RICI Revista Ibero-Americana de Ciência da Informação

ISSN 1983-5213

Preservación digital: retos, experiencias y oportunidades.[1]

Manuela Moro Cabero
Universidad de Salamanca, Facultad de Traducción y Documentación, Salamanca, España
moroca@usal.es

DOI: https://doi.org/10.26512/rici.v12.n1.2019.10523

Recebido/Recibido/Received: 2018-07-12
Aceitado/Aceptado/Accepted: 2018-09-03

ARTIGOS

Resumen: La economía digital representa un nuevo modelo productivo en el que el profesional de la información debe erigirse como agente facilitador. El objeto de trabajo del profesional ha mudado del mundo analógico al digital. Esto exige adoptar métodos y disponer de conocimientos para su empleo que permitan preservar el recurso digital durante el tiempo que se estime necesario. Desde este enfoque, el gestor debe reflexionar sobre la naturaleza y alcance de la preservación; de este modo podrá asumir un rol proactivo y dirigido al logro de un archivo electrónico sostenible. El presente estudio tiene como finalidad conceptualizar la preservación a la par que plantea su complejidad. Se persiguen dos objetivos. El primero, se centra en exponer las amenazas más destacadas del recurso digital, mientras que en el segundo se expone el alcance de un plan de actuación así como sus actuaciones básicas. El estudio se plantea como un estudio de naturaleza descriptiva, basado en fuentes bibliográficas y en el análisis de las herramientas tecnológicas y normativas empleadas en la preservación. Los resultados esperados son los siguientes: relación de las amenazas más significativas, identificación de los enfoques necesarios para abordar la preservación, re-conceptualización de la preservación y finalmente, determinación de acciones de actuación.
Palabras-clave: preservación digital.

A preservação digital: desafios, experiências e oportunidades

Resumo: A economia digital representa um novo modelo produtivo no qual o profissional da informação deve estabelecer-se como agente facilitador. O objeto de trabalho do profissional mudou do mundo analógico para o digital. Isso significa adotar métodos e dispor de conhecimentos para o seu emprego que permitam preservar o recurso digital durante o tempo necessário. Partindo disso, o gestor deve refletir sobre a natureza e alcance da preservação; deste modo, poderá assumir um papel proativo dirigido a obtenção de um arquivo eletrônico sustentável. O presente estudo tem como finalidade conceituar a preservação ao mesmo tempo que aumenta a sua complexidade. Busca-se alcançar dois objetivos. O primeiro, centra-se em expor as ameaças mais destacadas do recurso digital, enquanto que o segundo consiste em expor o alcance de um plano de atuação, bem como suas atuações básicas. O estudo se caracteriza como de natureza descritiva, baseando-se em fontes bibliográficas e na análise das ferramentas tecnológicas e normativas empregadas na preservação. Os resultados esperados são os seguintes: relação das ameaças mais significativas, identificação dos enfoques necessários para abordar a preservação, reconceitualização da preservação e, finalmente, determinação de formas de atuação.
Palavras-chave: preservação digital.

[1] Texto originado de palestra proferida no XI Workshop Internacional em Ciência da Informação, Faculdade de Ciência da Informação e Programa de Pós-graduação em Ciência da Informação da Universidade de Brasília. Brasília, 12-15 de setembro de 2016.

Digital preservation: challenges, experiences and opportunities

Abstract - The digital economy represents a new productive model in which the information professional must establish himself as a facilitating agent. The work object of the professional has changed from analogue to digital. This means adopting methods and having knowledge for your job that will preserve the digital resource for the time needed. From this, the manager should reflect on the nature and scope of preservation; in this way, it can assume a proactive role aimed at obtaining a sustainable electronic file. The present study aims to conceptualize preservation while increasing its complexity. It seeks to achieve two objectives. The first one focuses on exposing the most outstanding threats of the digital resource, while the second one is about exposing the scope of an action plan, as well as its basic actions. The study is characterized as being of a descriptive nature, based on bibliographic sources and the analysis of the technological and normative tools used in preservation. The expected results are as follows: list of the most significant threats, identification of the approaches needed to address preservation, reconceptualization of preservation and, finally, determination of ways of acting.
Keywords: digital preservation.

