AUDITORÍA DE PRESERVACIÓN DIGITAL CON *NDSA LEVELS*

Methodology of digital preservation audits with *NDSA Levels*

Miquel Térmens y David Leija

Miquel Térmens, doctor en Documentación, licenciado en Historia y diplomado en Biblioteconomía y Documentación, es profesor del *Departamento de Biblioteconomía, Documentación y Comunicación Audiovisual* de la *Universidad de Barcelona*. Es especialista en digitalización y en preservación digital de documentos.
http://orcid.org/0000-0002-7305-3424

Universidad de Barcelona
Departamento de Biblioteconomía, Documentación y Comunicación Audiovisual
Melcior de Palau, 140. 08014 Barcelona, España
termens@ub.edu

David Leija es licenciado en Ciencias de la Comunicación por la *Universidad Autónoma de Tamaulipas* (*UAT*) (México). Master en Gestión de Contenidos Digitales por la *Universidad de Barcelona – Universidad Pompeu Fabra* (España). Ha trabajado como periodista y como director de comunicación de publicidad y empresarial. Es profesor de la *Facultad de Arquitectura, Diseño y Urbanismo* de la *UAT*. Ha realizado su tesis doctoral en la *Universidad de Barcelona* sobre los sistemas de preservación digital distribuida y su aplicación a las universidades de México.
http://orcid.org/0000-0001-5782-2767

Universidad Autónoma de Tamaulipas
Facultad de Arquitectura, Diseño y Urbanismo
Centro Universitario Tampico-Madero
Circuito Interior, s/n. 1401 Tampico (Tamaulipas), México
dleija@uat.edu.mx

Resumen

NDSA Levels es una metodología creada por la *National Digital Stewardship Alliance* (*NDSA*), en los Estados Unidos para evaluar el nivel de preservación digital de una determinada institución. Se presentan los resultados de su aplicación en 8 organizaciones públicas y privadas en España, México, Brasil y Suiza. De esta experiencia se concluye que la metodología *NDSA Levels* es de fácil aplicación y que, además de alertar sobre los aspectos aún no implementados, ofrece una guía sobre las acciones técnicas que en el futuro se deberían incluir en un plan de preservación.

Palabras clave

Preservación digital; Planes de preservación; Auditorías; Autoevaluación; Repositorios institucionales; Archivos.

Abstract

NDSA Levels is a methodology created by the *National Digital Stewardship Alliance* (*NDSA*) at the United States to assess the level of digital preservation of a particular institution. Results of its application in 8 public and private organizations in Spain, Mexico, Brazil and Switzerland are presented. From this experience it is concluded that the *NDSA Levels* methodology is easy to apply and that its application besides alerting about the aspects not yet implemented, provides guidance on the technical actions that should be undertaken in the future within a preservation plan.

Keywords

Digital preservation; Preservation planning; Audits; Self-auditing; Institutional repositories; Archives.

Térmens, Miquel; **Leija, David** (2017). "Auditoría de preservación digital con *NDSA Levels*". *El profesional de la información*, v. 26, n. 3, pp. 447-456.

https://doi.org/10.3145/epi.2017.may.11

Artículo recibido el 10-01-2017
Aceptación definitiva: 08-02-2017

1. Introducción

La tecnología digital provee nuevas capacidades antes inimaginables, pero también origina nuevos problemas. Uno de ellos es la dificultad de valorar sencilla y objetivamente la adecuación de las tecnologías usadas. La informática es cada vez más compleja y, salvo en el caso de personal especializado, resulta casi imposible que alguien pueda comprender a fondo el flujo de datos de un determinado software y determinar si su funcionamiento es correcto. Cuando la tecnología se aplica a sistemas diseñados para dar soporte a la preservación de datos digitales a largo plazo, este desconocimiento puede resultar fatal. ¿Cómo podemos confiar en la perdurabilidad futura de la producción digital de nuestro presente si no somos capaces de valorar si los sistemas de preservación digital que usamos son correctos?

El diseño de repositorios de preservación confiables es una de las líneas de investigación más importantes a nivel internacional en preservación digital. Uno de sus objetivos es disponer de metodologías y herramientas para evaluar el grado de cumplimiento de estándares o buenas prácticas aceptadas en un sistema en particular. Una de las metodologías más extendidas para conseguir repositorios confiables son los sistemas de auditoría, realizados por personal experto, que permiten determinar si un repositorio es seguro y, por tanto, si podemos confiar en él.

> Los sistemas de auditoría permiten determinar si un repositorio de preservación es seguro y, por tanto, si podemos confiar en él

La mayoría de las herramientas existentes para evaluar el estado de la preservación digital en una organización están organizadas como sistemas tradicionales de auditoría: analizan un sistema desde fuera para comprobar si sigue de forma adecuada un conjunto de reglas o buenas prácticas establecidas. Este es el caso de la norma *ISO 27000 Gestión de la seguridad de la información*, la más utilizada en auditorías de seguridad informática, que sigue el método PDCA (*plan-do-check-act*) de mejora continua, común a otras normas como *ISO 9000 Gestión de la calidad*, *ISO 5000 Gestión de la energía* o *ISO 14000 Gestión ambiental*.

El principal problema de la norma *ISO 27000* es que está orientada a la valoración de riesgos y sus respectivas salvaguardas en el momento actual, con el fin de asegurar un correcto funcionamiento a corto plazo del sistema en evaluación. Cuando los peligros se encuentran en el futuro, cómo por ejemplo en la obsolescencia de las propias tecnologías informáticas, o cuando el propio servicio está orientado al largo plazo, como en el caso de un repositorio de preservación, la *ISO 27000* deja de ser eficaz, pues no dispone de pruebas que cuestionen la preparación del sistema ante los retos que puede deparar el futuro. Para solucionar estas deficiencias, desde el entorno de los archivos y las bibliotecas han aparecido otros métodos elaborados específicamente para auditar sistemas de preservación (**Dryden**, 2011; **Maemura**; **Moles**; **Becker**, 2015; 2016), entre las que destacan el *Digital preservation capability maturity model* (*Dpcmm*) (**Dollar**; **Ashley**, 2014), *Drambora*, *Nestor* (*Nestor*, 2008; **Dobratz**; **Schoger**, 2007), *TRAC* (*TRAC*, 2007) y la norma *ISO 16363* (*ISO*, 2012).

En general, los métodos de auditoría no sirven para realizar un análisis previo a la implementación de acciones de preservación digital. Por el contrario, están diseñados para testear el buen diseño y funcionamiento de un sistema de preservación ya existente, localizar en el mismo no conformidades respecto a los niveles de calidad exigidos y, como resultado, obligar a sus gestores a establecer medidas correctivas y un plan de mejora. Por definición no se puede auditar un sistema que no existe.

> Muchas organizaciones pequeñas miran con aprensión el uso de auditorías tradicionales porqué son difíciles y caras de aplicar

Otro problema recurrente asociado a las auditorías tradicionales es que resultan complejas de aplicar y conllevan altos costes, al requerir para su aplicación personal experto, normalmente auditores profesionales. Por consiguiente, muchas organizaciones pequeñas muestran una actitud muy reacia a su aplicación o directamente las rechazan.

Existe por tanto un vacío que puede solucionarse con otro tipo de métodos más fáciles de usar, más asequibles y aplicables a organizaciones de distintos tamaños.

