y autenticidad de los documentos publicados. El Servicio de Documentación y Publicaciones debe ser seguro frente a **ataques, mala utilización, errores de operación y mal funcionamiento y fallo técnico**. Para garantizar esto deben tomarse medidas de tipo organizativo y técnico.

5 Seguridad de la información



6 Indexación de interfases

Para poder encontrar un documento electrónicos fuera del sistema local es clave que esté **indexado con metadatos descriptivos** y que estos metadatos estén **disponibles para el procesamiento por máquina**. En el núcleo de esto están los servicios de referencia y otros servicios adicionales que suministran terceras partes utilizando los datos y documentos suministrados por el Servicio de Documentación y Publicaciones. Opciones de búsqueda local y otros servicios adicionales son parte integral del Servicio de Documentación y Publicaciones.



7 Estadísticas de acceso

Las estadísticas de acceso basadas en los datos de servidor son la base **cualitativa, cuantitativa** o **tecnológica** para la evaluación del servicio. A nivel de “documento” la información de uso puede reflejar el impacto de un documento – sea como un impacto original de uso que puede tomarse como complementario respecto a otros conceptos de impacto (p. ej. una cita) o como un predictor de las citas. La información de uso relativa a un objeto puede ayudar en el futuro a detectar ciclos de uso de la información científica –incluso desglosada para diferentes disciplinas- enriquecer los análisis cientométricos.

8 Disponibilidad a largo plazo

Este certificado está enfocado a Servicios de Documentación y Publicaciones y no a archivos digitales a largo plazo tal como se tratan en el **Catálogo de Criterios para Archivos Digitales a Largo Plazo Fiables de Nestor** (Network of Expertise in long-term Storage and availability of digital Resources). Sin embargo, determinadas cuestiones relativas al archivo a largo plazo son también válidas para Servicios de Documentación y Publicaciones, en especial dado que los documentos publicados se transfieren a menudo a una institución de archivo a largo plazo, lo que precisa que se cumplen las condiciones previas apropiadas.

NESTOR: catálogo de criterios para Repositorios

- Home
- About us
  - Legal Bases
  - Collection Mandate
  - Special Collections
  - History
  - Organs
  - Overview of the Organisation
  - Strategy and Innovation
  - The Library as an Employer
- **Projects**
  - Cooperation

NESTOR - NETWORK OF EXPERTISE IN LONG-TERM STORAGE OF DIGITAL RESOURCES

Objective

The objective of the project was to create a competence network of long-term archival storage and long-term availability of digital resources in Germany. The co
create structures, which ensure that digital resources in Germany are archived on a long-term basis, are secured and are made available for use. Through natio
operation, a contribution was achieved towards safeguarding our global cultural heritage. Within the project, the following range of choices were developed, am

- a Web-based information forum with various content options for long-term archival storage and long-term availability of digital resources in Germany
- criteria for trusted digital repositories
- suggestions for procedures for a certification system for digital archives
- policies for long-term archival storage of digital resources
- a work-structure for the long-term availability of digital resources in the museum area
- co-ordination of division of duties and the assumption of long-term duties, especially in the delineation between the library, archive and museum areas

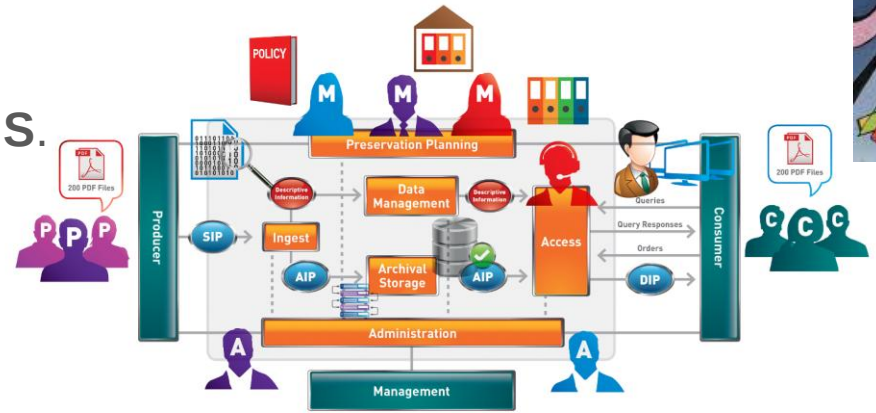
Project partners

German National Library was in charge of carrying out the project in co-operation with

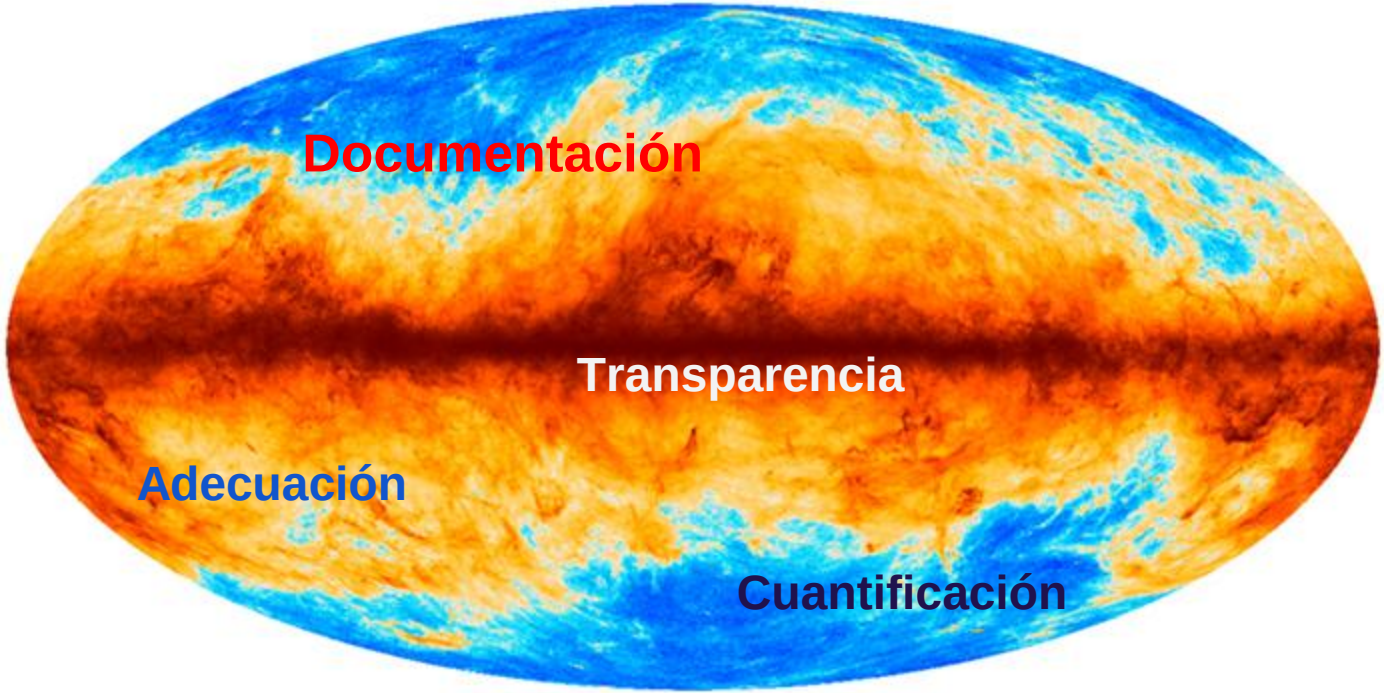
NESTOR: catálogo de criterios para Repositorios confiables

El objetivo del catálogo es formular un conjunto de criterios (organizacionales y técnicos) que puede usar un amplio espectro de repositorios digitales que desean mantener sus objetos digitales por largos períodos de tiempo. **Abstracción.**

Conformidad con OAIS.



NESTOR: principios básicos para aplicar los criterios

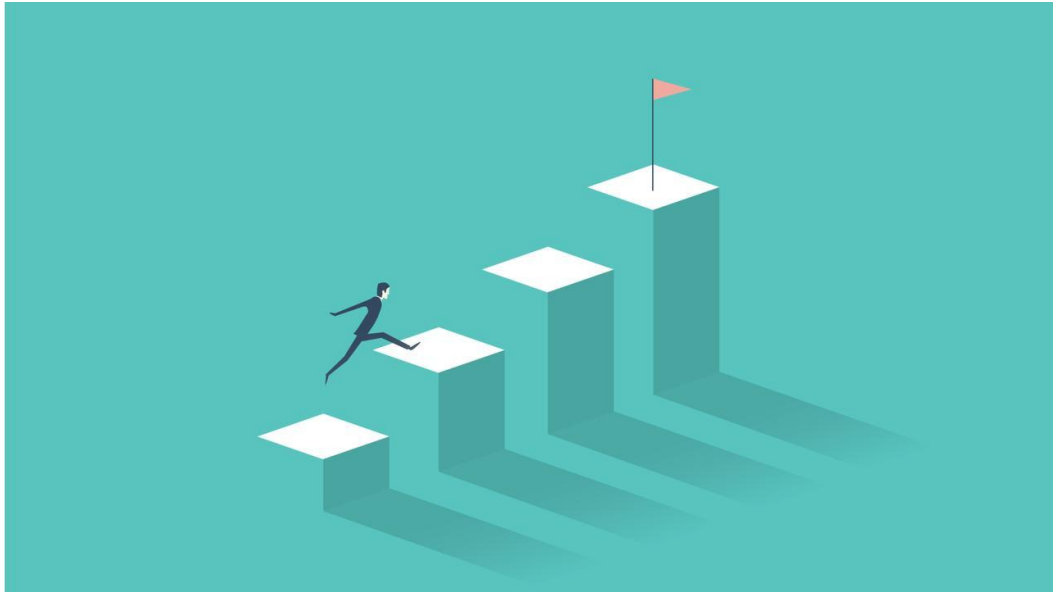


NESTOR: Catálogo de criterios

A. Marco de referencia organizacional

B. Gestión del objeto

C. Infraestructura y seguridad



http://www.dnb.de/Subsites/nestor/EN/Siegel/siegel.html
2018
http://www.langzeitarchivierung.de/Subsites/nestor/EN/Siegel/siegel_node.html

NESTOR

Catálogo de criterios

NESTOR: Catálogo de criterios

A. Marco de referencia organizacional

1 El RD ha definido sus objetivos.

1.1 Ha desarrollado criterios para la selección de sus objetos digitales.

1.2 El RD asume la responsabilidad por la preservación a largo plazo de la información representada en los objetos digitales.

1.3 El RD ha definido su/sus comunidad designada.

NESTOR: Catálogo de criterios

A. Marco de referencia organizacional

2 El repositorio garantiza a la comunidad designada el uso adecuado de la información representada en los objetos digitales.

2.1 El RD concede a su comunidad designada acceso a la información representada en los objetos digitales.

2.2 El RD asegura que la comunidad designada puede interpretar correctamente los objetos digitales.

NESTOR: Catálogo de criterios

A. Marco de referencia organizacional

3 Se respetan las reglas legales y contractuales.

3.1 Existen contratos legales entre productores y el RD.

3.2 En el devenir de sus tareas de archivado, el repositorio actúa sobre la base de reglas legales..

3.3 Con respecto al uso el RD actúa sobre la base de los requerimiento legales.

NESTOR: Catálogo de criterios

A. Marco de referencia organizacional

4 La forma organizacional es adecuada para el RD.

4.1 El financiamiento adecuado del RD está asegurado.

4.2 Tiene disponible el número adecuado de personal calificado.

4.3 Existen estructuras organizacionales adecuadas para el RD.

4.4 El RD aborda el planeamiento a largo plazo.

4.5 La continuidad de las tareas de preservación aún más allá de la existencia del RD.

NESTOR: Catálogo de criterios

A. Marco de referencia organizacional

5 La gestión de la calidad se conduce de manera adecuada.

5.1 Todos los procesos y las responsabilidades han sido definidos.

5.2 El repositorio digital documenta todos sus elementos con base en procesos definidos.

5.3 El repositorio digital reaccione ante cambios sustanciales.

NESTOR:
Catálogo de criterios

B. Gestión del objeto

NESTOR: Catálogo de criterios

B. Gestión del objeto

6 El RD asegura la integridad de los objetos digitales durante todas las etapas de procesamiento.

6.1 Ingesta: el RD asegura la integridad de los objetos digitales.

6.2 Archivo: el RD asegura la integridad de los objetos digitales.

6.3 Acceso: el RD asegura la integridad de los objetos digitales.

NESTOR: Catálogo de criterios

B. Gestión del objeto

7 El RD asegura la autenticidad del objeto digital y sus metadatos durante todas las etapas de procesamiento.

7.1 Ingesta: el repositorio digital asegura la autenticidad de los objetos digitales.

7.2 Archivo: el repositorio digital asegura la autenticidad de los objetos digitales.

7.3 Acceso: el repositorio digital asegura la autenticidad de los objetos digitales.

NESTOR: Catálogo de criterios

B. Gestión del objeto

8 El repositorio digital tiene un plan estratégico para todas las medidas que toma para la preservación digital

NESTOR: Catálogo de criterios

B. Gestión del objeto

9 El RD acepta objetos digitales desde los productores en base a criterios definidos.

9.1 El RD especifica los objetos de transferencia (Submission Information Packages, SIPs).

9.2 El RD identifica cuáles características de los objetos digitales son significativas para la información de la preservación..

9.3 El RD tiene control físico sobre los objetos digitales para poder llevar adelante la preservación a largo plazo.

NESTOR: Catálogo de criterios

B. Gestión del objeto

10 El almacenamiento de los archivos de los OD es emprendido de acuerdo a las especificaciones definidas.

10.1 El RD define sus objetos de archivo (Archival Information Packages, AIPs).

10.2 El RD toma a su cargo la transformación de los objetos de transferencia (SIPs) a objetos de archivo (AIPs).

10.3 El RD garantiza el almacenamiento y legibilidad de los AIPs.

10.4 El RD implementa estrategias para la preservación a largo plazo de cada AIP.

NESTOR: Catálogo de criterios

B. Gestión del objeto

11 El RD permite el uso de los objetos digitales de acuerdo a criterios definidos.

11.1 El RD define el uso de los objetos (Dissemination Information Packages, DIPs).

11.2 El RD la transformación del AIPs a DIPs.

NESTOR: Catálogo de criterios

B. Gestión del objeto

12 El sistema de gestión de datos es capaz de proveer las funciones necesarias para el RD.

12.1 El RD de manera unívoca y permanente identifica sus objetos y relaciones.

12.2 El RD adquiere/desarrolla metadatos adecuados para la descripción e identificación formal y basada en el contenido de los objetos digitales..

12.3 El RD desarrolla metadatos adecuados para la descripción estructural de los objetos digitales..

NESTOR: Catálogo de criterios

B. Gestión del objeto

12 El sistema de gestión de datos es capaz de proveer las funcior necesarias para el RD.

12.4 El RD desarrolla los metadatos adecuados para almacenar los cambios realizados por el RD a los objetos digitales.

12.5 El RD desarrolla los metadatos adecuados para la descripción técnica de los OD.

12.6 El RD desarrolla los metadatos adecuados para para almacenar los derechos de y condiciones de uso.

12.7 La asignación de metadatos a los OD se asegura todo el tiempo.

NESTOR: Catálogo de criterios

NESTOR: Catálogo de criterios

C. Infraestructura y seguridad

13 La infraestructura tecnológica es adecuada.

13.1 La infraestructura de IT implementa las demandas de gestión de objetos..

13.2 La infraestructura de IT implementa la seguridad que requiere el sistema.

NESTOR: Catálogo de criterios

C. Infraestructura y seguridad

14 La infraestructura protege al RD y a sus objetos digitales.

El checklist de los criterios está disponible en:

https://docs.google.com/spreadsheets/d/17w6QODPVDaQAUa9AIow5_GNvctSi_vnEsRvqw1elUNU/edit#gid=0

Aspectos a evaluar

Tu propuesta de aspectos

Construye tu norma

Construye tu Norma

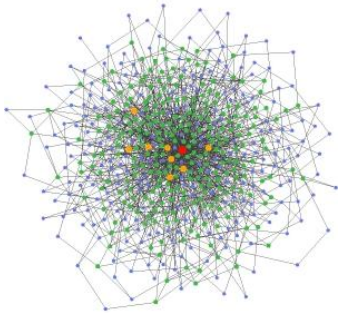
ISO 16363

El documento sigue los criterios TRAC para generarse como norma. Las secciones 1 y 2 son informativas y las secciones 3-5 proporcionan las métricas sobre:

- Infraestructura organizacional.
- Gestión de objetos digitales.
- Gestión de Riesgos de infraestructura y seguridad.

