



## SPANISH TRANSLATION FOR THE 2019 LEVELS OF PRESERVATION MATRIX

The 2019 NDSA Levels of Digital Preservation Matrix has been translated into Spanish.

Please find a link to the Spanish translation below.

Citation information and a link to the Spanish translation is as follows:

[Leija, David](#); [Térmens, Miquel](#). (2019). NDSA 2019 Digital Preservation Levels Translation: Spanish Translation of Version 2.0. APREDIG - Asociación Iberoamericana de Preservación Digital.

- V2.0 in Spanish <https://osf.io/eqjk8> | <http://www.apredig.org/npdndsa2019/>

## TRADUCCIÓN AL ESPAÑOL DE LA MATRIZ DE NIVELES DE PRESERVACIÓN DIGITAL 2019

La matriz de niveles de preservación digital NDSA 2019, ha sido traducida al español.

Encuentre un enlace a la traducción al español a continuación:

La información para citar el trabajo y el enlace a la traducción en español es la siguiente:

[Leija, David](#); [Térmens, Miquel](#). (2019). Traducción de Niveles de Preservación Digital NDSA 2019: Traducción al Español de Versión 2.0. APREDIG - Asociación Iberoamericana de Preservación Digital.

- V2.0 en Español: <https://osf.io/eqjk8> | <http://www.apredig.org/npdndsa2019/>

Área Funcional	Nivel			
	Nivel 1 - (Conocer su contenido)	Nivel 2 - (Proteger su contenido)	Nivel 3 - (Controlar su contenido)	Nivel 4 - (Mantener su contenido)
<b>Almacenamiento</b>	<p>Tener dos copias completas en ubicaciones separadas</p> <p>Documentar todos los medios de almacenamiento donde este almacenado el contenido</p> <p>Poner el contenido en soportes de almacenamiento estables</p>	<p>Tener tres copias completas con al menos una copia en una ubicación geográfica distinta</p> <p>Documentar el almacenamiento y medios de almacenamiento, indicando los recursos y las dependencias que estos requieren para funcionar</p>	<p>Tener al menos una copia en una ubicación geográfica con amenaza de desastre diferente a las otras copias</p> <p>Tener al menos una copia en un medio de almacenamiento de diferente tipo</p> <p>Rastrear la obsolescencia del almacenamiento y los medios</p>	<p>Tener al menos tres copias en ubicaciones geográficas distintas, cada una con una amenaza de desastre diferente</p> <p>Maximizar la diversificación del almacenamiento para evitar puntos únicos de falla</p> <p>Tener un plan y realizar acciones para abordar la obsolescencia del hardware, software y medios de almacenamiento</p>
<b>Integridad</b>	<p>Verificar que la información de integridad se ha proporcionado con el contenido</p> <p>Generar información de integridad si esta no ha sido proporcionada con el contenido</p> <p>Se verifica virus en todo el contenido; se aísla el contenido en cuarentena según sea necesario</p>	<p>Verificar la información de integridad al mover o copiar contenido</p> <p>Usar bloqueadores de escritura cuando se trabaja con medios originales</p> <p>Hacer una copia de seguridad de la información de integridad y almacenar una copia en una ubicación separada del contenido</p>	<p>Verificar la información de integridad del contenido en intervalos fijos</p> <p>Documentar los procesos y resultados de verificación de información de integridad</p> <p>Realizar una auditoría de la información de integridad bajo demanda</p>	<p>Verificar la información de integridad en respuesta a eventos o actividades específicas</p> <p>Reemplazar o reparar el contenido dañado según sea necesario</p>
<b>Control</b>	<p>Se determinan los agentes humanos y de software que deben estar autorizados para leer, escribir, mover y eliminar contenido</p>	<p>Documentar a los agentes humanos y de software autorizados para leer, escribir, mover y eliminar contenido y aplicar estos</p>	<p>Mantener los registros (logs) y se identifican a los agentes humanos y de software que realizaron acciones sobre el contenido.</p>	<p>Se realizan revisiones periódicas de acciones / registros (logs) de acceso</p>
<b>Metadatos</b>	<p>Crear un inventario de contenido, documentando también la ubicación de almacenamiento actual de estos</p> <p>Hacer una copia de respaldo del inventario y se almacena al menos una copia por separado</p>	<p>Almacenar suficientes metadatos para saber cuál es el contenido (esto podría incluir alguna combinación de aspectos administrativos, técnicos, descriptivos, de preservación y estructurales)</p>	<p>Determinar qué estándares de metadatos aplicar</p> <p>Encuentra y completa los vacíos en sus metadatos para cumplir con esos estándares</p>	<p>Registrar las acciones de preservación asociadas con el contenido y cuándo ocurren esas acciones Implementa los estándares de metadatos elegidos</p>
<b>Contenido</b>	<p>Documentar los formatos de archivo y otras características de contenido esenciales, incluido cómo y cuándo fueron identificados</p>	<p>Verificar los formatos de archivo y otras características de contenido esenciales</p> <p>Establecer relaciones con los creadores de contenido para fomentar la elección sostenible de archivos</p>	<p>Monitorear la obsolescencia y los cambios en las tecnologías de las que depende el contenido</p>	<p>Realizar migraciones, normalizaciones, emulación y actividades similares que garanticen el acceso al contenido</p>