2. *NDSA Levels*

En 2010 se fundó la *National Digital Stewardship Alliance* (*NDSA*) en EUA, un consorcio de instituciones comprometidas en la preservación de recursos digitales.
http://ndsa.org

Está formada por más de 160 miembros y sus actividades se centran en la difusión de buenas prácticas y en la mejora de la formación de los profesionales. En esta línea, dentro de *NDSA* se creó un grupo de trabajo con el encargo de crear una metodología que permitiera a las instituciones testear de forma fácil el nivel de desarrollo alcanzado por sus soluciones de preservación digital. El grupo de trabajo estuvo formado, entre otros, por representantes de la *National Archives and Records Administration* (*NARA*), el *Metropolitan New York Library Council* (*Metro*), la *Harvard Library* y la *Library of Congress*. Las propuestas de este grupo se presentaron a lo largo de 2012 en varias reuniones científicas y en ellas incorporaron numerosas aportaciones de expertos en preservación digital. El redactado final de las propuestas se presentó en la conferencia *Archiving 2013*, celebrada en Washington DC en abril de 2013 (*Levels*, 2013; **Phillips** *et al.*, 2013).

El documento de propuestas, conocido como *NDSA Levels*, consiste en una única tabla formada por preguntas sobre 5 campos (tabla 1):

Tabla 1. *NDSA Levels*. Documento de propuestas

	Nivel 1 (Proteja sus datos)	**Nivel 2 (Conozca sus datos)**	**Nivel 3 (Controle sus datos)**	**Nivel 4 (Repare sus datos)**
Almacenamiento y localización geográfica	Dos copias completas que no estén unidas.	Como mínimo tres copias completas.	Como mínimo una copia en una localización geográfica con una amenaza de desastres diferente.	Como mínimo tres copias en localizaciones geográficas con amenazas de desastres diferentes.
	Para datos en soportes heterogéneos (discos ópticos, discos duros, etc.) quitar el contenido del soporte y ponerlo en vuestro sistema de almacenamiento.	Como mínimo una copia en una localización geográfica distinta.	Controle el proceso de obsolescencia de su(s) sistema(s) de almacenamiento y de sus soportes.	Disponga de un plan integral preparado para mantener los ficheros y los metadatos accesibles en los actuales soportes o sistemas.
		Documentar su(s) sistema(s) de almacenamiento y soportes de almacenamiento y lo que usted necesite para usarlos.		
No alteración de ficheros e integridad de los datos	Comprobar la integridad de los ficheros en el momento de la ingesta si sus valores han sido proporcionados junto con el contenido.	Comprobar la integridad de todas las ingestas.	Comprobar la integridad del contenido a intervalos regulares.	Comprobar la integridad de todo el contenido en respuesta a situaciones o actividades específicas.
	Crear la información de integridad si no fue proporcionada junto con el contenido.	Usar dispositivos con escritura bloqueada cuando se trabaje con los soportes originales.	Mantener registros de la información de integridad; realizar auditoría bajo demanda.	Capacidad para reemplazar o reparar datos corrompidos.
		Comprobar virus en contenido de alto riesgo.	Capacidad para detectar datos corrompidos.	Asegúrese de que ninguna persona tiene acceso de escritura a todas las copias.
			Comprobar virus en todo el contenido.	
Seguridad de la información	Identificar quién ha leído, escrito, movido o eliminado la autorización a ficheros concretos.	Documentar las restricciones de acceso de los contenidos.	Mantener registros de quién ha realizado qué acciones con los ficheros, incluyendo acciones de borrado y preservación.	Realizar auditorías de los registros.
	Restringir quién tiene este tipo de autorizaciones a ficheros concretos.			
Metadatos	Inventario del contenido y de su localización en el almacenamiento.	Almacenar metadatos administrativos.	Almacenar metadatos estándar técnicos y descriptivos.	Almacenar metadatos estándar de preservación.
	Asegurar una copia de seguridad separada del inventario.	Almacenar metadatos de las transformaciones y registrar las incidencias.		
Formatos de ficheros	Cuando usted puede participar en la creación de archivos digitales fomente el uso de un conjunto limitado de formatos abiertos y conocidos de ficheros y de *codecs*	Disponer de un inventario de los formatos de ficheros usados.	Monitorear los problemas de obsolescencia de los formatos de ficheros.	Realizar migraciones de formatos, emulaciones o actividades similares si es necesario.

Fuente: *Levels*, 2013

- sistema de almacenamiento y ubicación geográfica de los ficheros;
- alteración de los ficheros e integridad de los datos;
- medidas de seguridad de la información;
- metadatos;
- formatos de los ficheros.

Para cada uno de los 5 campos se presentan tareas a realizar, ordenadas en 4 niveles, desde el nivel más bajo de exigencia, o nivel primario (nivel 1) al nivel más alto, o nivel completo (nivel 4) de preservación digital. La presentación de la tabla *NDSA Levels* es intencionadamente sencilla, fácilmente comprensible por cualquier profesional para evitar el efecto rechazo que provocan muchos sistemas tradicionales de auditoría.

Algunas de las características positivas dignas de mención en la tabla *NDSA Levels* son:

- se centra en actividades, no tanto en técnicas o en equipamiento, como es habitual en preservación digital;
- pregunta sobre aquellas acciones que competen o están al alcance de los profesionales de la información, olvidándose de aquellas otras que dependen de la estructura externa o del entorno como la financiación, la legislación o la propia política estratégica de la institución;
- utiliza un lenguaje claro, que huye de los tecnicismos.

> El principal déficit observado en los repositorios es la falta de suficientes copias de los datos, lo más separadas posible

Como elementos negativos destacan tres:

- algunos puntos favorecen respuestas potencialmente erróneas, como por ejemplo las preguntas sobre los controles de integridad de ficheros. En consecuencia, las respuestas pueden ofrecer una visión más optimista de la que correspondería a la situación real;
- su sencillez aparente puede comportar que algunas personas subestimen vigilar otros aspectos necesarios para alcanzar un buen nivel de preservación. Así olvidarán que la tabla ofrece una visión simplificada de las tareas de preservación y no un listado exhaustivo de las mismas como, por ejemplo, se puede encontrar en *Nestor*, *TRAC* o *ISO 16363*;
- *NDSA Levels* se centra en evaluar cómo trabaja un repositorio, no el conjunto de la organización, y se centra en las capacidades tecnológicas, ignorando otras facetas clave como la robustez institucional o la sostenibilidad económica. Estas carencias han sido señaladas por diversos autores (*DartBlog*, 2016).

Tanto los aspectos positivos como los negativos se han reflejado en los casos de estudio y se comentan en el apartado de resultados.

Como primera observación se puede afirmar que *NDSA Levels* quizá resuelva algunos de los problemas propios de las metodologías previas, pero lo hace a costa de sacrificar algunas de sus virtudes. Si se tiene en cuenta que el objetivo de *NDSA Levels* no es el de sustituir los métodos existentes, es posible manifestar que su aportación es positiva en determinados contextos. Así lo han entendido varias organizaciones, que han usado *NDSA Levels* para evaluar el estado de la preservación digital de sus sistemas como *ARTStor* (**Ying**, 2013) o *Harvard University* (**Goethals**, 2013; *Harvard University*, 2014). Además, se ha hecho una adaptación de *NDSA Levels* para las organizaciones que preservan datos de tipo geográfico (*USGS*, 2014; **Faundeen**, 2014).