ISO 16363:2012 Audit and certification of trustworthy digital repositories

Las secciones 1 y 2 son informativas y las secciones 3-5 proporcionan las métricas sobre:



3. Infraestructura Organizativa
4. Gestión del objeto digital
5. Gestión de riesgos de Infraestructura y seguridad

Cada criterio es acompañado de una justificación, ejemplos y explicación

Norma UNE-ISO 16363:2017

ISO 16363 antecedentes

El propósito principal de esta norma es definir una Práctica Recomendada en la que basar un proceso de auditoría y certificación para evaluar la confianza de los repositorios digitales.

El desarrollo del Modelo de Referencia de Sistema Abierto de Información de Archivo (OAIS) consensuó lo que se requiere para que un repositorio digital provea conservación a largo plazo.

3 Infraestructura organizativa

3.1 Viabilidad de la organización y su gobierno

3.1.1 El repositorio debe tener una declaración de la misión que refleje un compromiso con la información digital para su conservación, retención a largo plazo, gestión y acceso. Esto es la declaración de la misión o el acta constitutiva del repositorio.

La declaración de la misión del repositorio debería tratar explícitamente la conservación. Si la conservación no se encuentra entre los fines primarios de una organización que aloja un repositorio digital, entonces la conservación podría no ser esencial para la misión de dicha organización. En algunos casos, un repositorio persigue su misión de conservación como un añadido de objetivos mayores de una organización en la que se aloja, tal como una universidad

3 Infraestructura organizativa

3.1 Viabilidad de la organización y su gobierno

3.1.1 El repositorio debe tener una declaración de la misión que refleje un compromiso con la información digital para su conservación, retención a largo plazo, gestión y acceso. Esto es la declaración de la misión o el acta constitutiva del repositorio.

La declaración de la misión del repositorio o de su organización matriz debería tratar explícitamente la conservación. Si la conservación no se encuentra entre los fines primarios de una organización que aloja un repositorio digital, entonces la conservación podría no ser esencial para la misión de dicha organización. En algunos casos, un repositorio persigue su misión de conservación como un añadido de objetivos mayores de una organización en la que se aloja, tal como una universidad

3 Infraestructura organizativa

3.1 Viabilidad de la organización y su gobierno

3.1.2 El repositorio debe tener un Plan Estratégico de Conservación que defina el enfoque que el repositorio mantendrá en el soporte a largo plazo de su misión.

El plan estratégico debería basarse en la misión establecida en la organización y en sus principios definidos, visión y metas. Los planes estratégicos típicamente engloban un período de tiempo finito y concreto, normalmente dentro de un rango de 3-5 años.

3.1.2.1 Plan de continuidad, plan de contingencia por si deja de funcionar.

3.1.2.2 El repositorio debe supervisar su entorno para determinar cuándo ejecutar su plan de sucesión, los planes de contingencia y/o acuerdos de garantía

3 Infraestructura organizativa

3.1 Viabilidad de la organización y su gobierno

3.1.3 El repositorio debe tener una Política de Colección/Fondo u otro documento que especifique el tipo de información que conservará.

La política de colección se puede usar para comprender lo que alberga el repositorio/ lo que no y por qué, sirve para apoyar la misión más amplia del repositorio, sin ella es probable que almacene de manera al azar o guarde grandes cantidades de contenido digital de bajo valor. Ayuda a la organización a identificar los contenidos digitales que aceptará para su ingreso y los que no. En una organización con una misión más amplia que la conservación del contenido digital, la política de colección ayuda a definir el papel del repositorio dentro de un contexto organizativo más amplio. Ver: https://digital.csic.es/dc/politicas/#politica1

3. Infraestructura organizativa

3.1 Viabilidad de la organización y su gobierno

3.1.1 El repositorio debe tener una declaración de la misión que refleje su compromiso con la información digital para su conservación, retención a largo plazo, gestión y acceso

3.1.2 El repositorio debe tener un Plan Estratégico de Conservación que defina el enfoque que el repositorio mantendrá en el soporte a largo plazo de su misión: 1) Plan de continuidad y 2) saber cuándo ejecutarlos.

3.1.3 El repositorio debe tener una Política de Colección que especifique el tipo de información que preservará.

3 Infraestructura organizativa

3.2 Estructura organizativa y provisión de personal

3.2.1 El repositorio debe tener identificadas y establecidas las responsabilidades necesarias a llevar a cabo y debe tener personal designado con adecuadas habilidades y experiencia para cumplir estas funciones.

3.2.1.1 El repositorio debe haber identificado sus funciones.

Plan de dotación de personal; definición de competencias; descripciones del trabajo; planes de desarrollo profesional; certificados de formación y acreditación; además de la evidencia de que el repositorio revisa estos documentos.

3.2.1.2 El repositorio debe tener el número apropiado de personal para apoyar todas las funciones y servicios.

Organigramas; definiciones de los roles y responsabilidades; comparación de los niveles de dotación de personal con los parámetros y estándares de la industria.

3.2.1.3 El repositorio debe contar con un activo programa de desarrollo profesional que proporcione oportunidades de desarrollo al personal con habilidades y conocimientos.

3. Infraestructura organizativa

3.2 Estructura organizativa y provisión de personal

3.2.1 El repositorio debe tener identificadas y establecidas las responsabilidades necesarias a llevar a cabo. 1) Debe haber identificado las funciones y el personal para cumplir esas funciones 2) en la cantidad adecuada y 3) formado!

3.2.1.1 Plan de dotación de personal; definición de competencias; descripciones del trabajo; planes de desarrollo profesional; certificados de formación y acreditación; además de la evidencia de que el repositorio revisa estos documentos.

3.2.1.2 Organigramas; definiciones de los roles y responsabilidades.

3.2.1.3 El repositorio debe contar con un activo programa de desarrollo profesional para su personal.

3 Infraestructura organizativa

3.3 Marco de procedimiento de responsabilidad y política de conservación

La documentación asegura a las partes interesadas (usuarios y productores) que el repositorio cumple con sus requisitos y es un repositorio de confianza. Un repositorio tiene que producir la documentación que refleja su Declaración de la Misión y el Plan Estratégico y captar sus actividades normales.

3 Infraestructura organizativa

3.3 Marco de procedimiento de responsabilidad y política de conservación

3.3.1 El repositorio debe tener definida su **Comunidad Específica** y debe tener estas definiciones accesibles.

3.3.2 El repositorio debe contar con **Políticas de Conservación** para asegurar que cumplirá con su Plan Estratégico de Conservación.

3.3.2.1 El repositorio debe tener **mecanismos para la revisión, actualización y desarrollo continuo de sus Políticas de Conservación** tal y como el repositorio crece y cómo evolucionan la tecnología y la práctica de la comunidad.

Especificaciones de los ciclos de revisión de la documentación.

3 Infraestructura organizativa

3.3 Marco de procedimiento de responsabilidad y política de conservación

3.3.3 El repositorio debe tener una **historia documentada** de los cambios en sus operaciones, procedimientos, software y hardware.

Los inventarios de bienes de capital; documentación de la adquisición, implementación, actualización y retirada del repositorio del software y hardware crítico; registros de los calendarios y políticas de retención y disposición, de las copias de las versiones anteriores de las políticas y procedimientos; las actas de las reuniones.

3 Infraestructura organizativa

3.3 Marco de procedimiento de responsabilidad y política de conservación

3.3.4 El repositorio debe **comprometerse con la transparencia y la rendición de responsabilidad** en todas las acciones de apoyo al funcionamiento y gestión del repositorio que afecte a la conservación del contenido digital a través del tiempo.

Los informes de las auditorías y certificaciones técnicas y financieras; divulgación de los documentos de gobierno, revisión independiente de programas, así como los contratos y acuerdos con los proveedores de fondos y servicios críticos.

3 Infraestructura organizativa

3.3 Marco de procedimiento de responsabilidad y política de conservación

3.3.5 El repositorio debe definir, recopilar, rastrear y proporcionar adecuadamente sus **mediciones de integridad de la información.**

Escrito sobre la definición o especificación de las medidas de integridad del repositorio (por ejemplo, la suma de controles calculada o el valor hash); documentación de los procedimientos y mecanismos para el seguimiento de las medidas de integridad y para responder a la monitorización de las mediciones de integridad que indican si el contenido digital está en riesgo; un proceso de auditoría para la recogida, el seguimiento y la presentación de las mediciones de integridad; Política de Conservación y documentación del flujo de trabajo.

3 Infraestructura organizativa

3.3 Marco de procedimiento de responsabilidad y política de conservación

3.3.6 El repositorio debe estar comprometido con un **programa regular de autoevaluación y certificación externa**

Listas de control de fechas de las autoevaluaciones y/o auditorías de terceros; certificados para el cumplimiento de las normas ISO pertinentes; presupuesto.

3. Infraestructura organizativa

3.3 Marco de procedimiento de responsabilidad y política de conservación

3.3.2.1 El repositorio debe tener mecanismos para la revisión, y desarrollo continuo de sus Políticas de Conservación tal y como el repositorio crece y cómo evolucionan la tecnología y las prácticas.

Debe tener una historia documentada de los cambios en sus operaciones, procedimientos, software y hardware.

Debe comprometerse con la transparencia y la rendición de responsabilidad en todas las acciones de apoyo al funcionamiento y gestión del repositorio que afecte a la conservación del contenido digital a través del tiempo.

Debe definir, recopilar, rastrear y proporcionar adecuadamente sus mediciones de integridad de la información. p.e. hash.

Debe estar comprometido con un programa regular de autoevaluación y/o certificación externa

3 Infraestructura organizativa

3.4 Sostenibilidad financiera

3.4.1 El repositorio debe contar en su sitio con procesos de **planificación de negocios a corto y largo plazo** para mantener el repositorio a lo largo del tiempo.

Actualizado, varios años de planes estratégicos, operativos y/o de actividad; estados financieros anuales auditados; previsiones financieras con múltiples opciones de presupuestos; planes de contingencia; análisis de mercado.

3.4.2 El repositorio debe tener **prácticas financieras y procedimientos que sean transparentes**, que cumplan con las normas y prácticas de contabilidad pertinentes, y auditadas por terceros de conformidad con los requisitos legales nacionales.

Requisitos de consulta demostrados en la planificación y prácticas de actividad; notificaciones y/o ejemplos de los requisitos de contabilidad y auditoría, normas y práctica; estados financieros anuales auditados.

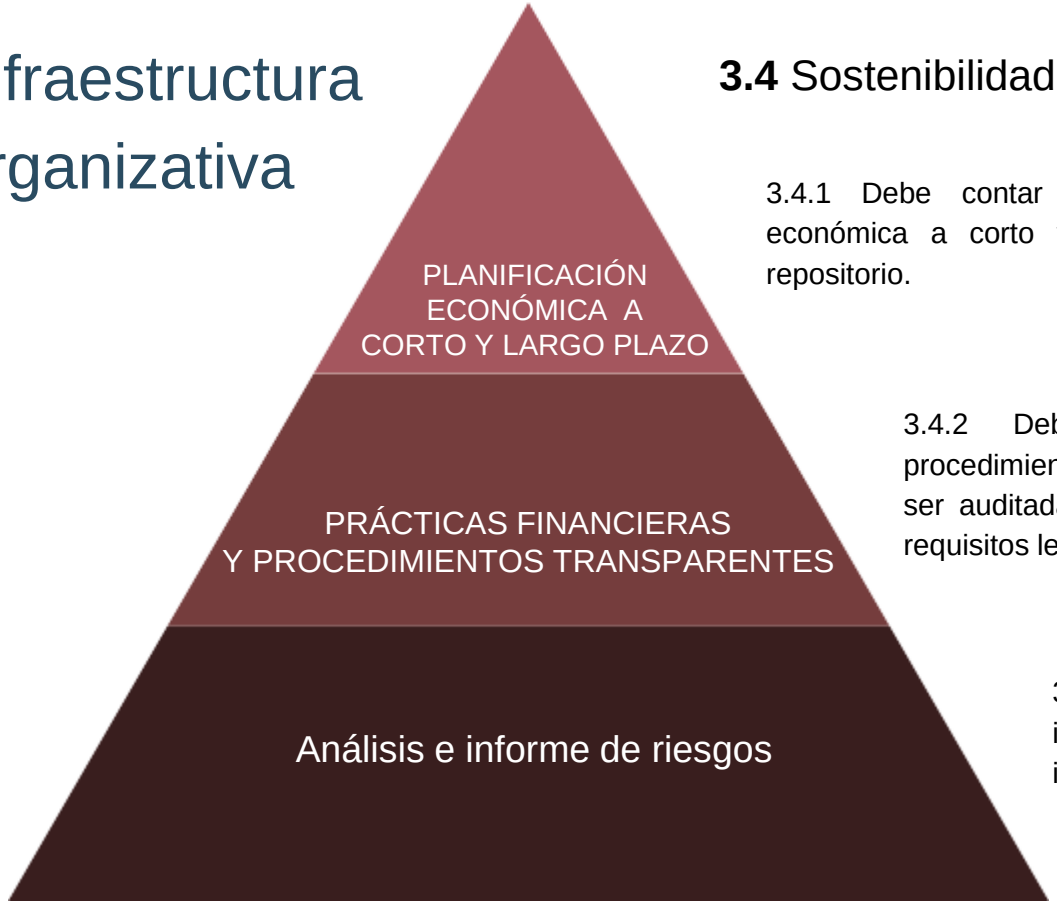
3 Infraestructura organizativa

3.4 Sostenibilidad financiera

3.4.3 El repositorio debe tener un **compromiso continuado en analizar e informar** sobre el riesgo financiero, el beneficio, la inversión y el gasto (incluyendo activos, licencias y pasivos)

Documentos de gestión de riesgos que identifican las amenazas percibidas y las potenciales y respuestas planificadas o puestas en ejecución (un registro del riesgo); documentos de planificación en inversión de infraestructura tecnológica; análisis de coste/beneficio; documentos de inversiones financieras y carteras; requisitos y ejemplos de licencias, contratos y administración de activos; evidencia de la revisión basada en riesgos.

3. Infraestructura organizativa



3.4 Sostenibilidad financiera

3.4.1 Debe contar con procesos de planificación económica a corto y largo plazo para mantener el repositorio.

3.4.2 Debe tener prácticas financieras y procedimientos que sean transparentes, que puedan ser auditadas por terceros de conformidad con los requisitos legales.

3.4.3 Debe tener un compromiso para analizar e informar sobre el riesgo financiero, el beneficio, la inversión y los gastos.

3 Infraestructura organizativa

3.5 Contratos, licencias, y pasivos

3.5.1 El repositorio debe **tener y mantener los contratos apropiados** o **contratos de depósito** para los materiales digitales que gestiona, conserva, y/o para los que proporciona acceso

Debidamente firmados y ejecutados los convenios de depósito y de los certificados de conformidad con las leyes y regulaciones locales, nacionales e internacionales; políticas en materia de acuerdos de depósito de terceros; las definiciones de los niveles de servicio y los usos permitidos; políticas de repositorio en el tratamiento de "obras huérfanas" y resolución de disputas de derechos de autor; informes de las evaluaciones de riesgo independientes de estas políticas; procedimientos para la revisión y el mantenimiento de convenios, contratos y licencias de forma regular.