1 Preservar. Una laguna de amenazas sin solución aparente

En el siguiente enunciado se analiza una batería de amenazas identificadas en el hecho preservador. Estas discurren desde meras confusiones de la parte por el todo (tomar una estrategia por la función, por ejemplo) a ausencias notables en el macro-proceso preservador, tales como la deficiente normalización de procesos, o de herramientas y modelos de almacenamiento; se remarca, igualmente, el desconocimiento de métodos y técnicas más apropiadas a la naturaleza del recurso digital, como es el caso del análisis de riesgos, entre otros.

1.1 Interpretar inconsistencias para actuar con consistencia como estrategia

En el informe Enumerate'2014 (COMISIÓN EUROPEA, 2014) se constata que el 92% de las entidades estudiadas[2] dispone de memoria digital con carácter patrimonial. Un 85% de ese porcentaje es híbrido. Esto es, dispone de patrimonio documental convencional y digital. La ratio de documentos nacidos digitales alcanza al 52% del conjunto de documentos. Esto es, más de la mitad del patrimonio documental ya es nacido digital. A esta cuantía, se debe sumar aquel patrimonio documental convencional que es digitalizado y almacenado en los e-depósitos.

La digitalización retrospectiva ha representado una de las estrategias preservadoras de mayor peso empleada en el proceso de mutación de oficinas sin papel y Archivo electrónico. Una muestra de ello se observa en el informe Enumerate (2014), donde se especifica que el 17% de los fondos/colecciones se encuentran en fase de digitalización, precisándose digitaliza,

[2] Se analizaron 1.900 centros informacionales, de los que 1.375 son bibliotecas, archivos y museos.

un 52%. De hecho, con excesiva frecuencia esta estrategia es asimilada al concepto de preservar, primando la parte por el todo. Esta confusión conlleva consecuencias muy negativas para la función preservadora en una entidad. De este modo, observamos como la digitalización, al ser asociada a la conversión del soporte del mundo tangible al numérico, es considerada factor de desarrollo en el progreso de los pueblos, dado que contribuye a construir democracia, al facilitar la difusión de la información, su acceso, su rápida recuperación, así como su pronta disposición ante cualquier consulta.

En esta línea, Thurston (2012) especifica la paradoja que representa este enfoque, donde digitalización es asociada a factor de progreso, frente a la preservación misma que, curiosamente, no es observada como factor de desarrollo por la sociedad. De facto, así se refleja en los presupuestos destinados a preservar y a digitalizar. Termens (2013) señala que se ha venido destinando un 50% del presupuesto de preservación exclusivamente a la ingesta de documentos analógicos en el sistema electrónico. Esto es, a su digitalización, siendo únicamente un 33% aquella ratio dedicada a acciones propias del almacenamiento y a migración de datos.

Si observamos los resultados obtenidos del informe Enumerate'2014, se confirman comportamientos presupuestarios bien llamativos, aunque con menor peso presupuestario destinado para la captura, dado que el 47% del presupuesto lo acaparan los costes fijos, siendo un 53% el dedicado a costes variables. De este 53%, es el 37% el dedicado a digitalización, mientras que un 19% sustenta la concreción de metadatos. No obstante, aunque se especifica una ratio más baja, continua sorprendiendo el monto económico destinado a la estrategia de preservación frente a otras actividades necesarias para lograr un adecuado despliegue de la función preservadora en una organización.

En este informe, resultan igualmente llamativas las ratios presupuestarias destinadas para el Archivo nacido digital. De los costes fijos, únicamente un 23% son presupuestados para almacenamiento, mientras que un 18% se destina a su gestión.

Estimando la notable cuantía porcentual presupuestada (entre un 37% y un 50%) para la ingesta en un repositorio, y más concretamente a la digitalización, cabe señalar que en el proceso de acometer dicha estrategia se vinculan riesgos de todo tipo en los resultados obtenidos, en cuanto a calidad, accesibilidad, reutilización, etc. Además, el proceso de digitalización precisa un adecuado y reflexionado proyecto. Cualquier tipo de deficiencia existente, tanto en proyecto como en proceso, redunda en resultados muy negativos, para la

preservación de los recursos, considerando su alcance conservador y de disponibilidad de los recursos digitalizados.