3. Metodología

Las preguntas de la tabla *NDSA Levels* están formuladas para ser respondidas afirmativa o negativamente, aunque en algunos apartados puede resultar difícil dar una respuesta categórica. El problema se incrementa en aquellas preguntas cuya aplicación puede suponer la realización de más de una tarea. Aun así, se recomienda cumplimentar la tabla dando respuestas categóricas. Una forma para conseguirlo es marcar con un trazo o con un color especial las respuestas afirmativas en la tabla. Cuando se termina de responder, los resultados se pueden apreciar rápidamente de forma visual.

Otro aspecto relevante para asegurar la calidad del resultado del cuestionario es determinar qué personas lo rellenarán y qué formación han recibido para hacerlo. Aunque como se ha mencionado previamente *NDSA Levels* presenta un lenguaje simple, el personal debe conocer la terminología o los principios técnicos que subyacen a los enunciados de las preguntas para responderlas adecuadamente. En muchos casos será recomendable planificar una formación previa o mecanismos de acompañamiento a los responsables de realizar el cuestionario.

En los casos de estudio las tablas se han respondido usando las siguientes estrategias:

Cumplimentación del cuestionario dentro de una sesión de formación en grupo

Dentro de cursos de formación reglada y no reglada sobre preservación digital, se explicaron los objetivos de la tabla *NDSA* y cómo dar respuesta a los apartados. A continuación, los alumnos de forma individual o en grupo, cumplimentaron los datos correspondientes a las instituciones en las que trabajaban. El trabajo en grupo facilitó la resolución de dudas sobre los apartados de más difícil comprensión. Por el contrario, la necesidad de completar la tabla en una única sesión presencial evidenció que para obtener algunas respuestas era imprescindible preguntar a otros empleados, en especial al personal informático.

Esta estrategia se usó, de forma experimental, en centros de documentación independientes y en una red de bibliotecas especializadas.

Formación previa del personal propio del repositorio

Como evolución de la anterior estrategia se ofreció formación al personal participante sobre el uso de la tabla *NDSA* y se dispuso de un mínimo de dos semanas para cumplimentarla. Con esta estrategia, los responsables pudieron consultar a otras personas implicadas y disponer de más tiempo para reflexionar las respuestas.

Este método se ha utilizado en empresas y fundaciones privadas y en órganos de la administración local y autonómica en Madrid, Cataluña y Baleares.

Entrevista directa con el personal administrador del repositorio

Se trata de la variante más parecida a una auditoría tradicional. Una persona experta mantiene diversas reuniones privadas con el personal responsable de un repositorio, tanto a nivel documental como a nivel informático.

Este método se ha aplicado a los repositorios de dos universidades públicas de Cataluña.

Encuesta a un grupo de instituciones

La tabla se entregó bajo la forma de un cuestionario a un conjunto de instituciones. La finalidad era recoger datos de un gran número de organizaciones y así obtener tanto un retrato de la situación de cada una de ellas como una visión del conjunto de las mismas. Tras una primera inspección de los datos, se resolvieron algunas dudas con los encuestados, y una vez clarificadas las respuestas, éstas se volcaron a una matriz global para su posterior análisis.

Esta estrategia se aplicó a un estudio sobre todo el sistema de educación superior de México, más concretamente sobre el estado actual y las alternativas de preservación digital para los repositorios institucionales de sus universidades.

Dado que los resultados obtenidos en las distintas pruebas son confidenciales y pueden revelar situaciones anómalas en las organizaciones estudiadas, en el presente artículo todos los resultados se presentan de forma anónima. Advertimos que la selección de los casos no pretende ser una muestra, ni siquiera una ilustración del estado de la preservación en un sector o país. Por el contrario, la selección obedece al interés de mostrar situaciones reales dispares que pueden ser detectadas y analizadas gracias a *NDSA Levels*.

> La metodología *NDSA Levels* es fácil de aprender, con una curva de aprendizaje muy baja

4. Resultados

En esta sección se presentan los resultados obtenidos en 8 organizaciones, descritas en la tabla 2. Se han descartado las organizaciones que rellenaron el cuestionario siguiendo la estrategia 1 pues consideramos que los resultados así obtenidos no tienen suficiente validez, al no poder contrastarse con los responsables de sus respectivos sistemas informáticos.

También se describen los problemas detectados por el personal que ha cumplimentado las tablas, y que incluyen algunos problemas operativos y de comprensión recogidos durante su aplicación:

Tabla 2. Organizaciones estudiadas

Caso	Tipo de organización	Método aplicado
1	Archivo de una ciudad capital de provincia. España	2
2	Organismo de administración local. España	2
3	Organismo auditor de una comunidad autónoma. España	2
4	Repositorio de una universidad pública. España	3
5	Repositorio de una universidad pública. México	4
6	Repositorio de una universidad pública. Brasil	2
7	Empresa multinacional del sector servicios. Suiza	2
8	Festival de cine. España	2

- en algunos apartados resulta difícil valorar el grado de cumplimiento y dar una respuesta a la tabla. El usuario tampoco dispone de indicaciones sobre el alcance de los apartados, qué se considera como cumplimiento correcto, etc.; este problema existe también en normas reconocidas de auditoría, en los que las valoraciones no son más claras o explícitas, sino que acaban siendo afinadas por los equipos de auditoría en base a su experiencia;
- dificultades con la terminología: a pesar de que la tabla está expresada de forma clara, persisten problemas de terminología (como ejemplo véanse los términos "dispositivo con escritura bloqueada", "integridad", "ingesta", "datos corrompidos") propia de la especialidad de preservación digital, pero no necesariamente conocida por el personal responsable de los ficheros a preservar;
- el personal no especializado a veces no comprende la razón por la que se pide realizar determinadas acciones;
- la tabla no está preparada para una entrada automatizada de los resultados. Debido a ello resulta difícil elaborar índices de cumplimiento que permitan una comparación cuantitativa de los resultados de distintas organizaciones.

A continuación, se muestran los resultados de los ocho casos estudiados, agrupados por su naturaleza, según sean administración pública, centros universitarios u organismos privados.

> *NDSA Levels* permite la evaluación (auditoría) y la elaboración de un plan de mejora a partir de las carencias detectadas

Los organismos de las administraciones públicas incluidos en el estudio presentan una gran diversidad en cuanto a atribuciones, recursos y nivel de desarrollo. Lo mismo ocurre con los respectivos archivos digitales, como pone en evidencia la figura 2. En el caso 1 se observa cómo un gran archivo municipal aún no ha asumido las obligaciones técnicas que le impone la administración electrónica o, como