3 Infraestructura organizativa

3.5 Contratos, licencias, y pasivos

3.5.1.1 El repositorio debe tener contratos o acuerdos de depósito que especifiquen y transfieran todos los derechos de conservación necesarios, y deben documentarse los derechos transferidos

Convenios de depósito; especificación(ones) de derechos cedidos por diferentes tipos de contenido digital (si es aplicable); declaraciones de política sobre el requisito de derechos de conservación.

Como el derecho de modificar la información digital está a menudo restringido por derecho de autor, es importante que los convenios incluyan permiso de modificar los objetos digitales para mantenerlos accesibles.

3 Infraestructura organizativa

3.5 Contratos, licencias, y pasivos

3.5.1.2 El repositorio debe haber especificado todos los aspectos pertinentes de la **adquisición, mantenimiento, acceso y retirada de acuerdos escritos** con los depositantes y otras partes pertinentes

Esto es necesario con el fin de garantizar que son entendidos y aceptados por todas las partes las funciones respectivas del repositorio, los productores de contenido digital y la transferencia de la responsabilidad de la conservación.

Correcta ejecución de acuerdos de transferencia, convenios de depósito, y escrituras de donación; escritos de procedimientos operativos estándar.

3 Infraestructura organizativa

3.5 Contratos, licencias, y pasivos

3.5.1.3 El repositorio debe tener **políticas escritas** que indiquen cuando acepta la responsabilidad de la conservación del contenido de cada conjunto de objetos de datos transferidos

Correcta ejecución de acuerdos de transferencia, convenios de depósito, y escrituras de donación; confirmación de recepción enviada al productor/depositante.

3.5.1.4 El repositorio debe contar con políticas establecidas para abordar la responsabilidad y desafíos en la propiedad/derechos.

Una definición de los derechos, licencias y permisos de los productores y contribuyentes de contenido; menciones a las leyes y reglamentos pertinentes.

3. Infraestructura organizativa

3.5 Contratos, licencia y pasivos

3.5.1 El repositorio debe tener y mantener los contratos apropiados o contratos de depósito para los materiales digitales que gestiona, conserva, y/o para los que proporciona acceso.

3.5.1.1 El repositorio debe tener contratos o acuerdos de depósito que especifiquen y transfieran todos los derechos de conservación necesarios, y deben documentarse los derechos transferidos.

3.5.1.2 Debe haber especificado todos los aspectos pertinentes de la adquisición, mantenimiento, acceso y retirada de acuerdos.

3.5.1.3 Debe tener políticas escritas que indiquen cuando acepta la responsabilidad de la conservación del contenido de cada conjunto de objetos.

3.5.1.4 Debe contar con políticas establecidas para abordar la responsabilidad y desafíos en la propiedad/derechos

3 Infraestructura organizativa

3.5 Contratos, licencias, y pasivos

3.5.2 El repositorio debe **rastrear y administrar los derechos de propiedad intelectual** y las restricciones en el uso de los contenidos del repositorio como exige el acuerdo, contrato o licencia de depósito.

Una declaración de la Política de Conservación que defina y especifique los requisitos del repositorio y los procedimientos para la gestión de los derechos de propiedad intelectual; convenios de los depositantes; plantillas de los convenios y otros documentos que especifiquen y se ocupen de los derechos de propiedad intelectual; documentación de monitorización del repositorio en el tiempo, cambios en estado y propiedad intelectual de los contenidos digitales mantenidos por el repositorio; los metadatos en que se captura la información de los derechos.

3. Infraestructura organizativa

3.5 Contratos, licencia y pasivos

3.5.2 El repositorio debe rastrear y administrar los derechos de propiedad intelectual y las restricciones en el uso de los contenidos del repositorio como exige el acuerdo, contrato o licencia de depósito.

4 Gestión del objeto digital

4.1 Ingreso: adquisición de contenido

4.1.1 El repositorio debería identificar la **Información de Contenido** y las **Propiedades de la Información** que va a preservar.

Declaración de misión, convenios de transferencia; convenios de depósito o escrituras de donaciones; documentos de flujos de procesos de trabajo y sobre Políticas de Conservación, incluyendo definiciones escritas sobre las propiedades acordadas en el convenio de depósito o escritura de donación; procedimientos escritos de procesos y documentación sobre las propiedades para ser conservadas.

4 Gestión del objeto digital

4.1 Ingreso: adquisición de contenido

4.1.1 El repositorio debería identificar la Información de Contenido y las Propiedades de la Información que va a preservar.

4.1.1.1 El repositorio debe tener un(os) **procedimiento**(s) para identificar las Propiedades de la Información que conservará.

Definiciones de las Propiedades de Información que deberían ser conservadas; convenios de transferencia/convenios de depósitos; políticas de conservación; procedimientos escritos de procesos, flujos de trabajo de procesos. Tipologías documentales y propiedades de cada una a conservar y de qué modo.

4 Gestión del objeto digital

4.1 Ingreso: adquisición de contenido

4.1.1 El repositorio debería identificar la Información de Contenido y las Propiedades de la Información que va a preservar.

4.1.1.2 El repositorio debe tener un **documento** de la Información de Contenido y de las Propiedades de la Información que conservará

Políticas de Conservación, manuales de procesos; inventarios de colecciones/fondos o cuestionarios, logs de los tipos de Información de Contenido; estrategias adquiridas de conservación y planes de acción.

4. Gestión del objeto digital

4.1 Ingreso: adquisición de contenido

4.1.2 El repositorio debe especificar claramente la información que necesita ser asociada con la Información de Contenido específica en el momento de su depósito

4.1.3 El repositorio debe tener especificaciones adecuadas que permitan el reconocimiento y análisis de los SIPs

4.1.4 El repositorio debe tener mecanismos para verificar apropiadamente la identidad del Productor de todos los materiales

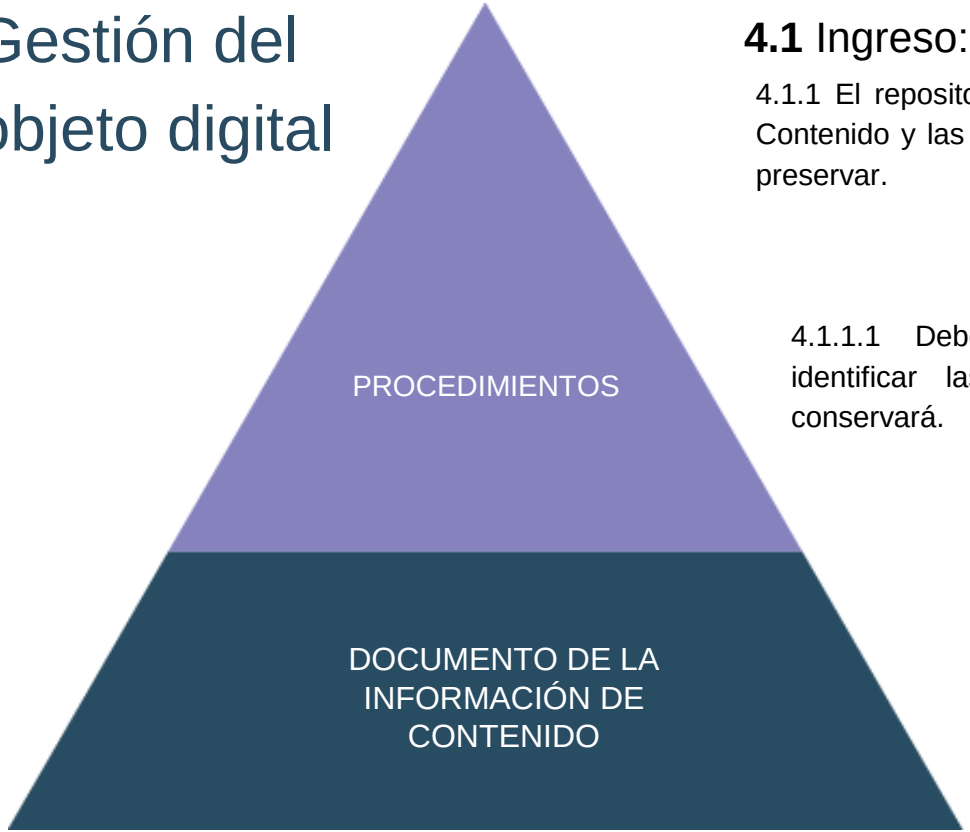
4.1.5 El repositorio debe tener un proceso de ingreso que verifique cada SIP por completitud y exactitud

4.1.6 El repositorio debe obtener control suficiente sobre los Objetos Digitales para conservarlos

4.1.7 El repositorio debe proveer al productor/depositante con las acciones adecuadas en puntos acordados durante el proceso de ingreso

4.1.8 El repositorio debe tener documentos vigentes de las acciones de los procesos de administración relevantes para la adquisición de contenido

4. Gestión del objeto digital



4.1 Ingreso: adquisición de contenido

4.1.1 El repositorio debería identificar la Información de Contenido y las Propiedades de la Información que va a preservar.

4.1.1.1 Debe tener un(os) procedimiento(s) para identificar las Propiedades de la Información que conservará.

4.1.1.2 Debe tener un documento de la Información de Contenido y de las Propiedades de la Información que conservará

4 Gestión del objeto digital

4.1 Ingreso: adquisición de contenido

4.1.2 El repositorio debe especificar claramente la información que necesita ser asociada con la Información de Contenido específica en el momento de su depósito

Ejemplos: Requisitos de transferencia; convenios del productor-archivo; planes de flujos de trabajo para producir el AIP.

4 Gestión del objeto digital

4.1 Ingreso: adquisición de contenido

4.1.3 El repositorio debe tener especificaciones adecuadas que permitan el reconocimiento y análisis de los SIP

Ejemplos: Información de Empaquetamiento para los SIPs; Información de Representación para los datos de contenido del SIP, incluyendo especificaciones documentadas sobre los formatos de archivo; estándares de datos publicados; documentación de construcción de objetos válidos.

4 Gestión del objeto digital

4.1 Ingreso: adquisición de contenido

4.1.4 El repositorio debe tener mecanismos para verificar apropiadamente la identidad del Productor de todos los materiales

Convenios de transferencia normativamente vinculante/convenios de depósito/escrituras de donación, evidencia de medidas tecnológicas adecuadas; ficheros de actividades de procedimientos y autentificaciones.

4 Gestión del objeto digital

4.1 Ingreso: adquisición de contenido

4.1.5 El repositorio debe tener un proceso de ingreso que verifique cada SIP (SIP) por completitud y exactitud

Política Adecuada de Conservación, documentos del Plan de Implementación de la Conservación y ficheros log derivados de procedimientos de ingreso del sistema(s); logs o registros de ficheros recibidos durante la transferencia y proceso de ingreso; documentación de procedimientos operativos estandarizados; procedimientos detallados y otros diagramas de flujos de trabajo, registros de formatos; definiciones de completitud y exactitud.

4 Gestión del objeto digital

4.1 Ingreso: adquisición de contenido

4.1.6 El repositorio debe obtener control suficiente sobre los Objetos Digitales para conservarlos

Documentos que demuestren el nivel de control físico que el repositorio tiene. Una base de datos/catálogo de metadatos enumerando todos los objetos digitales en el repositorio y los metadatos suficientes para validar la integridad de esos objetos (tamaño de fichero, verificaciones, función hash, ubicación, número de copias, etc.).

4 Gestión del objeto digital

4.1 Ingreso: adquisición de contenido

4.1.7 El repositorio debe proveer al productor/depositante con las acciones adecuadas en puntos acordados durante el proceso de ingreso

Convenios de transferencia/convenios de depósito/escrituras de donación; documentación de flujos de trabajo; procedimientos operativos estándares; evidencia de “informar” tales como informes, correspondencia, notas o correos electrónicos.

4 Gestión del objeto digital

4.1 Ingreso: adquisición de contenido

4.1.8 El repositorio debe tener documentos vigentes de las acciones de los procesos de administración relevantes para la adquisición de contenido

Documentación escrita de decisiones y/o acciones realizadas; metadatos de conservación, guardados y enlazados con los objetos digitales relevantes, recibos de confirmación devueltos a los proveedores.

4 Gestión del objeto digital

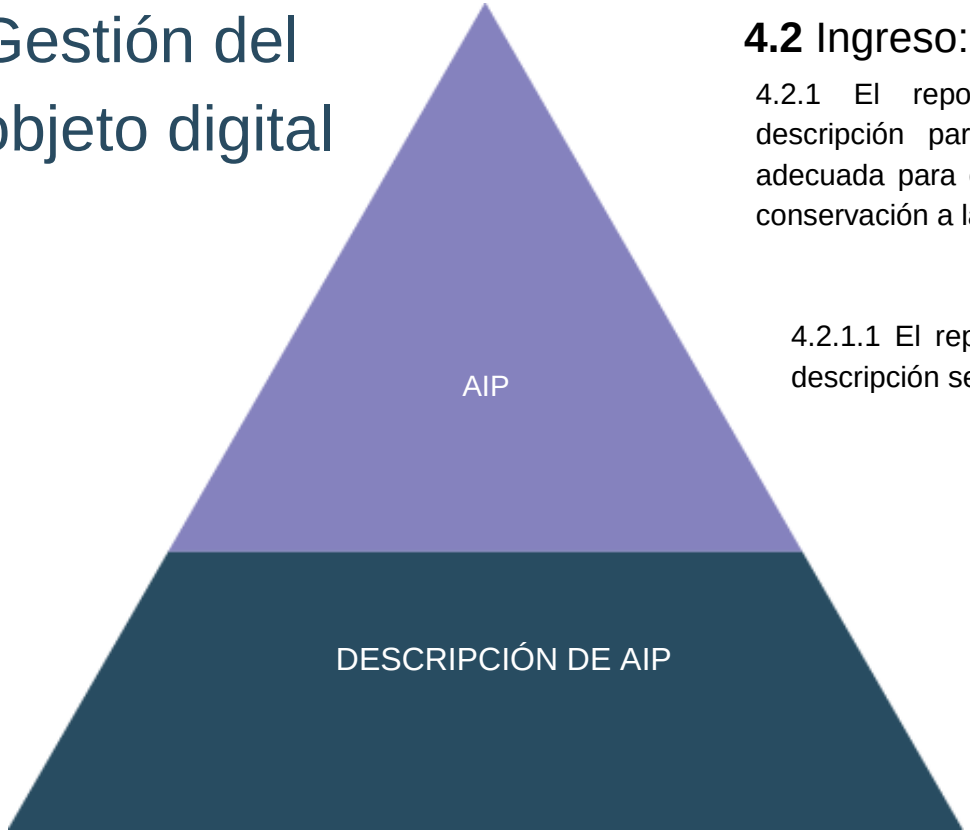
4.2 Ingreso: creación del AIP

4.2.1 El repositorio debe tener conservada una descripción para cada AIP o cada clase de AIPs, adecuada para el análisis del AIP y las necesidades de conservación a largo plazo

4.2.1.1 El repositorio debe ser capaz de identificar qué descripción se aplica a qué AIP Justificación

4.2.1.2 El repositorio debe tener una descripción para cada AIP que sea adecuada para la conservación a largo plazo, permitiendo la identificación y análisis de todos los componentes requeridos dentro del AIP

4.
Gestión del objeto digital



4.2 Ingreso: creación del AIP

4.2.1 El repositorio debe tener conservada una descripción para cada AIP o cada clase de AIPs, adecuada para el análisis del AIP y las necesidades de conservación a largo plazo

4.2.1.1 El repositorio debe ser capaz de identificar qué descripción se aplica a qué AIP Justificación

4.2.1.2 El repositorio debe tener una descripción para cada AIP que sea adecuada para la conservación a largo plazo, permitiendo la identificación y análisis de todos los componentes requeridos dentro del AIP

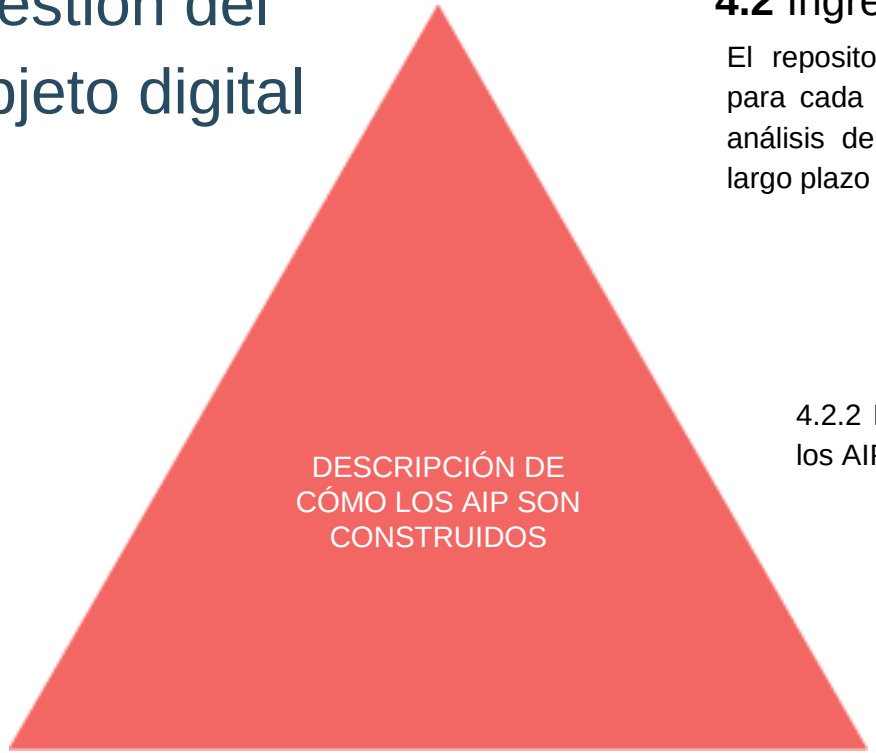
4 Gestión del objeto digital

4.2 Ingreso: creación del AIP

4.2.2 El repositorio debe tener una descripción de cómo los AIPs son construidos desde los SIP

Documentos de descripción de procesos; documentación de la relación entre el SIP y el AIP; documentación evidente de cómo los AIP se derivan de los SIP.