Nivel	Área Funcional				
	Almacenamiento	Integridad	Control	Metadatos	Contenido
<b>Nivel 1 - (Conocer su contenido)</b>	<p>Tener dos copias completas en ubicaciones separadas</p> <p>Documentar todos los medios de almacenamiento donde este almacenado el contenido</p> <p>Poner el contenido en soportes de almacenamiento estables</p>	<p>Verificar que la información de integridad se ha proporcionado con el contenido</p> <p>Generar información de integridad si esta no ha sido proporcionada con el contenido</p> <p>Se verifica virus en todo el contenido; se aísla el contenido en cuarentena según sea necesario</p>	<p>Se determinan los agentes humanos y de software que deben estar autorizados para leer, escribir, mover y eliminar contenido</p>	<p>Crear un inventario de contenido, documentando también la ubicación de almacenamiento actual de estos</p> <p>Hacer una copia de respaldo del inventario y se almacena al menos una copia por separado</p>	<p>Crear un inventario de contenido, documentando también la ubicación de almacenamiento actual de estos</p> <p>Hacer una copia de respaldo del inventario y se almacena al menos una copia por separado</p>
<b>Nivel 2 - (Proteger su contenido)</b>	<p>Tener tres copias completas con al menos una copia en una ubicación geográfica distinta</p> <p>Documentar el almacenamiento y medios de almacenamiento, indicando los recursos y las dependencias que estos requieren para funcionar</p>	<p>Verificar la información de integridad al mover o copiar contenido</p> <p>Usar bloqueadores de escritura cuando se trabaja con medios originales</p> <p>Hacer una copia de seguridad de la información de integridad y almacenar una copia en una ubicación separada del contenido</p>	<p>Documentar a los agentes humanos y de software autorizados para leer, escribir, mover y eliminar contenido y aplicar estos</p>	<p>Almacenar suficientes metadatos para saber cuál es el contenido (esto podría incluir alguna combinación de aspectos administrativos, técnicos, descriptivos, de preservación y estructurales)</p>	<p>Verificar los formatos de archivo y otras características de contenido esenciales</p> <p>Establecer relaciones con los creadores de contenido para fomentar la elección sostenible de archivos</p>
<b>Nivel 3 - (Controlar su contenido)</b>	<p>Tener al menos una copia en una ubicación geográfica con amenaza de desastre diferente a las otras copias</p> <p>Tener al menos una copia en un medio de almacenamiento de diferente tipo</p> <p>Rastrear la obsolescencia del almacenamiento y los medios</p>	<p>Verificar la información de integridad del contenido en intervalos fijos</p> <p>Documentar los procesos y resultados de verificación de información de integridad</p> <p>Realizar una auditoría de la información de integridad bajo demanda</p>	<p>Mantener los registros (logs) y se identifican a los agentes humanos y de software que realizaron acciones sobre el contenido.</p>	<p>Determinar qué estándares de metadatos aplicar</p> <p>Encuentra y completa los vacíos en sus metadatos para cumplir con esos estándares</p>	<p>Monitorear la obsolescencia y los cambios en las tecnologías de las que depende el contenido</p>
<b>Nivel 4 - (Mantener su contenido)</b>	<p>Tener al menos tres copias en ubicaciones geográficas distintas, cada una con una amenaza de desastre diferente</p> <p>Maximizar la diversificación del almacenamiento para evitar puntos únicos de falla</p> <p>Tener un plan y realizar acciones para abordar la obsolescencia del hardware, software y medios de almacenamiento</p>	<p>Verificar la información de integridad en respuesta a eventos o actividades específicas</p> <p>Reemplazar o reparar el contenido dañado según sea necesario</p>	<p>Se realizan revisiones periódicas de acciones / registros (logs) de acceso</p>	<p>Registrar las acciones de preservación asociadas con el contenido y cuándo ocurren esas acciones</p> <p>Implementa los estándares de metadatos elegidos</p>	<p>Realizar migraciones, normalizaciones, emulación y actividades similares que garanticen el acceso al contenido</p>