	Nivel 1 (Proteja sus datos)	Nivel 2 (Conozca sus datos)	Nivel 3 (Controle sus datos)	Nivel 4 (Repare sus datos)
Almacenamiento y localización geográfica	Dos copias completas que no estén unidas.	Como mínimo tres copias completas.	Como mínimo una copia en una localización geográfica con una amenaza de desastres diferente.	Como mínimo tres copias en localizaciones geográficas con amenazas de desastres diferentes.
	Para datos en soportes heterogéneos (discos ópticos, discos duros, etc.) quitar el contenido del soporte y ponerlo en vuestro sistema de almacenamiento.	Como mínimo una copia en una localización geográfica distinta.	Controle el proceso de obsolescencia de su(s) sistema(s) de almacenamiento y de sus soportes.	Disponga de un plan integral preparado para mantener los ficheros y los metadatos accesibles en los actuales soportes o sistemas.
		Documentar su(s) sistema(s) de almacenamiento y soportes de almacenamiento y lo que usted necesite para usarlos.		
No alteración de ficheros e integridad de los datos	Comprobar la integridad de los ficheros en el momento de la ingesta si sus valores han sido proporcionados junto con el contenido.	Comprobar la integridad de todas las ingestas.	Comprobar la integridad del contenido a intervalos regulares.	Comprobar la integridad de todo el contenido en respuesta a situaciones o actividades específicas.
	Crear la información de integridad si no fue proporcionada junto con el contenido.	Usar dispositivos con escritura bloqueada cuando se trabaje con los soportes originales.	Mantener registros de la información de integridad; realizar auditoría bajo demanda.	Capacidad para reemplazar o reparar datos corrompidos.
		Comprobar virus en contenido de alto riesgo.	Capacidad para detectar datos corrompidos.	Asegúrese de que ninguna persona tiene acceso de escritura a todas las copias.
			Comprobar virus en todo el contenido.	
Seguridad de la información	Identificar quién ha leído, escrito, movido o eliminado la autorización a ficheros concretos.	Documentar las restricciones de acceso de los contenidos.	Mantener registros de quién ha realizado qué acciones con los ficheros, incluyendo acciones de borrado y preservación.	Realizar auditorías de los registros.
	Restringir quién tiene este tipo de autorizaciones a ficheros concretos.			
Metadatos	Inventario del contenido y de su localización en el almacenamiento.	Almacenar metadatos administrativos.	Almacenar metadatos estándar técnicos y descriptivos.	Almacenar metadatos estándar de preservación.
	Asegurar una copia de seguridad separada del inventario.	Almacenar metadatos de las transformaciones y registrar las incidencias.		
Formatos de ficheros	Cuando usted puede participar en la creación de archivos digitales fomente el uso de un conjunto limitado de formatos abiertos y conocidos de ficheros y de *codecs*	Disponer de un inventario de los formatos de ficheros usados.	Monitorear los problemas de obsolescencia de los formatos de ficheros.	Realizar migraciones de formatos, emulaciones o actividades similares si es necesario.

Caso 1

	Nivel 1 (Proteja sus datos)	Nivel 2 (Conozca sus datos)	Nivel 3 (Controle sus datos)	Nivel 4 (Repare sus datos)
Almacenamiento y localización geográfica	Dos copias completas que no estén unidas.	Como mínimo tres copias completas.	Como mínimo una copia en una localización geográfica con una amenaza de desastres diferente.	Como mínimo tres copias en localizaciones geográficas con amenazas de desastres diferentes.
	Para datos en soportes heterogéneos (discos ópticos, discos duros, etc.) quitar el contenido del soporte y ponerlo en vuestro sistema de almacenamiento.	Como mínimo una copia en una localización geográfica distinta.	Controle el proceso de obsolescencia de su(s) sistema(s) de almacenamiento y de sus soportes.	Disponga de un plan integral preparado para mantener los ficheros y los metadatos accesibles en los actuales soportes o sistemas.
		Documentar su(s) sistema(s) de almacenamiento y soportes de almacenamiento y lo que usted necesite para usarlos.		
No alteración de ficheros e integridad de los datos	Comprobar la integridad de los ficheros en el momento de la ingesta si sus valores han sido proporcionados junto con el contenido.	Comprobar la integridad de todas las ingestas.	Comprobar la integridad del contenido a intervalos regulares.	Comprobar la integridad de todo el contenido en respuesta a situaciones o actividades específicas.
	Crear la información de integridad si no fue proporcionada junto con el contenido.	Usar dispositivos con escritura bloqueada cuando se trabaje con los soportes originales.	Mantener registros de la información de integridad; realizar auditoría bajo demanda.	Capacidad para reemplazar o reparar datos corrompidos.
		Comprobar virus en contenido de alto riesgo.	Capacidad para detectar datos corrompidos.	Asegúrese de que ninguna persona tiene acceso de escritura a todas las copias.
			Comprobar virus en todo el contenido.	
Seguridad de la información	Identificar quién ha leído, escrito, movido o eliminado la autorización a ficheros concretos.	Documentar las restricciones de acceso de los contenidos.	Mantener registros de quién ha realizado qué acciones con los ficheros, incluyendo acciones de borrado y preservación.	Realizar auditorías de los registros.
	Restringir quién tiene este tipo de autorizaciones a ficheros concretos.			
Metadatos	Inventario del contenido y de su localización en el almacenamiento.	Almacenar metadatos administrativos.	Almacenar metadatos estándar técnicos y descriptivos.	Almacenar metadatos estándar de preservación.
	Asegurar una copia de seguridad separada del inventario.	Almacenar metadatos de las transformaciones y registrar las incidencias.		
Formatos de ficheros	Cuando usted puede participar en la creación de archivos digitales fomente el uso de un conjunto limitado de formatos abiertos y conocidos de ficheros y de *codecs*	Disponer de un inventario de los formatos de ficheros usados.	Monitorear los problemas de obsolescencia de los formatos de ficheros.	Realizar migraciones de formatos, emulaciones o actividades similares si es necesario.

Caso 2

	Nivel 1 (Proteja sus datos)	Nivel 2 (Conozca sus datos)	Nivel 3 (Controle sus datos)	Nivel 4 (Repare sus datos)
Almacenamiento y localización geográfica	Dos copias completas que no estén unidas.	Como mínimo tres copias completas.	Como mínimo una copia en una localización geográfica con una amenaza de desastres diferente.	Como mínimo tres copias en localizaciones geográficas con amenazas de desastres diferentes.
	Para datos en soportes heterogéneos (discos ópticos, discos duros, etc.) quitar el contenido del soporte y ponerlo en vuestro sistema de almacenamiento.	Como mínimo una copia en una localización geográfica distinta.	Controle el proceso de obsolescencia de su(s) sistema(s) de almacenamiento y de sus soportes.	Disponga de un plan integral preparado para mantener los ficheros y los metadatos accesibles en los actuales soportes o sistemas.
		Documentar su(s) sistema(s) de almacenamiento y soportes de almacenamiento y lo que usted necesite para usarlos.		
No alteración de ficheros e integridad de los datos	Comprobar la integridad de los ficheros en el momento de la ingesta si sus valores han sido proporcionados junto con el contenido.	Comprobar la integridad de todas las ingestas.	Comprobar la integridad del contenido a intervalos regulares.	Comprobar la integridad de todo el contenido en respuesta a situaciones o actividades específicas.
	Crear la información de integridad si no fue proporcionada junto con el contenido.	Usar dispositivos con escritura bloqueada cuando se trabaje con los soportes originales.	Mantener registros de la información de integridad; realizar auditoría bajo demanda.	Capacidad para reemplazar o reparar datos corrompidos.
		Comprobar virus en contenido de alto riesgo.	Capacidad para detectar datos corrompidos.	Asegúrese de que ninguna persona tiene acceso de escritura a todas las copias.
			Comprobar virus en todo el contenido.	
Seguridad de la información	Identificar quién ha leído, escrito, movido o eliminado la autorización a ficheros concretos.	Documentar las restricciones de acceso de los contenidos.	Mantener registros de quién ha realizado qué acciones con los ficheros, incluyendo acciones de borrado y preservación.	Realizar auditorías de los registros.
	Restringir quién tiene este tipo de autorizaciones a ficheros concretos.			
Metadatos	Inventario del contenido y de su localización en el almacenamiento.	Almacenar metadatos administrativos.	Almacenar metadatos estándar técnicos y descriptivos.	Almacenar metadatos estándar de preservación.
	Asegurar una copia de seguridad separada del inventario.	Almacenar metadatos de las transformaciones y registrar las incidencias.		
Formatos de ficheros	Cuando usted puede participar en la creación de archivos digitales fomente el uso de un conjunto limitado de formatos abiertos y conocidos de ficheros y de *codecs*	Disponer de un inventario de los formatos de ficheros usados.	Monitorear los problemas de obsolescencia de los formatos de ficheros.	Realizar migraciones de formatos, emulaciones o actividades similares si es necesario.