4.
Gestión del objeto digital



4.2 Ingreso: creación del AIP

El repositorio debe tener conservada una descripción para cada AIP o cada clase de AIP, adecuada para el análisis del AIP y las necesidades de conservación a largo plazo

4.2.2 El repositorio debe tener una descripción de cómo los AIPs son construidos desde los SIP

4 Gestión del objeto digital

4.2 Ingreso: creación del AIP

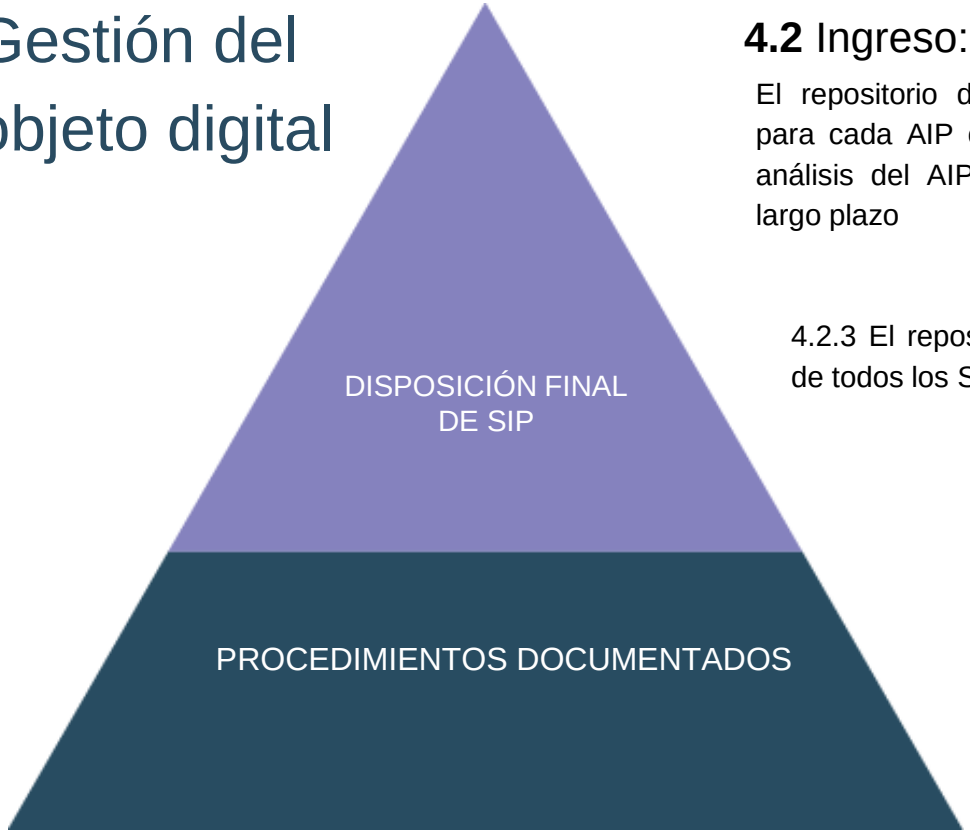
4.2.3 El repositorio debe documentar la disposición final de todos los SIP

En particular, tiene que comprobarse el aspecto siguiente:

4.2.3.1 El repositorio debe seguir procedimientos documentados cuando un SIP no se incorpore a un AIP o se descarte, indicándose las razones

Ficheros de procesos del sistema; calendarios de conservación; convenios del depositante o donante/escrituras de donación; sistema de registro de seguimiento de la procedencia; sistema de ficheros de log; documentos de descripción de proceso; documentación de vinculación del SIP con el AIP; documentación evidente de cómo los AIP derivan de los SIP; documentación del estándar/proceso sobre el cual sucede la normalización; documentación del resultado de normalización y de cómo el AIP resultante difiere del(de los) SIP.

4.
Gestión del objeto digital



4.2 Ingreso: creación del AIP

El repositorio debe tener conservada una descripción para cada AIP o cada clase de AIP, adecuada para el análisis del AIP y las necesidades de conservación a largo plazo

4.2.3 El repositorio debe documentar la disposición final de todos los SIP

4.2.3.1 El repositorio debe seguir procedimientos documentados cuando un SIP no se incorpore a un AIP o se descarte, indicándose las razones

4 Gestión del objeto digital

4.2 Ingreso: creación del AIP

4.2.4 El repositorio debe tener y usar una convención para generar identificadores unívocos y continuos para todos los AIP. Tienen que comprobarse los siguientes aspectos:

4.2.4.1 El repositorio debe identificar unívocamente cada AIP en el propio repositorio

4.2.4.1.1 El repositorio debe de disponer de identificadores unívocos

4.2.4.1.2 El repositorio debe asignar y mantener identificadores continuos

4.2.4.1.3 La documentación debe describir cualquier proceso empleado para cambiar cada uno de los identificadores

4 Gestión del objeto digital

4.2 Ingreso: creación del AIP

4.2.4 El repositorio debe tener y usar una convención para generar identificadores unívocos y continuos para todos los AIP. Tienen que comprobarse los siguientes aspectos:

4.2.4.1.4 El repositorio debe ser capaz de proporcionar una lista completa de todos esos identificadores y hacer controles aleatorios por las duplicaciones

4.2.4.1.5 El sistema de identificadores debe ser adecuado para validar los actuales y futuros requisitos del repositorio, tal como el número de objetos

4 Gestión del objeto digital

4.2 Ingreso: creación del AIP

4.2.4 El repositorio debe tener y usar una convención para generar identificadores unívocos y continuos para todos los AIP. Tienen que comprobarse los siguientes aspectos:

4.2.4.2 El repositorio debe tener un sistema de seguridad de conexión/servicio de resolución para encontrar unívocamente el objeto identificado sin importar su ubicación física

Documentación describiendo los nombres convenidos y la evidencia física de sus aplicaciones. (Ejemplo, los logs). Documentación describiendo los nombres convenidos y las evidencias físicas de su aplicación. (Ejemplo, los logs).

4 Gestión del objeto digital

4.2 Ingreso: creación del AIP

4.2.5 El repositorio debe tener acceso a las herramientas y recursos necesarios para proveer la Información de Representación fidedigna para todos los objetos digitales que contengan. Tienen que comprobarse los siguientes aspectos:

4.2.5.1 El repositorio debe tener herramientas y métodos para identificar los tipos de ficheros de todos los Objetos de Datos transferidos

4.2.5.2 El repositorio debe tener herramientas y métodos para determinar qué Información de Representación es necesaria para hacer cada Objeto de Datos comprensible a cada Comunidad Específica

4 Gestión del objeto digital

4.2 Ingreso: creación del AIP

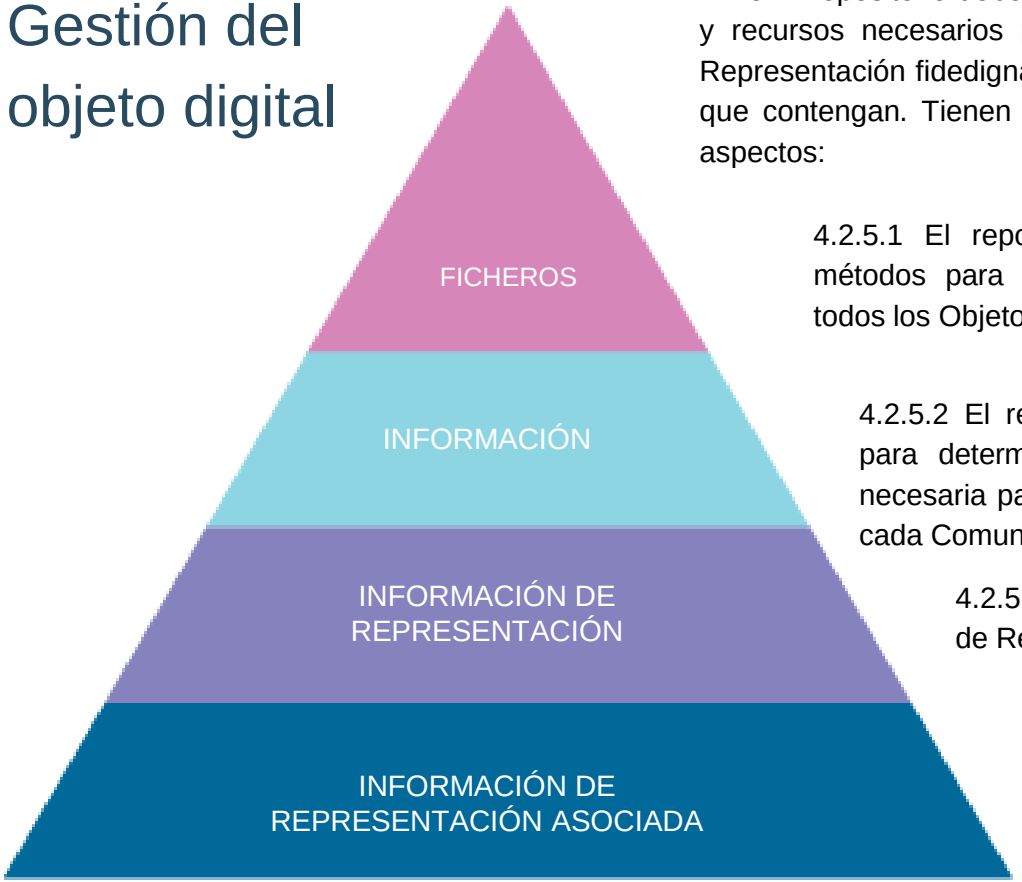
4.2.5 El repositorio debe tener acceso a las herramientas y recursos necesarios para proveer la Información de Representación fidedigna para todos los objetos digitales que contengan. Tienen que comprobarse los siguientes aspectos:

4.2.5.3 El repositorio debe tener acceso a la Información de Representación

4.2.5.4 El repositorio debe tener herramientas y métodos para asegurar que la Información de Representación requerida sea asociada de modo continuo con los Objetos de Datos correspondientes

Suscripción o acceso a registros de Información de Representación (incluyendo registros de formato); documentos visibles en registros locales (con enlace continuo a los objetos digitales); documentos de bases de datos que incluyen Información de Representación y un enlace continuo a los objetos digitales correspondientes.

4. Gestión del objeto digital



4.2 Ingreso: creación del AIP

4.2.5 El repositorio debe tener acceso a las herramientas y recursos necesarios para proveer la Información de Representación fidedigna para todos los objetos digitales que contengan. Tienen que comprobarse los siguientes aspectos:

4.2.5.1 El repositorio debe tener herramientas y métodos para identificar los tipos de ficheros de todos los Objetos de Datos transferidos

4.2.5.2 El repositorio debe tener herramientas y métodos para determinar qué Información de Representación es necesaria para hacer cada Objeto de Datos comprensible a cada Comunidad Específica

4.2.5.3 El repositorio debe tener acceso a la Información de Representación

4.2.5.4 El repositorio debe tener herramientas y métodos para asegurar que la Información de Representación requerida sea asociada de modo continuo con los Objetos de Datos correspondientes

4 Gestión del objeto digital

4.2 Ingreso: creación del AIP

4.2.6 El repositorio debe disponer de procesos documentados para adquirir la Información de Descripción de Conservación (PDI) para su Información de Contenido asociada y para adquirir la PDI de acuerdo con los procesos documentados. En particular, tiene que comprobar los siguientes aspectos:

4.2.6.1 El repositorio debe documentar los procesos para adquirir la PDI

4.2.6.2 El repositorio debe ejecutar sus procesos documentados para adquirir la PDI

4.2.6.3 El repositorio debe asegurar que la PDI sea continuamente asociada con la Información de Contenido correspondiente

Procedimientos operativos normalizados; manuales que describan los procedimientos de “ingreso”; documentación visible sobre la forma en que el repositorio adquiere y gestiona la Información de Descripción de Conservación (PDI); crear “sumas de verificación” o compendios, consultar a la Comunidad Específica acerca del Contexto.

4. Gestión del objeto digital

4.2 Ingreso: creación del AIP

El repositorio debe disponer de procesos documentados para adquirir la Información de Descripción de Conservación (PDI) para su Información de Contenido asociada y para adquirir la PDI de acuerdo con los procesos documentados. En particular, tiene que comprobar los siguientes aspectos:

4.2.6.1 El repositorio debe documentar los procesos para adquirir la PDI

4.2.6.2 El repositorio debe ejecutar sus procesos documentados para adquirir la PDI

4.2.6.3 El repositorio debe asegurar que la PDI sea continuamente asociada con la Información de Contenido correspondiente

4 Gestión del objeto digital

4.2 Ingreso: creación del AIP

4.2.7 El repositorio debe asegurar que la Información de Contenido del AIP es comprensible por su Comunidad Específica en cualquier momento de la creación del AIP

En particular hay que verificar los siguientes aspectos.

4.2.7.1 El repositorio debe tener un proceso documentado para verificar la inteligibilidad de la Información de Contenido de los AIP en su creación para su Comunidad Específica

4.2.7.2 El repositorio debe ejecutar el proceso de verificación para cada clase de Información de Contenido

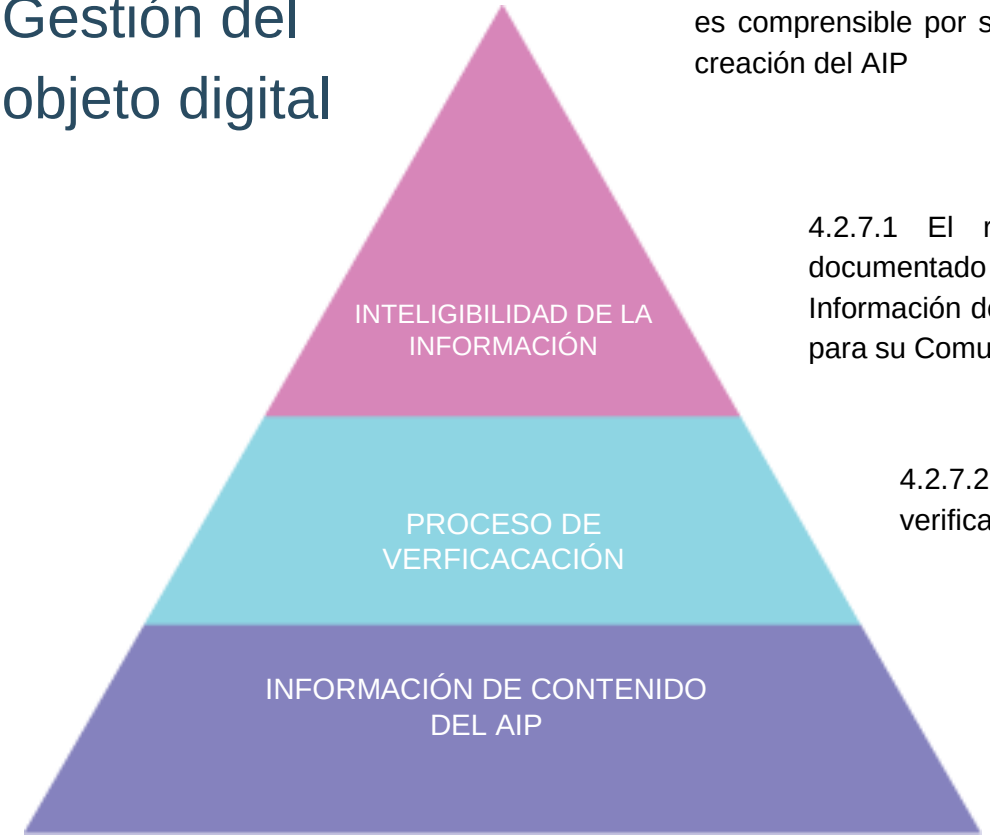
4.2.7.3 El repositorio debe llevar la Información de Contenido del AIP hasta el nivel requerido de inteligibilidad si la verificación de inteligibilidad falla

Procedimientos de verificación que operen contra los fondos digitales para asegurar su inteligibilidad a la Comunidad Específica definida; registro de que estos test han sido llevados a cabo y evaluados; evidencia de la recopilación o identificación de la Información de Representación, para llenar los vacíos que hayan podido encontrarse en la inteligibilidad; fidelización de individuos con experiencia en la materia.

4. Gestión del objeto digital

4.2 Ingreso: creación del AIP

4.2.7 El repositorio debe asegurar que la Información de Contenido del AIP es comprensible por su Comunidad Específica en cualquier momento de la creación del AIP



4.2.7.1 El repositorio debe tener un proceso documentado para verificar la inteligibilidad de la Información de Contenido de los AIPs en su creación para su Comunidad Específica

4.2.7.2 El repositorio debe ejecutar el proceso de verificación para cada clase de Información de Contenido

4.2.7.3 El repositorio debe llevar la Información de Contenido del AIP hasta el nivel requerido de inteligibilidad si la verificación de inteligibilidad falla

4 Gestión del objeto digital

4.2 Ingreso: creación del AIP

4.2.8 El repositorio debe verificar que cada AIP está completo y es correcto desde el momento en que se crea

Descripción del procedimiento que verifica que los AIPs están completos y son correctos; logs del procedimiento.

4.2.9 El repositorio debe proporcionar un funcionamiento independiente para verificar la integridad de la colección/fondo/contenido del repositorio

Documentación proporcionada por 4.2.1 a través de 4.2.4; convenios documentados y negociados entre el productor y el repositorio (véase 4.1.1-4.1.8); logs de las fechas de recepción del material y su acción asociada (acuse de recibo, acción, etc.); logs de las verificaciones periódicas.

4 Gestión del objeto digital

4.2 Ingreso: creación del AIP

4.2.10 El repositorio debe tener documentos actualizados de las acciones y procesos de administración que son relevantes para la creación del AIP

Documentación escrita de las decisiones y/o acciones tomadas con sellos de tiempo; metadatos de conservación registrados, almacenados y vinculados a los objetos digitales pertinentes.

4 Gestión del objeto digital

4.3 Planificación de la conservación

4.3.1 El repositorio debe tener estrategias de conservación documentadas relevantes para sus fondos

Documentación que identifique cada riesgo de conservación y la estrategia.

4.3.2 El repositorio debe monitorear su entorno de conservación

Encuestas a la Comunidad Específica del repositorio.

4.3.2.1 El repositorio debe tener dispositivos para monitorear y notificar cuándo la Información de Representación es inadecuada para que la Comunidad Específica comprenda los fondos de datos.

Suscripción a un servicio de registro de Información de Representación; suscripción a un servicio de vigilancia de tecnología; encuestas entre los miembros de su Comunidad Específica; procesos de trabajo pertinentes para tratar esta información.

4 Gestión del objeto digital

4.3 Planificación de la conservación

4.3.3 El repositorio debe tener mecanismos para cambiar sus planes de conservación como resultado de sus actividades de monitorización

Planes de Conservación vinculados a vigilancia(s) tecnológica(s) formal(es) o informal(es); planifica- ción o procesos de conservación que se establecen para intervalos más cortos (por ejemplo, no más de cinco años); prueba de actualizaciones frecuentes de las Políticas de Conservación y los Planes de Conservación; secciones de las Políticas de Conservación que aborden cómo actualizar los planes y que aborden la frecuencia con que se requiere que los planes se revisen, reafirmen o actualicen.

4.3.3.1 El repositorio debe tener mecanismos para crear, identificar o reunir cualquier Información de Representación extra que se le requiera

Suscripción a un servicio de registro de formatos; suscripción a un servicio de observación de tecnología; planes de conservación.

4 Gestión del objeto digital

4.3 Planificación de la conservación

4.3.4 El repositorio debe proporcionar evidencia de la efectividad de sus actividades de conservación

Colección de metadatos de conservación apropiados; prueba de la usabilidad de objetos digitales custodiados dentro del sistema seleccionados aleatoriamente; historial demostrable para los objetos digitales conservados usables a lo largo del tiempo; sondeos a la Comunidad Específica.

4 Gestión del objeto digital

4.4 Conservación del AIP

4.4.1 El repositorio debe tener especificaciones sobre cómo se almacenan los AIPs hasta el nivel de bit

Documentación del formato de los AIPs; descripciones EAST y Data Entity Dictionary Specification Language (DEDSL) de los componentes datos (véase referencias [B6] y [B7].

4.4.1.1 El repositorio debe conservar la Información de Contenido de los AIPs

Documentación del procedimiento del flujo de trabajo de conservación; documentación del procedimiento del flujo de trabajo; documentos de la Política de Conservación que especifiquen el tratamiento de los AIPs y bajo qué circunstancias se pueden borrar; habilidad para demostrar la secuencia de conversiones para un AIP para cualquier objeto digital particular o grupo de objetos ingresados; documentación que vincule los objetos ingresados y las AIPs actuales.

4 Gestión del objeto digital

4.4 Conservación del AIP

4.4.1 El repositorio debe tener especificaciones sobre cómo se almacenan los AIPs hasta el nivel de bit

Documentación del formato de los AIPs; descripciones EAST y Data Entity Dictionary Specification Language (DEDSL) de los componentes datos (véase referencias [B6] y [B7].

4.4.1.2 El repositorio debe monitorizar activamente la integridad de los AIPs

información de su fijeza (por ejemplo, verificaciones) para cada objeto digital/AIP ingresado en el sistema; logs de las verificaciones de la fijeza; documentación sobre cómo los AIPs y la información de Fijeza se conservan separadamente; documentación sobre cómo los AIPs y los registros de acceso se conservan separadamente.

4 Gestión del objeto digital

4.4 Conservación del AIP

4.4.2 El repositorio debe tener registros contemporáneos a las acciones y procesos de administración relevantes para el almacenamiento y la conservación de los AIPs

Documentación escrita de las decisiones y/o acción llevada cabo; metadatos de conservación registrados, almacenados y vinculados a los objetos digitales pertinentes.

4.4.2.1 El repositorio debe tener procedimientos para todas las acciones llevadas a cabo en los AIPs

Documentación escrita que describa todas las acciones que se pueden llevar a cabo contra un AIP.

4.4.2.2 El repositorio debe ser capaz de demostrar que cualquier acción llevada a cabo en los AIPs cumple con los requisitos de la especificación de esas acciones

Metadatos de conservación registrados, almacenados y vinculados a sus correspondientes objetos digitales y documentación de esa acción; auditorías de procedimientos del repositorio que muestren que todas las acciones concuerdan con los procesos documentados.

4 Gestión del objeto digital

4.5 Gestión de la información

4.5.1 El repositorio debe especificar los requisitos de información mínimos para permitir a la Comunidad Específica descubrir e identificar el material de interés

Información descriptiva y de recuperación, metadatos de descubrimiento, como Dublin Core y otra documentación que describa el objeto.

4.5.2 El repositorio debe capturar o crear la información descriptiva mínima y asegurarse de que está asociada al AIP

Metadatos descriptivos; identificador o localizador unívoco, interno o externo continuo que esté asociado con el AIP (véase también 4.2.4 acerca del identificador unívoco continuo); documentación del sistema y arquitectura técnica; convenios del depositante; documentación de la política de metadatos que incorpore detalles de los requisitos de metadatos y una declaración que describa dónde cae la responsabilidad de su adquisición; documentación del proceso del flujo de trabajo.

4 Gestión del objeto digital

4.5 Gestión de la información

4.5.3 El repositorio debe mantener una vinculación bidireccional entre cada AIP y su información descriptiva

Metadatos descriptivos; identificador o localizador unívoco, continuo, asociado con el AIP; relación documentada entre el AIP y sus metadatos; documentación del sistema y arquitectura técnica; documentación del proceso del flujo de trabajo.

4.5.3.1 El repositorio debe mantener las asociaciones entre sus AIPs y su información descriptiva a lo largo del tiempo

Log que detalle el mantenimiento en curso o verificación de la integridad de los datos y sus relaciones con la información descriptiva asociada, especialmente en el seguimiento de la reparación o modificación de un AIP; herencia de información descriptiva; mantenimiento del identificador o localizador; relación documentada entre el AIP y su información descriptiva; documentación del sistema y arquitectura técnica; documentación del proceso del flujo de trabajo.

4 Gestión del objeto digital

4.6 Gestión de acceso

El término “acceso” tiene varios significados, incluyendo el acceso de los usuarios al repositorio, por ejemplo, la seguridad física y la autenticación de usuarios, y los distintos pasos en el acceso a los documentos (hacer una solicitud, comprobar los derechos del solicitante, y preparar y enviar un Paquete de Información de Consulta [DIP]). Este apartado trata todos estos puntos. Se divide en dos requisitos principales, uno relativo a la existencia e implementación de políticas de acceso, y otro relativo a la capacidad del repositorio de demostrar que ofrece objetos auténticos como DIP. Así, el primer requisito está relacionado con las solicitudes iniciadas por el usuario y la forma en la que el repositorio las gestiona para asegurar que se respectan los derechos y acuerdos, se monitoriza la seguridad, se da respuesta a las solicitudes, etc. El segundo requisito está relacionado con qué se envía al Consumidor y la confianza que se puede poner en esta información.

Tiene que entenderse que las capacidades y la sofisticación del sistema de acceso variarán dependiendo de la Comunidad Específica del repositorio, y de sus obligaciones para dar acceso. Dada la variedad de repositorios y obligaciones de acceso, estos criterios pueden ser objeto de interpretación y distinta aplicabilidad a nivel local.

4 Gestión del objeto digital

4.6 Gestión de acceso

4.6.1 El repositorio debe cumplir con sus Políticas de Acceso Justificación

Esto es necesario para asegurar que el repositorio ha considerado todos los aspectos del uso que podrían afectar a su confiabilidad, particularmente en referencia al soporte a la comunidad de usuarios.

Declaraciones de políticas disponibles para las comunidades de usuarios; información acerca de las posibilidades ofrecidas a los usuarios (matrices de autenticación); logs y pistas de auditoría de peticiones de acceso; pruebas explícitas de ciertos tipos de acceso.

4.6.1.1 El repositorio debe registrar y revisar todos los fallos y anomalías en la gestión de accesos

Los logs de acceso, la capacidad del sistema de usar herramientas de análisis y monitorización automático y generar mensajes de error/problema; notas de las revisiones realizadas y de la acciones llevadas a cabo como resultado de las revisiones.

4 Gestión del objeto digital

4.6 Gestión de acceso

4.6.2 El repositorio debe seguir políticas y procedimientos que permitan la consulta de objetos digitales trazables a los originales, con evidencias que soporten su autenticidad

Documentos de diseño del sistema; instrucciones de trabajo (si los DIP implican algún procesamiento manual); revisiones guiadas del proceso; producción de una copia de ejemplo con evidencias de su autenticidad; documentación de los requisitos de la comunidad para evidenciar la autenticidad.

4.6.2.1 El repositorio debe registrar y actuar ante los problemas relativos a errores en los datos o en las respuestas de los usuarios

Documentos de diseño del sistema; instrucciones de trabajo (si los DIPs implican procesamiento manual); revisiones guiadas del proceso; logs de solicitudes y de la producción de DIP; documentación de informes de errores y de las acciones llevadas a cabo.

5. Gestión de riesgos de infraestructura y de seguridad

5.1 Gestión de riesgos de infraestructura técnica

5.2 Gestión del riesgo de seguridad

5. Gestión de riesgos de infraestructura y de seguridad

5.1 Gestión de riesgos de infraestructura técnica

5.2 Gestión del riesgo de seguridad

5.1 Gestión de riesgos de infraestructura técnica

5.1.1 El repositorio debe identificar y gestionar los riesgos que afecten a sus actividades de conservación y a los objetivos asociados con su infraestructura técnica

5.1.2 El repositorio debe gestionar el número y la localización de copias de todos los objetos digitales

5.1 Gestión de riesgos de infraestructura técnica

5.1.1 El repositorio debe identificar y gestionar los riesgos que afecten a sus actividades de conservación y a los objetivos asociados con su infraestructura técnica

1) Inventario de infraestructura de los componentes del sistema;
2) evaluaciones periódicas de la tecnología;
3) estimaciones de la obsolescencia de los componentes del sistema;
4) exportación de registros auténticos a un sistema independiente;
5) uso de software soportado por la comunidad y abierto;
6) re-creación de archivos a partir de copias de seguridad.

5.1.1 El repositorio debe identificar y gestionar los riesgos que afecten a sus actividades de conservación y a los objetivos asociados con su IT

5.1.1.1 El repositorio debe utilizar observatorios tecnológicos u otros monitoreos de las tecnologías.

5.1.1.2 El repositorio debe disponer de hardware y software adecuados para realizar las copias de seguridad, conservar el contenido del repositorio y monitorizar sus funciones.

5.1.1.3 El repositorio debe disponer de mecanismos efectivos para detectar la pérdida/corrupción de bits.

5.1.1.4 El repositorio debe disponer de un proceso para registrar y reaccionar ante la disponibilidad de actualizaciones de seguridad, basado en una evaluación riesgo-beneficio.

5.1.1.5 El repositorio debe disponer de procesos definidos para cambios en los medios de almacenamiento y/o en el hardware (por ejemplo, migración o refresco).

5.1.1.6 El repositorio debe haber identificado y documentado los procesos críticos que afectan a su capacidad para cumplir con las responsabilidades que tiene asignadas.