Caso 3

Figura 1. Casos administración pública (1, 2, 3)

mínimo, aún no ha iniciado el despliegue de las actividades necesarias para preservar a largo plazo los nuevos registros electrónicos, pues en los resultados se puede apreciar que sólo dispone de dos copias de los datos y únicamente de la capacidad de testear la presencia de virus informáticos.

El caso 2 corresponde también a una administración local que, por el contrario, está mucho más avanzada a nivel técnico. Esta organización dispone de hasta tres copias de sus datos y ha desarrollado más allá del nivel básico todos los apartados de preservación. Como aspecto negativo, cabe destacar la deficiente atención prestada a los metadatos, pero este hecho puede deberse a las características propias de sus documentos.

El caso 3 es singular, pues se trata de un organismo con funciones de auditoría y control sobre otras entidades de la administración pública. Por ello no es de extrañar que tengan un nivel medio en almacenamiento y que alcancen la excelencia en seguridad y control de acceso a los documentos. Dado el contexto de este ejemplo puede resultar comprensible su indiferencia ante los formatos de los ficheros pues, al fin y al cabo, los reciben de otras administraciones o los crean ellos mismos. Sin embargo, resulta un gran problema que no presten ninguna atención al control de la integridad de los ficheros, pues dicha integridad es un primer paso para certificar la validez de los actos jurídicos recogidos en los ficheros custodiados.

	Nivel 1 (Proteja sus datos)	Nivel 2 (Conozca sus datos)	Nivel 3 (Controle sus datos)	Nivel 4 (Repare sus datos)
Almacenamiento y localización geográfica	Dos copias completas que no estén unidas.	Como mínimo tres copias completas.	Como mínimo una copia en una localización geográfica con una amenaza de desastres diferente.	Como mínimo tres copias en localizaciones geográficas con amenazas de desastres diferentes.
	Para datos en soportes heterogéneos (discos ópticos, discos duros, etc.) quitar el contenido del soporte y ponerlo en vuestro sistema de almacenamiento.	Como mínimo una copia en una localización geográfica distinta.	Controle el proceso de obsolescencia de su(s) sistema(s) de almacenamiento y de sus soportes.	Disponga de un plan integral preparado para mantener los ficheros y los metadatos accesibles en los actuales soportes o sistemas.
		Documentar su(s) sistema(s) de almacenamiento y soportes de almacenamiento y lo que usted necesite para usarlos.		
No alteración de ficheros e integridad de los datos	Comprobar la integridad de los ficheros en el momento de la ingesta si sus valores han sido proporcionados junto con el contenido.	Comprobar la integridad de todas las ingestas.	Comprobar la integridad del contenido a intervalos regulares.	Comprobar la integridad de todo el contenido en respuesta a situaciones o actividades específicas.
	Crear la información de integridad si no fue proporcionada junto con el contenido.	Usar dispositivos con escritura bloqueada cuando se trabaje con los soportes originales.	Mantener registros de la información de integridad; realizar auditoría bajo demanda.	Capacidad para reemplazar o reparar datos corrompidos.
		Comprobar virus en contenido de alto riesgo.	Capacidad para detectar datos corrompidos.	Asegúrese de que ninguna persona tiene acceso de escritura a todas las copias.
			Comprobar virus en todo el contenido.	
Seguridad de la información	Identificar quién ha leído, escrito, movido o eliminado la autorización a ficheros concretos.	Documentar las restricciones de acceso de los contenidos.	Mantener registros de quién ha realizado qué acciones con los ficheros, incluyendo acciones de borrado y preservación.	Realizar auditorías de los registros.
	Restringir quién tiene este tipo de autorizaciones a ficheros concretos.			
Metadatos	Inventario del contenido y de su localización en el almacenamiento.	Almacenar metadatos administrativos.	Almacenar metadatos estándar técnicos y descriptivos.	Almacenar metadatos estándar de preservación.
	Asegurar una copia de seguridad separada del inventario.	Almacenar metadatos de las transformaciones y registrar las incidencias.		
Formatos de ficheros	Cuando usted puede participar en la creación de archivos digitales fomente el uso de un conjunto limitado de formatos abiertos y conocidos de ficheros y de *codecs*	Disponer de un inventario de los formatos de ficheros usados.	Monitorear los problemas de obsolescencia de los formatos de ficheros.	Realizar migraciones de formatos, emulaciones o actividades similares si es necesario.

Caso 4

	Nivel 1 (Proteja sus datos)	Nivel 2 (Conozca sus datos)	Nivel 3 (Controle sus datos)	Nivel 4 (Repare sus datos)
Almacenamiento y localización geográfica	Dos copias completas que no estén unidas.	Como mínimo tres copias completas.	Como mínimo una copia en una localización geográfica con una amenaza de desastres diferente.	Como mínimo tres copias en localizaciones geográficas con amenazas de desastres diferentes.
	Para datos en soportes heterogéneos (discos ópticos, discos duros, etc.) quitar el contenido del soporte y ponerlo en vuestro sistema de almacenamiento.	Como mínimo una copia en una localización geográfica distinta.	Controle el proceso de obsolescencia de su(s) sistema(s) de almacenamiento y de sus soportes.	Disponga de un plan integral preparado para mantener los ficheros y los metadatos accesibles en los actuales soportes o sistemas.
		Documentar su(s) sistema(s) de almacenamiento y soportes de almacenamiento y lo que usted necesite para usarlos.		
No alteración de ficheros e integridad de los datos	Comprobar la integridad de los ficheros en el momento de la ingesta si sus valores han sido proporcionados junto con el contenido.	Comprobar la integridad de todas las ingestas.	Comprobar la integridad del contenido a intervalos regulares.	Comprobar la integridad de todo el contenido en respuesta a situaciones o actividades específicas.
	Crear la información de integridad si no fue proporcionada junto con el contenido.	Usar dispositivos con escritura bloqueada cuando se trabaje con los soportes originales.	Mantener registros de la información de integridad; realizar auditoría bajo demanda.	Capacidad para reemplazar o reparar datos corrompidos.
		Comprobar virus en contenido de alto riesgo.	Capacidad para detectar datos corrompidos.	Asegúrese de que ninguna persona tiene acceso de escritura a todas las copias.
			Comprobar virus en todo el contenido.	
Seguridad de la información	Identificar quién ha leído, escrito, movido o eliminado la autorización a ficheros concretos.	Documentar las restricciones de acceso de los contenidos.	Mantener registros de quién ha realizado qué acciones con los ficheros, incluyendo acciones de borrado y preservación.	Realizar auditorías de los registros.
	Restringir quién tiene este tipo de autorizaciones a ficheros concretos.			
Metadatos	Inventario del contenido y de su localización en el almacenamiento.	Almacenar metadatos administrativos.	Almacenar metadatos estándar técnicos y descriptivos.	Almacenar metadatos estándar de preservación.
	Asegurar una copia de seguridad separada del inventario.	Almacenar metadatos de las transformaciones y registrar las incidencias.		
Formatos de ficheros	Cuando usted puede participar en la creación de archivos digitales fomente el uso de un conjunto limitado de formatos abiertos y conocidos de ficheros y de *codecs*	Disponer de un inventario de los formatos de ficheros usados.	Monitorear los problemas de obsolescencia de los formatos de ficheros.	Realizar migraciones de formatos, emulaciones o actividades similares si es necesario.