5. Gestión de riesgos de infraestructura y de seguridad

5.1.1 Gestión de riesgos de infraestructura técnica

5.1.1.1 El repositorio debe utilizar observatorios tecnológicos u otros sistemas de monitorización de las tecnologías

5.1.1.2 Debe disponer de hardware y software adecuados para realizar las copias de seguridad, conservar el contenido.

5.1.1.3 El repositorio debe disponer de mecanismos efectivos para detectar la pérdida y corrupción de bits

5.1.1.4 Debe disponer de un proceso para registrar y reaccionar ante la disponibilidad de actualizaciones de seguridad, basado en una evaluación riesgo-beneficio

5.1.1.5 Debe disponer de procesos definidos para cambios en los medios de almacenamiento y/o en el hardware (por ejemplo, migración o refresco)

5.1.1.6 Debe haber identificado y documentado los procesos críticos que afectan su capacidad

5.1.1.1 El repositorio debe utilizar observatorios tecnológicos u otros sistemas de monitorización de las tecnologías

5.1.1.1.1 El repositorio debe disponer de tecnologías hardware adecuadas a los servicios que ofrece a las Comunidades Específicas

5.1.1.1.2 El repositorio debe disponer de procedimientos implantados para monitorizar y recibir notificaciones cuando sean necesarios cambios en la tecnología hardware

5.1.1.1.3 El repositorio debe disponer de procedimientos implantados para evaluar cuándo es necesario hacer cambios en el hardware existente

5.1.1.1 El repositorio debe utilizar observatorios tecnológicos u otros sistemas de monitorización de las tecnologías

5.1.1.1.4 El repositorio debe disponer de procedimientos, compromiso y financiación para reemplazar el hardware cuando la evaluación indique que esto se necesita

5.1.1.1.5 El repositorio debe disponer de tecnologías software adecuadas para los servicios que ofrece a sus comunidades específicas

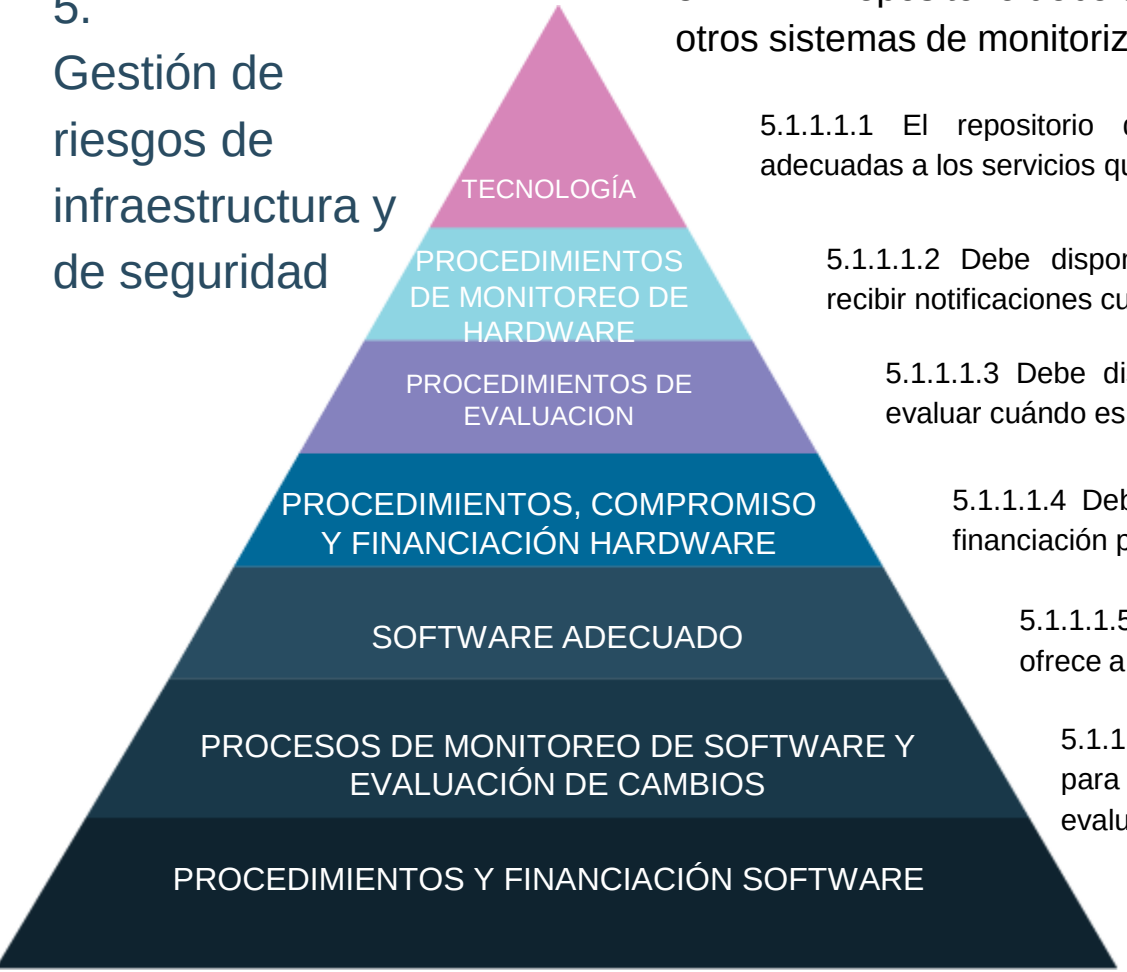
5.1.1.1.6 El repositorio debe disponer de procedimientos implantados para monitorizar y recibir notificaciones cuando sean necesarios los cambios en el software

5.1.1.1 El repositorio debe utilizar observatorios tecnológicos u otros sistemas de monitorización de las tecnologías

5.1.1.1.7 El repositorio debe disponer de procedimientos implantados para evaluar cuándo se necesitan hacer cambios en el software existente

5.1.1.1.8 El repositorio debe disponer de procedimientos, compromiso y financiación para reemplazar el software cuando la evaluación indique que esto se necesita

5. Gestión de riesgos de infraestructura y de seguridad



5.1.1.1 El repositorio debe utilizar observatorios tecnológicos u otros sistemas de monitorización de las tecnologías

5.1.1.1.1 El repositorio debe disponer de tecnologías hardware adecuadas a los servicios que ofrece a las Comunidades Específicas

5.1.1.1.2 Debe disponer de procedimientos Para monitorizar y recibir notificaciones cuando sean necesarios cambios de hardware

5.1.1.1.3 Debe disponer de procedimientos implantados para evaluar cuándo es necesario hacer cambios en el hardware

5.1.1.1.4 Debe disponer de procedimientos, compromiso y financiación para reemplazar el hardware cuando se necesite

5.1.1.1.5 Software adecuado para los servicios que ofrece a sus comunidades específicas

5.1.1.1.6 y 5.1.1.1.7 Debe disponer de procedimientos para monitorear el software, recibir notificaciones y evaluar cuándo realizar los cambios

5.1.1.1.8 El repositorio debe disponer de procedimientos, compromiso y financiación para reemplazar el software cuando la evaluación indique que esto se necesita

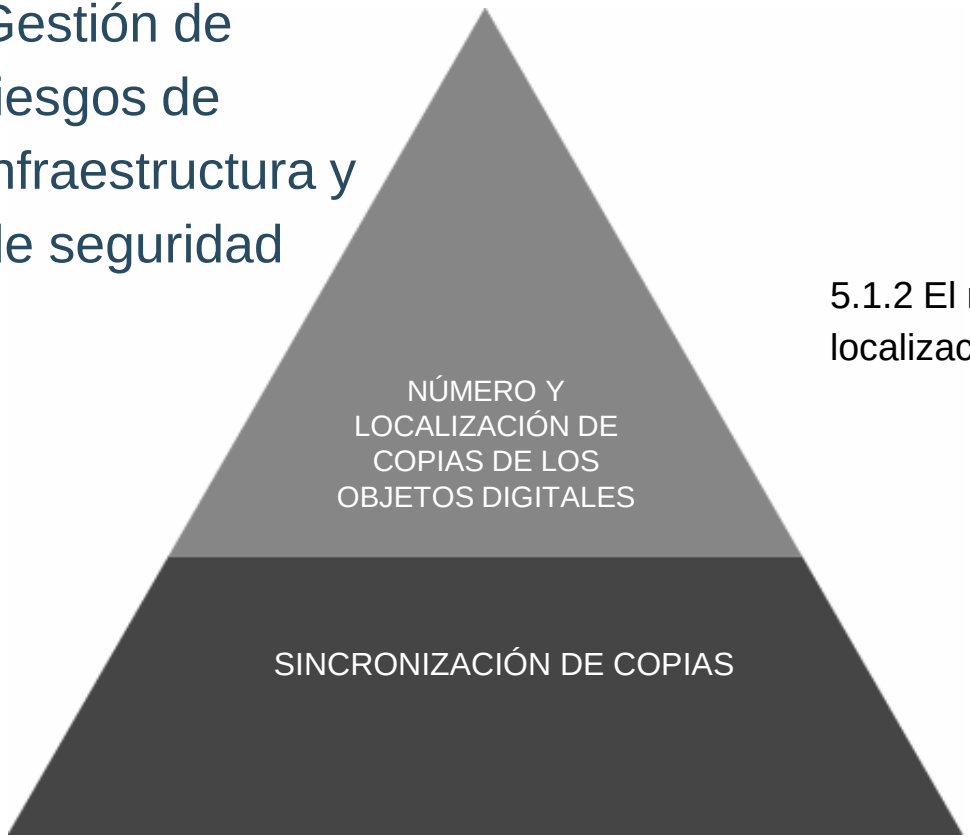
5.1.2 El repositorio debe gestionar el número y la localización de copias de todos los objetos digitales

Ejemplos: Pruebas aleatorias de recuperación; validación de la existencia de un objeto para cada localización registrada; validación de una localización registrada en sistemas de almacenamiento para cada objeto; comprobación de la información de procedencia y fijeza; registro/log de localización de los objetos digitales en comparación con el número previsto y localización de las copias de cada uno de los objetos.

5.1.2.1 El repositorio debe tener mecanismos vigentes para asegurar que están sincronizadas cualesquiera/múltiples copias de los objetos digitales

Sincronización de los flujos de trabajo; análisis de sistema de cuánto tiempo mantiene las copias a sincronizar; procedimientos/documentación de los procesos de sincronización.

5. Gestión de riesgos de infraestructura y de seguridad



5.1.2 El repositorio debe gestionar el número y la localización de copias de todos los objetos digitales

5.1.2.1 El repositorio debe tener mecanismos vigentes para asegurar que están sincronizadas cualesquiera/múltiples copias de los objetos digitales

5.2 Gestión del riesgo de seguridad

5.2.1 El repositorio debe mantener un análisis sistemático de seguridad de los factores de riesgo asociados con los datos, sistemas, personal e instalaciones.

5.2.2 El repositorio debe tener implementados controles adecuadamente dirigidos a cada uno de los riesgos de seguridad definidos.

5.2.3 El personal del repositorio debe tener roles, responsabilidades y autorizaciones delimitados relacionados con los cambios de implementación dentro del sistema.

5.2.4 El repositorio debe tener un plan(es) de preparación y de prevención de desastres escrita adecuada, que incluya al menos una copia de seguridad fuera de las instalaciones de toda la información conservada asociada a una copia externa del plan(es) de prevención

5. Gestión de riesgos de infraestructura y de seguridad

5.2 Gestión del riesgo de seguridad

5.2.1 El repositorio debe mantener un análisis sistemático de seguridad de los factores de riesgo asociados con los datos, sistemas, personal e instalaciones.

5.2.2 El repositorio debe tener implementados controles adecuadamente dirigidos a cada uno de los riesgos de seguridad definidos.

5.2.3 El personal del repositorio debe tener roles, responsabilidades y autorizaciones delimitados relacionados con los cambios de implementación dentro del sistema.

5.2.4 El repositorio debe tener un plan(es) escrito de preparación y de prevención de desastres que incluya al menos una copia de seguridad fuera de las instalaciones de toda la información conservada

Comparación entre distintos estándares

- Análisis de tres directrices de certificación y auditoría de repositorios confiables: TRAC, NESTOR e ISO 16363.
- Tras presentar las tres directrices, se realiza un estudio comparativo de los criterios relativos a: marco organizativo, gestión del objeto digital e infraestructura técnica y seguridad.

Trustworthy repositories. Audit & Certification: Criteria and Checklist	Catalogue of Criteria for Trusted Digital Repositories	Audit and Certification of Trustworthy Digital Repositories / ISO 16363
TRAC	**NESTOR**	**CCSDS/ISO16363**
A. Organizational infrastructure A1. Governance & Organizational viability A2. Organizational structure & Staffing A3. Procedural accountability & Policy Framework A4. Financial Sustainability A5. Contracts, licenses, & liabilities	**A. Organizational framework** 1. The DR has defined its goals. 2. The DR grants its designated community/communities adequate access to the information represented by the digital objects. 3. Legal and contractual rules are observed. 4. The organizational form is appropriate for the DR. 5. The digital repository undertakes appropriate quality management.	**1. Organizational infrastructure** 1.1 Governance and Organizational viability 1.2. Organizational structure and Staffing 1.3. Procedural accountability and Policy Framework 1.4. Financial Sustainability 1.5. Contracts, licenses and liabilities
B. Digital Object Management B1. Ingest: acquisition of content B2. Ingest: creation of the archivable package B3. Preservation planning B4. Archival storage & preservation/maintenance of AIPs B5. Information management B6. Access management	**B. Object management** 6. The DR ensures the integrity of the digital object during all processing stages. 7. The DR ensures the authenticity of the digital objects during all processing stages. 8. The DR has a strategic plan for its technical preservation measures. 9. The DR accepts digital objects from the producers based on defined criteria 10. Archival storage of the digital objects is undertaken to defined specifications 11. The DR permits usage of the digital objects based on defined criteria 12. The data management system is capable of providing the necessary digital repository functions.	**2. Digital object management** 2.1. Ingest: acquisition of content 2.2. Ingest: creation of the AIP 2.3. Preservation planning 2.4. AIP Preservation 2.5. Information management 2.6. Access management
C. Technologies, Technical Infrastructure, & Security C1. System infrastructure C2 Appropriate technologies C3 Security	**C. Infrastructure and Security** 13. The IT infrastructure is adequate 14. The infrastructure protects the digital repository and its digital objects.	**3. Infrastructure and security risk management** 3.1. Technical infrastructure risk management 3.2. Security risk management

BONAL ZAZO, José Luis ; DE LORENZO - CÁCERES, María del Pilar Ortego (2017).

Ejercitación futura

1) Accede al checklist:

En español: https://docs.google.com/spreadsheets/d/1x5mtki40f1cU0DMZVA-TIMLTWlwPCti5fcmZep4k3wM/edit#gid=1982776616

En inglés:

https://docs.google.com/spreadsheets/d/1tWAjMcAbm6ufDGdGgvVNWxAeNrF4PwwbTAy95-OQQ2w/edit?usp=sharing

1) Haga una copia del mismo en su unidad en DRIVE.
2) Lea atentamente la solapa de preparación para la auditoría.
3) Complete las solapas 3, 4 y 5 (o las que le sean posibles) siguiendo las instrucciones del punto 1).

Bibliografía

Argentina. *Ley Nacional 26899: Creación de Repositorios Digitales Institucionales de Acceso Abierto, Propios o Compartidos*. , (2013).

Barrueco Cruz, J. M., De Miguel Estévez, M., González Copeiro, C., & Rico-Castro, P. (s. f.). *Guía para la evaluación de repositorios institucionales de Investigación. 2ª Edición. FECYT, RECOLECTA, CRUE y REBIUN*. 34.

Birds of a Feather group of audit checklist standardisation. Sección 5 del Modelo OAIS. (2013, mayo 24). Recuperado 9 de mayo de 2019, de RDA website: https://www.rd-alliance.org/groups/rdawds-certification-digital-repositories-ig.html

Bonal Zazo, J. L., & de Lorenzo - Cáceres, M. del P. O. (2017). Criterios de certificación y auditoría de repositorios digitales seguros en archivos. En M. Caixas, N. Vaquinhas, & H. Vinagre (Eds.), *Da produção à preservação informacional: desafios e oportunidades* (pp. 529-550). Recuperado de http://books.openedition.org/cidehus/2835

Cassella, M. (2010). Institutional Repositories: an Internal and External Perspective on the Value of IRs for Researchers' Communities. *LIBER Quarterly*, *20*(2), 210-225. https://doi.org/10.18352/lq.7989

Bibliografía

Certification and Assessment of Digital Repositories | CRL. (s. f.). Recuperado 9 de mayo de 2019, de https://www.crl.edu/archiving-preservation/digital-archives/certification-assessment

COAR » Technical recommendations for next generation repositories. (s. f.). Recuperado 12 de enero de 2018, de https://www.coar-repositories.org/news-media/technical-recommendations-for-next-generation-repositories/

Consultative Comitee for Space Data Systems (CCSDS). (2011). *Audit and Certification of Trustworthy Digital Repositories*. 77.

CRL and DCC Pilot Repository Audits. (s. f.). Recuperado 9 de mayo de 2019, de https://www.repositoryaudit.eu/

Cruz, B., Manuel, J., de València, U., & López, A. (2010). *Guía para la evaluación de repositorios institucionales de Investigación. 1ª Edición. FECYT, RECOLECTA, CRUE y REBIUN*. 29.

Data Seal of Approval. (s. f.). Recuperado 9 de mayo de 2019, de https://www.datasealofapproval.org/en/

Bibliografía

De Giusti, Marisa R. (2018, octubre). *Evaluación y certificación de repositorios institucionales de acceso abierto*. Presentado en XXVIII Asamblea General del ISTEC 2018 “La influencia de la tecnología en las comunidades del conocimiento” (Bolivia, 2018). Recuperado de http://sedici.unlp.edu.ar/handle/10915/69961

De Giusti, Marisa Raquel. (2017). *Indicadores de calidad en repositorios de acceso abierto*. Presentado en VIII Jornada Virtual de Acceso Abierto Argentina 2017 (Buenos Aires, 2017). Recuperado de http://hdl.handle.net/10915/63176

Deutsche Nationalbibliothek - Projects - NESTOR - Network of Expertise in Long-term Storage of Digital Resources. (s. f.). Recuperado 9 de mayo de 2019, de http://www.dnb.de/EN/Wir/Projekte/Archiv/nestor.html

DINI Certificate for Open Access Repositories and Publication Services. (2016). Recuperado 9 de mayo de 2019, de Deutsche Initiative für Netzwerkinformation e.V. website: https://dini.de/dienste-projekte/dini-zertifikat/english/about-the-certificate/

DINI Working Group, & Electronic Publishing. (2016). DINI Certificate for Open Access Repositories and Publication Services.

Bibliografía

DRAMBORA Interactive released. (s. f.). Recuperado 9 de mayo de 2019, de https://www.repositoryaudit.eu/

DRAMBORA: The Digital Repository Audit Method Based on Risk Assessment. (s. f.). Recuperado 9 de mayo de 2019, de ResearchGate website: https://www.researchgate.net/publication/31869604_DRAMBORA_The_Digital_Repository_Audit_Method_Based_on_Risk_Assessment

FAIR Principles. (s. f.). Recuperado 9 de mayo de 2019, de GO FAIR website: https://www.go-fair.org/fair-principles/

International Organization for Standardization (ISO). (2015). *UNE-ISO 14721:2015 Sistemas de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS). Modelo de referencia.* Recuperado de https://www.aenor.com/normas-y-libros/buscador-de-normas/iso/?c=062542

Bibliografía

International Organization for Standardization (ISO). (2017). *UNE-ISO 16363:2017 Sistemas de transferencia de información y datos espaciales. Auditoría y certificación de repositorios digitales de confianza.* Recuperado de https://www.aenor.com/normas-y-libros/buscador-de-normas/iso/?c=062542

Kim, Y. H., & Kim, H. H. (2008). Development and validation of evaluation indicators for a consortium of institutional repositories: A case study of dcollection. *Journal of the American Society for Information Science and Technology*, *59*(8), 1282-1294. https://doi.org/10.1002/asi.20818

Ministerio de Ciencia, Tecnología e Innovación Productiva. *Resolución 753- E/2016 MINCYT*. , (2016).

NDSA - Levels of Digital Preservation. (s. f.). Recuperado 9 de mayo de 2019, de National Digital Stewardship Alliance - Digital Library Federation website: http://ndsa.org//activities/levels-of-digital-preservation/

nestor Catalogue of Criteria for Trusted Digital Repositories | Digital Curation Centre. (s. f.). Recuperado 9 de mayo de 2019, de http://www.dcc.ac.uk/resources/repository-audit-and-assessment/nestor

Bibliografía

nestor repository criteria (Version 2). (s. f.). Recuperado 9 de mayo de 2019, de http://files.dnb.de/nestor/materialien/nestor_mat_08-eng.pdf

nestor Seal for Trustworthy Digital Archives. (s. f.). Recuperado 9 de mayo de 2019, de http://www.dnb.de/Subsites/nestor/EN/Siegel/siegel.html

nestor Working Group, & Trusted Repositiories – Certification. (2006). *Catalogue of Criteria for Trusted Digital Repositories Version 1 (draft for public comment)*. Recuperado de http://files.dnb.de/nestor/materialien/nestor_mat_08-eng.pdf

OpenAIRE Guidelines — OpenAIRE Guidelines documentation. (s. f.). Recuperado 9 de mayo de 2019, de https://guidelines.openaire.eu/en/latest/

Primary Research Group. (s. f.). Recuperado 9 de mayo de 2019, de https://www.primaryresearch.com/Pressrelease.aspx

RDA/WDS Certification of Digital Repositories IG. (2013, mayo 24). Recuperado 9 de mayo de 2019, de RDA website: https://www.rd-alliance.org/groups/rdawds-certification-digital-repositories-ig.html

Bibliografía

RLG/NARA Draft Audit Check-list for Repository Certification. (s. f.). Recuperado 9 de mayo de 2019, de http://www.dcc.ac.uk/news/audit-checklist-certifying-digital-repositories-released

Serrano Vicente, R. (2017). *Evaluación de los repositorios institucionales de acceso abierto en España* (Ph.D. Thesis, Universitat de Barcelona). Recuperado de http://www.tdx.cat/handle/10803/463047

Swan, A., & Houghton, J. (2012, julio 5). Going for Gold? The costs and benefits of Gold Open Access for UK research institutions: further economic modelling. Report to the UK Open Access Implementation Group [Other including Programme/Project deposits]. http://repository.jisc.ac.uk/610/2/Modelling_Gold_Open_Access_for_institutions_%2D_final_draft3.pdf

Térmens, M., & Leija, D. (2017). Auditoría de preservación digital con NDSA Levels. *El Profesional de la Información*, *26*(3), 447-456. https://doi.org/10.3145/epi.2017.may.11

Bibliografía

TRAC Metrics | CRL. (s. f.). Recuperado 9 de mayo de 2019, de https://www.crl.edu/archiving-preservation/digital-archives/metrics-assessing-and-certifying/trac

Vicente, R. S., Melero, R. M., & Abadal, E. (2014). Indicadores para la evaluación de repositorios institucionales de acceso abierto. *Anales de Documentación*, *17*(2). https://doi.org/10.6018/analesdoc.17.2.190821

Vierkant, P. (2013). ensus of Open Access Repositories in Germany: Turning Perceived Knowledge Into Sound Understanding. *D-Lib Magazine*, *19*(11/12). Recuperado de doi:10.1045/november2013-vierkant

Westell, M. (2006). Institutional repositories: proposed indicators of success. *Library Hi Tech*, *24*(2), 211-226. https://doi.org/10.1108/07378830610669583

¡Hagamos realidad la ciencia abierta!
¡Muchas gracias!

Consultas:
marisa.degiusti@sedici.unlp.edu.ar

Colección de nuestros trabajos:
http://sedici.unlp.edu.ar/handle/10915/25293

http://sedici.unlp.edu.ar

http://digital.cic.gba.gob.ar/

http://cesgi.cic.gba.gob.ar/

http://prebi.unlp.edu.ar

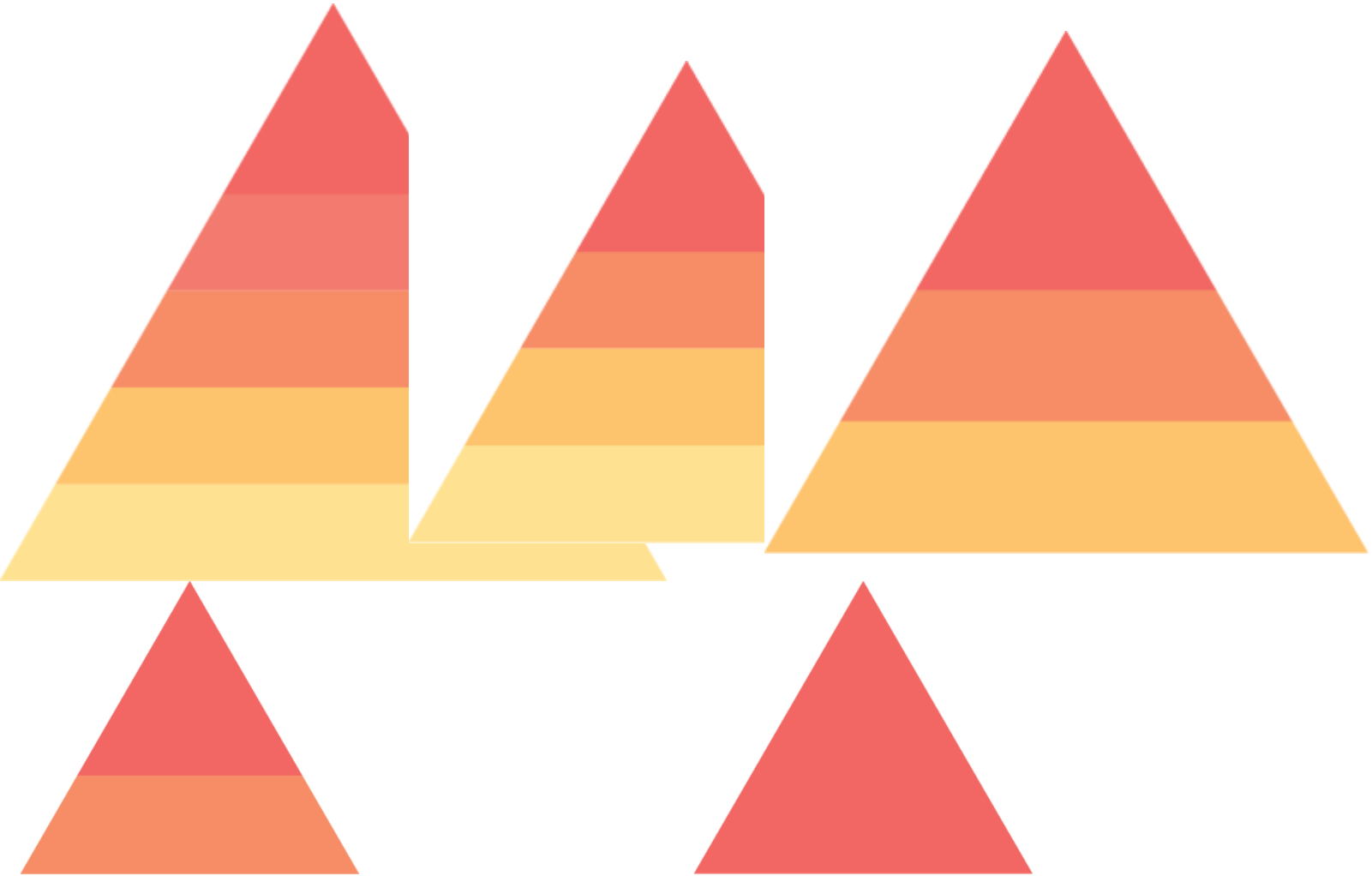
http://www.istec.org/liblink/

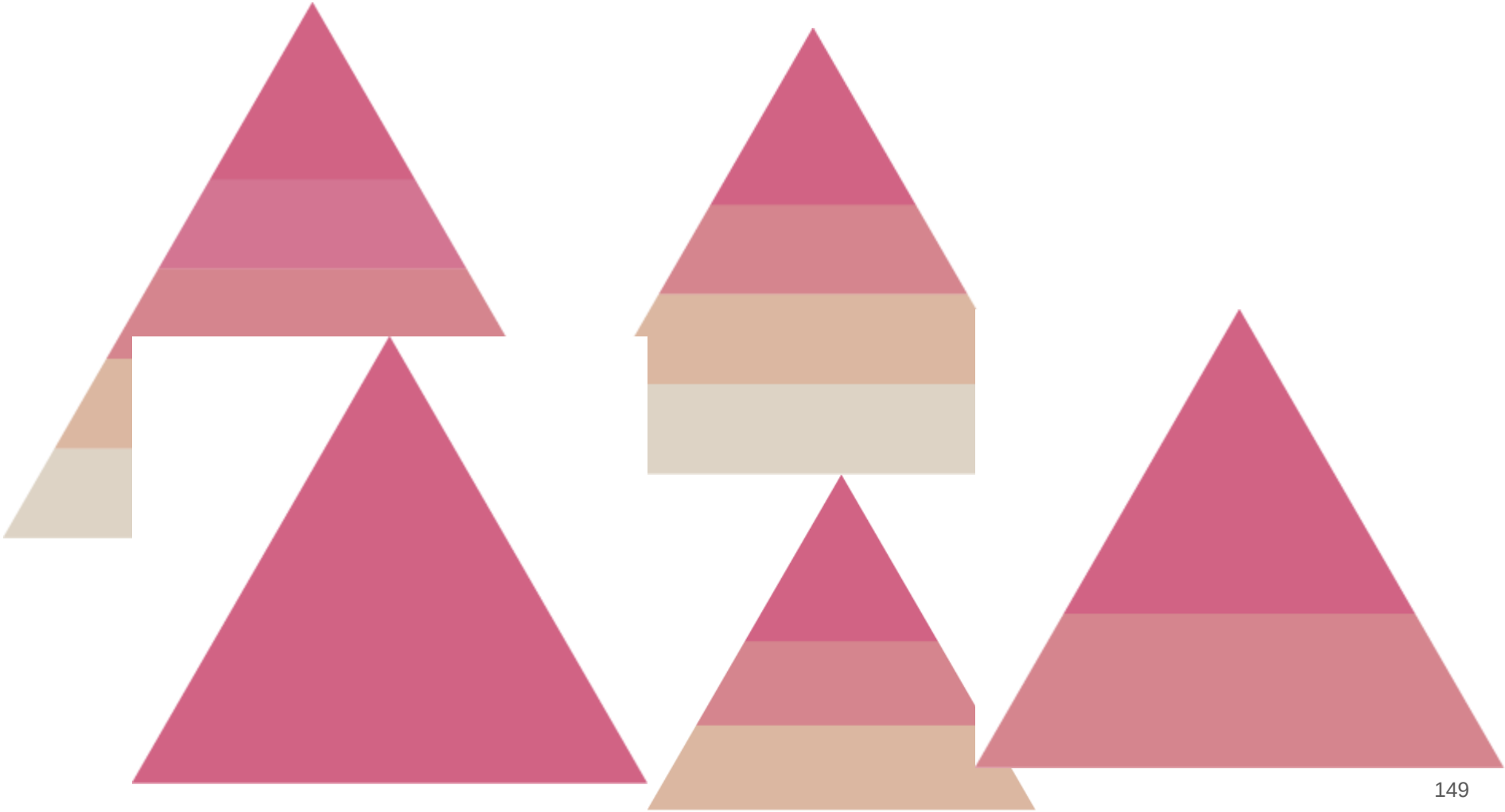
http://revistas.unlp.edu.ar/cientificas/

http://revistas.unlp.edu.ar

http://congresos.unlp.edu.ar

http://ibros.unlp.edu.ar





3 Gestión del objeto digital

3.1 Viabilidad de la organización y su gobierno

3.2 3.3 3.4 3.5

3.1.1 El repositorio debe tener una declaración de la misión que refleje un compromiso con la información digital para su conservación, retención a largo plazo, gestión y acceso. Esto es la declaración de la misión o el acta constitutiva del repositorio.

3.1.2 El repositorio debe tener un Plan Estratégico de Conservación que defina el enfoque que el repositorio mantendrá en el soporte a largo plazo de su misión.