Caso 5

Respecto a los centros universitarios, en la figura 2 se muestran las acciones de preservación digital que se aplican a los repositorios institucionales de tres universidades de titularidad pública de España, México y Brasil respectivamente.

El caso 4 corresponde a una gran universidad con un repositorio y un plan de preservación maduros. A primera vista se detecta un único aspecto deficitario en el número y la ubicación de las copias de ficheros, pues esta institución dispone únicamente de dos copias, y además las almacena en sus propias dependencias. Tras preguntar a los responsables por este problema, no acorde al nivel de buenas prácticas reflejado en los demás puntos del cuestionario, se descubre que este mal funcionamiento se debe a las restricciones presupuestarias sufridas durante la reciente crisis económica.

Los resultados del caso 5 muestran una situación muy grave, pues la universidad no dispone siquiera de dos copias de sus datos, funciona con una copia única. Aunque en este centro algunas preguntas de niveles avanzados se respondan afirmativamente ello no conlleva una buena planificación de preservación si al mismo tiempo quedan en blanco apartados básicos como los del primer y segundo nivel.

El caso 6 muestra una institución que ha avanzado de forma razonable en algunos aspectos como almacenamiento, seguridad y metadatos, pero ha descuidado otros como el control de la integridad de los ficheros.

	Nivel 1 (Proteja sus datos)	Nivel 2 (Conozca sus datos)	Nivel 3 (Controle sus datos)	Nivel 4 (Repare sus datos)
Almacenamiento y localización geográfica	Dos copias completas que no estén unidas.	Como mínimo tres copias completas.	Como mínimo una copia en una localización geográfica con una amenaza de desastres diferente.	Como mínimo tres copias en localizaciones geográficas con amenazas de desastres diferentes.
	Para datos en soportes heterogéneos (discos ópticos, discos duros, etc.) quitar el contenido del soporte y ponerlo en vuestro sistema de almacenamiento.	Como mínimo una copia en una localización geográfica distinta.	Controle el proceso de obsolescencia de su(s) sistema(s) de almacenamiento y de sus soportes.	Disponga de un plan integral preparado para mantener los ficheros y los metadatos accesibles en los actuales soportes o sistemas.
		Documentar su(s) sistema(s) de almacenamiento y soportes de almacenamiento y lo que usted necesite para usarlos.		
No alteración de ficheros e integridad de los datos	Comprobar la integridad de los ficheros en el momento de la ingesta si sus valores han sido proporcionados junto con el contenido.	Comprobar la integridad de todas las ingestas.	Comprobar la integridad del contenido a intervalos regulares.	Comprobar la integridad de todo el contenido en respuesta a situaciones o actividades específicas.
	Crear la información de integridad si no fue proporcionada junto con el contenido.	Usar dispositivos con escritura bloqueada cuando se trabaje con los soportes originales.	Mantener registros de la información de integridad; realizar auditoría bajo demanda.	Capacidad para reemplazar o reparar datos corrompidos.
		Comprobar virus en contenido de alto riesgo.	Capacidad para detectar datos corrompidos.	Asegúrese de que ninguna persona tiene acceso de escritura a todas las copias.
			Comprobar virus en todo el contenido.	
Seguridad de la información	Identificar quién ha leído, escrito, movido o eliminado la autorización a ficheros concretos.	Documentar las restricciones de acceso de los contenidos.	Mantener registros de quién ha realizado qué acciones con los ficheros, incluyendo acciones de borrado y preservación.	Realizar auditorías de los registros.
	Restringir quién tiene este tipo de autorizaciones a ficheros concretos.			
Metadatos	Inventario del contenido y de su localización en el almacenamiento.	Almacenar metadatos administrativos.	Almacenar metadatos estándar técnicos y descriptivos.	Almacenar metadatos estándar de preservación.
	Asegurar una copia de seguridad separada del inventario.	Almacenar metadatos de las transformaciones y registrar las incidencias.		
Formatos de ficheros	Cuando usted puede participar en la creación de archivos digitales fomente el uso de un conjunto limitado de formatos abiertos y conocidos de ficheros y de *codecs*	Disponer de un inventario de los formatos de ficheros usados.	Monitorear los problemas de obsolescencia de los formatos de ficheros.	Realizar migraciones de formatos, emulaciones o actividades similares si es necesario.

Caso 6

Figura 2. Casos correspondientes a repositorios ubicados en centros universitarios (4, 5, 6)

El tercer grupo de casos (figura 3) presenta dos ejemplos extremos dentro de la gran diversidad del mundo privado.

El caso 7 corresponde a una pequeña multinacional suiza, del sector publicitario, con sólo 200 empleados pero que opera en más de 30 países a través de delegaciones. Dado que su operativa es en red y que los datos son una de las bases de su negocio, esta empresa da una extraordinaria importancia a la seguridad de los datos. Es el único ejemplo analizado que dispone de un mínimo de tres copias, en tres ubicaciones geográficas distintas, con el coste y complejidad técnica que conllevan. Otros aspectos del cuestionario son también un claro indicador del interés en tener controlados los accesos, los metadatos y los formatos de los ficheros.

El caso 8 describe una fundación privada encargada de la organización de un festival de cine. Para esta fundación mantener la memoria del festival y de su trayectoria es muy relevante pues le facilitará su supervivencia y en ella se basa su prestigio a nivel nacional e internacional. Desgraciadamente, los resultados del cuestionario muestran pocos procesos que permitan asegurar la permanencia de su patrimonio digital. Esta organización es un ejemplo paradigmático de organización del sector cultural con más voluntarismo que medios materiales o conocimientos técnicos.

5. Discusión

En el artículo se han mostrado los resultados obtenidos de 8 instituciones que pretenden ejemplificar la aplicación del cuestionario *NDSA Levels*. Antes de comentar estos resultados resulta interesante mostrar también cuáles deberían ser los resultados ideales, esperables en una organización altamente comprometida con la misión de preservación digital.

NDSA Levels no establece ninguna priorización entre los 5 apartados en que divide las actuaciones analizadas, sino que por el contrario los considera todos igualmente importantes. Ahora bien, en cada uno de estos apartados sí que establece cuatro niveles sucesivos de cumplimiento. Se entiende, por tanto, que una organización ideal atendería de forma armónica los 5 apartados e iría aumentando su cumplimiento desde el nivel inferior hasta alcanzar el cuarto nivel. Concretamente, sería deseable que una organización cumpliera, como mínimo, el primer nivel de todos los apartados y que el cumplimiento de niveles superiores fuera progresivo. Por ejemplo, que una organización cumpla un nivel 4 sin cumplir el nivel 2 y el nivel 3 posiblemente es un indicador de que no sabe priorizar la puesta en marcha de sus actividades o que no entiende la importancia de acciones previas aparentemente simples.

Si se analizan los casos presentados, se puede observar cómo las organizaciones con mayor nivel de cumplimiento (2, 4, 7) también son las que tienen un cumplimiento más armónico, casi sin faltas en el primer y segundo niveles. Por el contrario, las organizaciones con un menor nivel de cumplimiento global (1, 6, 8) también son las que presentan más vacíos en los primeros niveles.

En una evaluación global se percibe que hay unos determi-

	Nivel 1 (Proteja sus datos)	Nivel 2 (Conozca sus datos)	Nivel 3 (Controle sus datos)	Nivel 4 (Repare sus datos)
Almacenamiento y localización geográfica	Dos copias completas que no estén unidas.	Como mínimo tres copias completas.	Como mínimo una copia en una localización geográfica con una amenaza de desastres diferente.	Como mínimo tres copias en localizaciones geográficas con amenazas de desastres diferentes.
	Para datos en soportes heterogéneos (discos ópticos, discos duros, etc.) quitar el contenido del soporte y ponerlo en vuestro sistema de almacenamiento.	Como mínimo una copia en una localización geográfica distinta.	Controle el proceso de obsolescencia de su(s) sistema(s) de almacenamiento y de sus soportes.	Disponga de un plan integral preparado para mantener los ficheros y los metadatos accesibles en los actuales soportes o sistemas.
		Documentar su(s) sistema(s) de almacenamiento y soportes de almacenamiento y lo que usted necesite para usarlos.		
No alteración de ficheros e integridad de los datos	Comprobar la integridad de los ficheros en el momento de la ingesta si sus valores han sido proporcionados junto con el contenido.	Comprobar la integridad de todas las ingestas.	Comprobar la integridad del contenido a intervalos regulares.	Comprobar la integridad de todo el contenido en respuesta a situaciones o actividades específicas.
	Crear la información de integridad si no fue proporcionada junto con el contenido.	Usar dispositivos con escritura bloqueada cuando se trabaje con los soportes originales.	Mantener registros de la información de integridad; realizar auditoría bajo demanda.	Capacidad para reemplazar o reparar datos corrompidos.
		Comprobar virus en contenido de alto riesgo.	Capacidad para detectar datos corrompidos.	Asegúrese de que ninguna persona tiene acceso de escritura a todas las copias.
			Comprobar virus en todo el contenido.	
Seguridad de la información	Identificar quién ha leído, escrito, movido o eliminado la autorización a ficheros concretos.	Documentar las restricciones de acceso de los contenidos.	Mantener registros de quién ha realizado qué acciones con los ficheros, incluyendo acciones de borrado y preservación.	Realizar auditorías de los registros.
	Restringir quién tiene este tipo de autorizaciones a ficheros concretos.			
Metadatos	Inventario del contenido y de su localización en el almacenamiento.	Almacenar metadatos administrativos.	Almacenar metadatos estándar técnicos y descriptivos.	Almacenar metadatos estándar de preservación.
	Asegurar una copia de seguridad separada del inventario.	Almacenar metadatos de las transformaciones y registrar las incidencias.		
Formatos de ficheros	Cuando usted puede participar en la creación de archivos digitales fomente el uso de un conjunto limitado de formatos abiertos y conocidos de ficheros y de *codecs*	Disponer de un inventario de los formatos de ficheros usados.	Monitorear los problemas de obsolescencia de los formatos de ficheros.	Realizar migraciones de formatos, emulaciones o actividades similares si es necesario.

Caso 7

	Nivel 1 (Proteja sus datos)	Nivel 2 (Conozca sus datos)	Nivel 3 (Controle sus datos)	Nivel 4 (Repare sus datos)
Almacenamiento y localización geográfica	Dos copias completas que no estén unidas.	Como mínimo tres copias completas.	Como mínimo una copia en una localización geográfica con una amenaza de desastres diferente.	Como mínimo tres copias en localizaciones geográficas con amenazas de desastres diferentes.
	Para datos en soportes heterogéneos (discos ópticos, discos duros, etc.) quitar el contenido del soporte y ponerlo en vuestro sistema de almacenamiento.	Como mínimo una copia en una localización geográfica distinta.	Controle el proceso de obsolescencia de su(s) sistema(s) de almacenamiento y de sus soportes.	Disponga de un plan integral preparado para mantener los ficheros y los metadatos accesibles en los actuales soportes o sistemas.
		Documentar su(s) sistema(s) de almacenamiento y soportes de almacenamiento y lo que usted necesite para usarlos.		
No alteración de ficheros e integridad de los datos	Comprobar la integridad de los ficheros en el momento de la ingesta si sus valores han sido proporcionados junto con el contenido.	Comprobar la integridad de todas las ingestas.	Comprobar la integridad del contenido a intervalos regulares.	Comprobar la integridad de todo el contenido en respuesta a situaciones o actividades específicas.
	Crear la información de integridad si no fue proporcionada junto con el contenido.	Usar dispositivos con escritura bloqueada cuando se trabaje con los soportes originales.	Mantener registros de la información de integridad; realizar auditoría bajo demanda.	Capacidad para reemplazar o reparar datos corrompidos.
		Comprobar virus en contenido de alto riesgo.	Capacidad para detectar datos corrompidos.	Asegúrese de que ninguna persona tiene acceso de escritura a todas las copias.
			Comprobar virus en todo el contenido.	
Seguridad de la información	Identificar quién ha leído, escrito, movido o eliminado la autorización a ficheros concretos.	Documentar las restricciones de acceso de los contenidos.	Mantener registros de quién ha realizado qué acciones con los ficheros, incluyendo acciones de borrado y preservación.	Realizar auditorías de los registros.
	Restringir quién tiene este tipo de autorizaciones a ficheros concretos.			
Metadatos	Inventario del contenido y de su localización en el almacenamiento.	Almacenar metadatos administrativos.	Almacenar metadatos estándar técnicos y descriptivos.	Almacenar metadatos estándar de preservación.
	Asegurar una copia de seguridad separada del inventario.	Almacenar metadatos de las transformaciones y registrar las incidencias.		
Formatos de ficheros	Cuando usted puede participar en la creación de archivos digitales fomente el uso de un conjunto limitado de formatos abiertos y conocidos de ficheros y de *codecs*	Disponer de un inventario de los formatos de ficheros usados.	Monitorear los problemas de obsolescencia de los formatos de ficheros.	Realizar migraciones de formatos, emulaciones o actividades similares si es necesario.

Caso 8

Figura 3. Casos sector privado (7, 8)

nados déficits muy comunes, que se repiten en las diversas organizaciones estudiadas:

- inexistencia de suficientes copias ubicadas en distintos emplazamientos;
- desconocimiento de cómo controlar la integridad de los ficheros;
- ausencia de sistemas que permitan realizar auditorías de registros de seguridad;
- ignorancia del papel de los metadatos;
- falta de políticas para controlar la obsolescencia de los formatos y preparar una solución a la misma.

Un análisis más detallado lleva a cuestionar la fiabilidad de algunas de las respuestas recogidas. El ejemplo más evidente de una posible malinterpretación de las preguntas lo encontramos en las respuestas acerca de la comprobación de la integridad de los ficheros. Resulta curioso que este proceso, que requiere ciertos conocimientos técnicos y que como se ha mostrado no se aplica en la mayoría de instituciones, aparentemente se esté aplicando correctamente en las organizaciones 4 y 5 cuando, especialmente el caso 5 muestra resultados poco equilibrados. Por ello se ha hecho una observación más detallada de los procedimientos concretos de trabajo que se aplican en la ingesta de ficheros en muchos repositorios institucionales: la gran mayoría de ficheros ingresados en estos repositorios proceden de proyectos de digitalización y suelen ir acompañados de sus valores *hash* generados por la empresa o la unidad de digitalización. Tanto el fichero del documento como sus valores *hash* (MD5 y SHA-1 son los más habituales) se ingresan en los sistemas de preservación, pero demasiado a menudo sin comprobar de nuevo el *hash* con lo que no puede asegurarse que el fichero ingresado es integro, que no ha sufrido ninguna alteración desde su producción.