- **3.1.2.1** Plan de continuidad, plan de contingencia por si deja de funcionar.
- **3.1.2.2** El repositorio debe supervisar su entorno para determinar cuándo ejecutar su plan de sucesión, los planes de contingencia y/o acuerdos de garantía

3.1.3 El repositorio debe tener una Política de Colección/Fondo u otro documento que especifique el tipo de información que conservará.

3.2.1

El repositorio debe tener identificadas y establecidas las responsabilidades necesarias a llevar a cabo y debe tener personal designado con adecuadas habilidades y experiencia para cumplir estas funciones.

3.2.1.1 El repositorio debe haber identificado sus funciones. Plan de dotación de personal; definición de competencias; descripciones del trabajo; planes de desarrollo profesional; certificados de formación y acreditación; además de la evidencia de que el repositorio revisa estos documentos.

3.2.1.2 El repositorio debe tener el número apropiado de personal para apoyar todas las funciones y servicios.

3.2.1.3 El repositorio debe contar con un activo programa de desarrollo profesional que proporcione oportunidades de desarrollo al personal con habilidades y conocimientos.

3 Gestión del objeto digital

3.3.1 El repositorio debe tener definida su Comunidad Específica y debe tener estas definiciones accesibles.

3.3.2 El repositorio debe contar con Políticas de Conservación para asegurar que cumplirá con su Plan Estratégico de Conservación.

3.3.2.1 El repositorio debe tener mecanismos para la revisión, actualización y desarrollo continuo de sus Políticas de Conservación tal y como el repositorio crece y cómo evolucionan la tecnología y la práctica de la comunidad.

3.3.3 El repositorio debe tener una historia documentada de los cambios en sus operaciones, procedimientos, software y hardware.

3.3.4 El repositorio debe comprometerse con la transparencia y la rendición de responsabilidad en todas las acciones de apoyo al funcionamiento y gestión del repositorio que afecte a la conservación del contenido digital a través del tiempo.

3.3.5 El repositorio debe definir, recopilar, rastrear y proporcionar adecuadamente sus mediciones de integridad de la información.

3.3.6 El repositorio debe estar comprometido con un programa regular de autoevaluación y certificación externa

3.4.1 El repositorio debe contar en su sitio con procesos de planificación de negocios a corto y largo plazo para mantener el repositorio a lo largo del tiempo.

3.4.2 El repositorio debe tener prácticas financieras y procedimientos que sean transparentes, que cumplan con las normas y prácticas de contabilidad pertinentes, y auditadas por terceros de conformidad con los requisitos legales nacionales.

3.4.3 El repositorio debe tener un compromiso continuado en analizar e informar sobre el riesgo financiero, el beneficio, la inversión y el gasto (incluyendo activos, licencias y pasivos)

3.5.1 El repositorio debe tener y mantener los contratos apropiados o contratos de depósito para los materiales digitales que gestiona, conserva, y/o para los que proporciona acceso

- **3.5.1.1** El repositorio debe tener contratos o acuerdos de depósito que especifiquen y transfieran todos los derechos de conservación necesarios, y deben documentarse los derechos transferidos
- **3.5.1.2** El repositorio debe haber especificado todos los aspectos pertinentes de la adquisición, mantenimiento, acceso y retirada de acuerdos escritos con los depositantes y otras partes pertinentes
- **3.5.1.3** El repositorio debe tener políticas escritas que indiquen cuando acepta la responsabilidad de la conservación del contenido de cada conjunto de objetos de datos transferidos
- **3.5.1.4** El repositorio debe contar con políticas establecidas para abordar la responsabilidad y desafíos en la propiedad/derechos.

3.5.2 El repositorio debe rastrear y administrar los derechos de propiedad intelectual y las restricciones en el uso de los contenidos del repositorio como exige el acuerdo, contrato o licencia de depósito.

4.1 Ingreso: adquisición de contenido

4.1.1 El repositorio debería identificar la Información de Contenido y las Propiedades de la Información que va a preservar.

- **4.1.1.1** Debe tener un(os) procedimiento(s) para identificar las Propiedades de la Información que conservará.
- **4.1.1.2** Debe tener un documento de la Información de Contenido y de las Propiedades de la Información que conservará

4.1.2 El repositorio debe especificar claramente la información que necesita ser asociada con la Información de Contenido específica en el momento de su depósito

4.1.3 El repositorio debe tener especificaciones adecuadas que permitan el reconocimiento y análisis de los SIPs

4.1.4 El repositorio debe tener mecanismos para verificar apropiadamente la identidad del Productor de todos los materiales

4.1.5 El repositorio debe tener un proceso de ingreso que verifique cada SIP por completitud y exactitud

4.1.6 El repositorio debe obtener control suficiente sobre los Objetos Digitales para conservarlos

4.1.7 El repositorio debe proveer al productor/depositante con las acciones adecuadas en puntos acordados durante el proceso de ingreso

4.1.8 El repositorio debe tener documentos vigentes de las acciones de los procesos de administración relevantes para la adquisición de contenido

4.2.1 El repositorio debe tener conservada una descripción para cada AIP o cada clase de AIPs, adecuada para el análisis del AIP y las necesidades de conserv ación a largo plazo

4.2.1.1 El repositorio debe ser capaz de identificar qué descripción se aplica a qué AIP Justificación

4.2.1.2 El repositorio debe tener una descripción para cada AIP que sea adecuada para la conservación a largo plazo, permitiendo la identificación y análisis de todos los componentes requeridos dentro del AIP

4.2.2
4.2.3
4.2.4
4.2.5
4.2.6
4.2.7
4.2.8
4.2.9
4.2.10

4.2.1

4.2.2 El repositorio debe tener una descripción de cómo los AIPs son construidos desde los SIP

4.2.3 El repositorio debe documentar la disposición final de todos los SIP

- **4.2.3.1** El repositorio debe seguir procedimientos documentados cuando un SIP no se incorpore a un AIP o se descarte, indicándose las razones

4.2.4 El repositorio debe tener y usar una convención para generar identificadores unívocos y continuos para todos los AIP. Tienen que comprobarse los siguientes aspectos

4.2.5

4.2.6

- **4.2.4.1** El repositorio debe identificar unívocamente cada AIP en el propio repositorio
  - **4.2.4.1.1** El repositorio debe de disponer de identificadores unívocos
  - **4.2.4.1.2** El repositorio debe asignar y mantener identificadores continuos
  - **4.2.4.1.3** La documentación debe describir cualquier proceso empleado para cambiar cada uno de los identificadores
  - **4.2.4.1.4** El repositorio debe ser capaz de proporcionar una lista completa de todos esos identificadores y hacer controles aleatorios por las duplicaciones
  - **4.2.4.1.5** El sistema de identificadores debe ser adecuado para validar los actuales y futuros requisitos del repositorio, tal como el número de objetos
- **4.2.4.2** El repositorio debe tener un sistema de seguridad de conexión/servicio de resolución para encontrar unívocamente el objeto identificado sin importar su ubicación física

4.2.7

4.2.8

4.2.9

4.2.10

4.2.1

4.2.2

4.2.3

4.2.4

4.2.5

4.2.6

4.2.7

4.2.8

4.2.9

4.2.10

El repositorio debe tener acceso a las herramientas y recursos necesarios para proveer la Información de Representación fidedigna para todos los objetos digitales que contengan. Tienen que comprobarse los siguientes aspectos:

- **4.2.5.1** El repositorio debe tener herramientas y métodos para identificar los tipos de ficheros de todos los Objetos de Datos transferidos
- **4.2.5.2** El repositorio debe tener herramientas y métodos para determinar qué Información de Representación es necesaria para hacer cada Objeto de Datos comprensible a cada Comunidad Específica
- **4.2.5.3** El repositorio debe tener acceso a la Información de Representación
- **4.2.5.4** El repositorio debe tener herramientas y métodos para asegurar que la Información de Representación requerida sea asociada de modo continuo con los Objetos de Datos correspondientes

4.2.1

4.2.2

4.2.3

4.2.4

4.2.5

4.2.6

4.2.7

4.2.8

4.2.9

4.2.10

El repositorio debe disponer de procesos documentados para adquirir la Información de Descripción de Conservación (PDI) para su Información de Contenido asociada y para adquirir la PDI de acuerdo con los procesos documentados. En particular, tiene que comprobar los siguientes aspectos:

- **4.2.6.1** El repositorio debe documentar los procesos para adquirir la PDI
- **4.2.6.2** El repositorio debe ejecutar sus procesos documentados para adquirir la PDI
- **4.2.6.3** El repositorio debe asegurar que la PDI sea continuamente asociada con la Información de Contenido correspondiente

4.2.1

4.2.2

4.2.3

4.2.4

4.2.5

4.2.6

4.2.7 El repositorio debe asegurar que la Información de Contenido del AIP es comprensible por su Comunidad Específica en cualquier momento de la creación del AIP

- **4.2.7.1** El repositorio debe tener un proceso documentado para verificar la inteligibilidad de la Información de Contenido de los AIP en su creación para su Comunidad Específica
- **4.2.7.2** El repositorio debe ejecutar el proceso de verificación para cada clase de Información de Contenido
- **4.2.7.3** El repositorio debe llevar la Información de Contenido del AIP hasta el nivel requerido de inteligibilidad si la verificación de inteligibilidad falla

4.2.8

4.2.9

4.2.10

4.2.1

4.2.2

4.2.3

4.2.4

4.2.5

4.2.6

4.2.7

4.2.8	El repositorio debe verificar que cada AIP está completo y es correcto desde el momento en que se crea
4.2.9	El repositorio debe proporcionar un funcionamiento independiente para verificar la integridad de la colección/fondo/contenido del repositorio
4.2.10	El repositorio debe tener documentos actualizados de las acciones y procesos de administración que son relevantes para la creación del AIP

4.3.1 El repositorio debe tener estrategias de conservación documentadas relevantes para sus fondos

4.3.2 El repositorio debe monitorear su entorno de conservación

4.3.2.1 El repositorio debe tener dispositivos para monitorear y notificar cuándo la Información de Representación es inadecuada para que la Comunidad Específica comprenda los fondos de datos.

4.3.3 El repositorio debe tener mecanismos para cambiar sus planes de conservación como resultado de sus actividades de monitorización

4.3.3.1 El repositorio debe tener mecanismos para crear, identificar o reunir cualquier Información de Representación extra que se le requiera

4.3.4 El repositorio debe proporcionar evidencia de la efectividad de sus actividades de conservación

4.4.1 El repositorio debe tener especificaciones sobre cómo se almacenan los AIPs hasta el nivel de bit

- **4.4.1.1** El repositorio debe conservar la Información de Contenido de los AIPs
- **4.4.1.2** El repositorio debe monitorizar activamente la integridad de los AIPs

4.4.2 El repositorio debe tener registros contemporáneos a las acciones y procesos de administración relevantes para el almacenamiento y la conservación de los AIPs

- **4.4.2.1** El repositorio debe tener procedimientos para todas las acciones llevadas a cabo en los AIPs
- **4.4.2.2** El repositorio debe ser capaz de demostrar que cualquier acción llevada a cabo en los AIPs cumple con los requisitos de la especificación de esas acciones

4.5.1 El repositorio debe especificar los requisitos de información míni

4.5.2 El repositorio debe capturar o crear la información descriptiva mínima y asegurarse de que está asociada al AIP

4.5.3 El repositorio debe mantener una vinculación bidireccional entre cada AIP y su información descriptiva

4.5.3.1 El repositorio debe mantener las asociaciones entre sus AIPs y su información descriptiva a lo largo del tiempo

4.6.1 El repositorio debe cumplir con sus Políticas de Acceso
Justificación

4.6.1.1 El repositorio debe registrar y revisar todos los fallos y anomalías en la gestión de accesos

4.6.2 El repositorio debe seguir políticas y procedimientos que permitan la consulta de objetos digitales trazables a los originales, con evidencias que soporten su autenticidad

4.6.2.1 El repositorio debe registrar y actuar ante los problemas relativos a errores en los datos o en las respuestas de los usuarios

5 Gestión de riesgos de infraestructura y de seguridad

5.1 Gestión de riesgos de infraestructura técnica 5.2

5.1.1 El repositorio debe identificar y gestionar los riesgos que afecten a sus actividades de conservación y a los objetivos asociados con su infraestructura técnica

5.1.2

5.1.1.1 El repositorio debe utilizar observatorios tecnológicos u otros sistemas de monitorización de las tecnologías

5.1.1.2 El repositorio debe disponer de hardware y software adecuados para realizar las copias de seguridad, conservar el contenido del repositorio y monitorizar sus funciones.

5.1.1.3 El repositorio debe disponer de mecanismos efectivos para detectar la pérdida/corrupción de bits

5.1.1.4 El repositorio debe disponer de un proceso para registrar y reaccionar ante la disponibilidad de actualizaciones de seguridad, basado en una evaluación riesgo-beneficio.

5.1.1.5 El repositorio debe disponer de procesos definidos para cambios en los medios de almacenamiento y/o en el hardware (por ejemplo, migración o refresco).

5.1.1.6 El repositorio debe haber identificado y documentado los procesos críticos que afectan a su capacidad para cumplir con las responsabilidades que tiene asignadas.

5 Gestión de riesgos de infraestructura y de seguridad

5.1 Gestión de riesgos de infraestructura técnica 5.2

5.1.1 El repositorio debe identificar y gestionar los riesgos que afecten a sus actividades de conservación y a los objetivos asociados con su infraestructura técnica

5.1.2

5.1.1.1 El repositorio debe utilizar observatorios tecnológicos u otros sistemas de monitorización de las tecnologías

5.1.1.2

5.1.1.3

5.1.1.4

5.1.1.5

5.1.1.6

5.1.1.1.1 El repositorio debe disponer de tecnologías hardware adecuadas a los servicios que ofrece a las Comunidades Específicas

5.1.1.1.2 El repositorio debe disponer de procedimientos implantados para monitorizar y recibir notificaciones cuando sean necesarios cambios en la tecnología hardware

5.1.1.1.3 El repositorio debe disponer de procedimientos implantados para evaluar cuándo es necesario hacer cambios en el hardware existente.

5.1.1.1.4 El repositorio debe disponer de procedimientos, compromiso y financiación para reemplazar el hardware cuando la evaluación indique que esto se necesita

5.1.1.1.5 El repositorio debe disponer de tecnologías software adecuadas para los servicios que ofrece a sus comunidades específicas

5.1.1.1.6 El repositorio debe disponer de procedimientos implantados para monitorizar y recibir notificaciones cuando sean necesarios los cambios en el software

5.1.1.1.7 El repositorio debe disponer de procedimientos implantados para evaluar cuándo se necesitan hacer cambios en el software existente

5.1.1.1.8 El repositorio debe disponer de procedimientos, compromiso y financiación para reemplazar el software cuando la evaluación indique que esto se necesita

5 Gestión de riesgos de infraestructura y de seguridad

5.1 Gestión de riesgos de infraestructura técnica 5.2

5.1.1 El repositorio debe identificar y gestionar los riesgos que afecten a sus actividades de conservación y a los objetivos asociados con su infraestructura técnica

5.1.2 El repositorio debe gestionar el número y la localización de copias de todos los objetos digitales

5.1.2.1 El repositorio debe tener mecanismos vigentes para asegurar que están sincronizadas cualesquiera/múltiples copias de los objetos digitales

5.2.1 El repositorio debe mantener un análisis sistemático de seguridad de los factores de riesgo asociados con los datos, sistemas, personal e instalaciones.

5.2.2 El repositorio debe tener implementados controles adecuadamente dirigidos a cada uno de los riesgos de seguridad definidos.

5.2.3 El personal del repositorio debe tener roles, responsabilidades y autorizaciones delimitados relacionados con los cambios de implementación dentro del sistema.

5.2.4 El repositorio debe tener un plan(es) de preparación y de prevención de desastres escrita adecuada, que incluya al menos una copia de seguridad fuera de las instalaciones de toda la información conservada asociada a una copia externa del plan(es) de prevención