Este ejemplo, y otros detectados durante el estudio nos alertan sobre la brecha existente entre:

a) disponer de la capacidad técnica u organizativa para efectuar un determinado control;

b) ejercer esta capacidad como una actividad regular.

De esta manera, los controles de la integridad de ficheros, el chequeo de la existencia de virus o la monitorización de las acciones de acceso a los ficheros u otras acciones de validación no siempre se aplican de forma sistemática, con lo que pierden buena parte de su razón de ser. Desgraciadamente, en algunas de las estrategias expuestas para responder la tabla *NDSA Levels*, estas disfunciones son difíciles de detectar.

Cabe recordar que cualquier método de autoevaluación tiene su mayor debilidad en la credibilidad de las informaciones aportadas, pues a menudo ni se exige ni se comprueba que exista una evidencia de su veracidad. Lo contrario ocurre con los sistemas de evaluación externa, que realizan una comprobación sistemática de cada evidencia (**Ross**; **McHugh**, 2006).

6. Conclusiones

NDSA Levels es una metodología con una curva de aprendizaje muy baja. Resulta fácil de aplicar por personal con conocimientos técnicos medios y no requiere disponer de profesionales especializados en auditorías. Permite encarar problemas técnicos por parte de personal no especializado y resulta comprensible por técnicos de distinta procedencia profesional. En este sentido facilita que la discusión sobre el cumplimiento de las buenas prácticas de preservación se aleje de normas y técnicas concretas y se eleve al plano superior de resultados y objetivos.

En definitiva, se trata de una metodología rápida y barata, que puede ser aplicada en organizaciones muy distintas: repositorios institucionales de universidades, centros de documentación aislados, unidades administrativas de organismos públicos, etc.

En cuanto a los resultados que permite obtener, cabe destacar que no sólo identifica los puntos pendientes, sino que también indica cuáles deben implementarse en primer lugar. En este sentido, supone una vía muy rápida para elaborar un plan de actuación, un plan de mejora o incluso un plan estratégico. Por tanto, se trata de un sistema de evaluación (auditoría) y de planificación al mismo tiempo muy similar en este aspecto a *Dpcmm* (**Dollar**; **Ashley**, 2014).

La experiencia práctica de los autores en su uso, en especial en dinámicas de grupo, les ha permitido observar que la tabla *NDSA Levels* se convierte en un instrumento útil para aprender conceptos de preservación digital y para entender cómo estos conceptos encajan entre ellos. Este atributo de *NDSA Levels* resulta especialmente interesante para la implicación y la mejora en el desempeño de profesionales no especialistas de la preservación digital pero que tienen algún tipo de responsabilidad o rol en la gestión del ciclo de vida de los objetos digitales.

Por último, se ha comprobado que, gracias a su simplicidad, *NDSA Levels* permite comparar con facilidad el estado de la preservación digital en distintas organizaciones, al menos a nivel técnico. Los ocho casos descritos se pueden considerar como una muestra de la gran variabilidad en que se encuentra la preservación digital en las organizaciones. En todos los casos estudiados existe la obligación o necesidad de preservar información y sin embargo el nivel de actuación observado ha sido realmente dispar.

7. Agradecimientos

Esta investigación se ha realizado dentro del proyecto *El acceso abierto a la ciencia en España: evaluación de su impacto en el sistema de comunicación científica* (Plan Nacional, ref. CSO2014-52830-P). También ha recibido soporte del GRC *Cultura i continguts digitals: aspectes documentals, polítics i econòmics*.

8. Bibliografía

DartBlog (2016). "Self-assessment as digital preservation training aid". *DartBlog*, 18 April.
https://dart.blogs.ulcc.ac.uk/2016/04/18/self-assessment-training-aid-dptp

Dobratz, Susanne; **Schoger, Astrid** (2007). "Trustworthy digital long-term repositories: The Nestor approach in the context of international developments". *Lecture notes in computer science*, v. 4675, pp. 210-222.
http://link.springer.com/chapter/10.1007/978-3-540-74851-9_18

Dollar, Charles M.; **Ashley, Lori** (2014). *Assessing digital preservation capability using a maturity model process improvement approach*.
http://www.securelyrooted.com/s/DPCMM-White-Paper_Revised-April-2014.pdf

Dryden, Jean (2011). "Measuring trust: Standards for trusted digital repositories". *Journal of archival organization*, v. 9, n. 2, pp. 127-130.
https://goo.gl/OcVJvh
http://dx.doi.org/10.1080/15332748.2011.590744

Faundeen, John (2014). "Building trust: *NDSA Levels* of digital preservation". En: *Digital preservation* (Washington, July 22-23).
http://www.digitalpreservation.gov/meetings/documents/ndiipp14/Faundeen_NDSALevels.pdf

Goethals, Andrea (2013). "An example self -assessment using the *NDSA Levels* of digital preservation". En: *CAIW Ipres*. Lisbon, 2-6 September.
https://benchmarkdigitalpreservation.files.wordpress.com/2013/09/caiw2013goethals.pdf

Harvard Library (2014). *The new DRS: Plan for metadata migration, Harvard Library & Library Technology Services*. Harvard Library.
http://slideplayer.com/slide/3854725

ISO (2012). *ISO 16363:2012. Space data and information transfer systems - Audit and certification of trustworthy digital repositories*. Geneva: ISO.

Levels (2013). *Levels of digital preservation*. NDSA; DLF.
http://ndsa.org/activities/levels-of-digital-preservation

Maemura, Emily; **Moles, Nathan**; **Becker, Christoph** (2015). "A survey of organizational assessment frameworks in digital preservation". En: *Intl conf on digital preservation (Ipres 2015)*.
http://hdl.handle.net/1807/74699

Maemura, Emily; **Moles, Nathan**; **Becker, Christoph** (2016). "Organizational assessment frameworks for digital preservation: A literature review and mapping". *Journal of the Association for Information Science and Technology*. First published: 28 April 2017.
https://doi.org/10.1002/asi.23807

Nestor (2008). *Catalogue of criteria for trusted digital repositories: Version 2*. Frankfurt: Nestor Working Group Trusted Repositories – Certification.
http://files.d-nb.de/nestor/materialien/nestor_mat_08_eng.pdf

Phillips, Megan; **Bailey, Jefferson**; **Goethals, Andrea**; **Owens, Trevor** (2013). "The *NDSA Levels* of digital preservation: An explanation and uses". En: *Archiving*.
http://digitalpreservation.gov/ndsa/working_groups/documents/NDSA_Levels_Archiving_2013.pdf

Ross, Seamus; **McHugh, Andrew** (2006). "The role of evidence in establishing trust in repositories". *D-lib magazine*, v. 12, n. 7/8.
http://www.dlib.org/dlib/july06/ross/07ross.html

TRAC (2007). *Trustworthy Repositories Audit & Certification: Criteria and checklist, Version 1.0*. The Center for Research Libraries; OCLC Online Computer Library Center.
http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf

USGS (2014). *USGS guidelines for the preservation of digital scientific data*.
http://www.digitalpreservation.gov/ndsa/working_groups/documents/USGS_Guidelines_for_the_Preservation_of_Digital_Scientific_Data_Final.pdf

Ying, William (2013). "ARTstor shared shelf preservation plan based on the *NDSA Levels* of digital preservation". En: *Digital preservation 2013 meeting*.
http://www.digitalpreservation.gov/meetings/documents/ndiipp13/Ying.pdf