En esta línea de inconsistencias, Thurston (2012), igualmente, subraya la importancia que se otorga a las nuevas tecnologías en el proceso de conformar la memoria patrimonial, frente a la función preservadora. Especifica que las tecnologías son consideradas por la sociedad como el instrumento que aportará soluciones a todo tipo de problemas. Ante esta perspectiva, la función preservadora es minimizada frente a la función tecnológica de las organizaciones. De este modo se maximiza la tecnología que genera, administra y almacena el recurso digital, frente al propio recurso dado o digitalizado y a su tratamiento. El binomio se concreta en entorno tecnológico/recurso digital y se transfiere al binomio Informático/preservador. Acontece que la función de asegurar el valor de evidencia del recurso digital (manteniendo su veracidad, integridad, fidedignidad, disponibilidad, interoperabilidad, etc.), desde el enfoque del Archivo, no es considerada en el mismo rango de importancia que aquel valor otorgado a las TICs (Tecnologías de la Información y Comunicación). Magnificando, en suma, la labor del tecnólogo en perjuicio de la desempeñada por el gestor de recursos digital y preservador.

Además, desde un abordaje archivístico, se considera que un sistema de archivo electrónico incluye y, a menudo requiere, varias respuestas tecnológicas. La razón radica en que los datos y las informaciones disponen de distintos valores, hecho que naturalmente obliga a pensar en diferentes arquitecturas técnicas, tanto de ingesta, gestión, almacenamiento, acceso, como de conservación a largo plazo. Por lo tanto, no es posible imaginar en una única realidad para trabajar y moldear el patrimonio digital de los pueblos. Es preciso identificar las variadas necesidades informativas de los usuarios, considerarlas como necesidades cambiantes y a partir de estos supuestos, reflexionar sobre el modelo de Archivo a construir para dar cabida a servicios efectivos. Servicios, sin lugar a dudas, que den respuesta a todo tipo de necesidades en el tiempo. No se debe olvidar que la finalidad del Archivo es facilitar, atendiendo a los supuestos legislativos, el servicio de los datos, información y documentos que administra y preserva.

En este sentido, el alcance del concepto de “appraisal” regulado en la norma ISO 15489-1 (2016), da fe del alcance de una investigación para recopilar suficiente información que permita conocer los requisitos de los usuarios de un sistema de gestión para los documentos, así como los riesgos, aportando información para su diseño e implementación. Esto se debe a la complejidad del sistema, dado que en una organización conviven el archivo físico, el archivo electrónico y los sistemas de gestión de documentos que disponen (o carecen) de una variada

gama de funcionalidades para el almacenamiento temporal y preservación de los documentos en el tiempo.

Desde esta perspectiva, son necesarias nuevas habilidades y competencias, tanto para la captura, gestión, acceso a la información, como para su preservación. Se debe consolidar una formación oficial de enseñanza superior, así como de naturaleza permanente puntual, basada en prospectiva y avances tecnológicos. No obstante, hasta la fecha, tanto en España como en Brasil, apenas se consigna como disciplina en estudios de grado y en posgrados (con la consiguiente ausencia de suficientes profesionales capacitados). En ninguno de los casos, es considerada como una macro-función que requiera de numerosas disciplinas para ser afrontada con los conocimientos y habilidades suficientes. No obstante, sí que ha sido materia de proyectos e investigaciones y por ende, se dispone de numerosas fuentes y recursos para su aprendizaje. Resumiendo, los conocimientos empleados para la conservación de recursos tradicionales no son suficientes; conforman una parte muy reducida de los conocimientos exigibles.

Otra inconsistencia la hallamos en la legislación, así como en el despliegue de políticas apropiadas a dicha función. Así, la preservación de recursos digitales, por ejemplo, en España, hasta fechas muy recientes, se dificultaba en la propia legislación, debido a los derechos regulados en leyes de propiedad industrial: ley de la propiedad intelectual, contratos comerciales, etc. De facto, la distribución y difusión de los recursos mediante entornos tecnológicos contemporáneos resulta de difícil aplicación sin vulnerar la legislación de propiedad intelectual o tramitar licencias de todo tipo, lo cual redunda en incremento de costes en el momento de actuar. Para la distribución de los recursos (difusión) se ha venido programado aquel material sujeto a dominio público o considerado obra huérfana. Si bien, hay un volumen muy numeroso de materiales que escapan a estas categorías. Así pues, la legislación ha de ser coordinada –en un plano nacional e internacional- para asegurar, al menos, la preservación del recurso digital que así haya sido estimado. Marcos legislativos restrictivos impiden la conservación y, a menudo, la disponibilidad de los documentos. En ocasiones, el enfoque debe centrarse en la coordinación de marcos legislativos bien diferentes, como es el caso de las situaciones transfronterizas generadas en almacenamiento de datos en la nube, por ejemplo, donde el proveedor de servicios dispone de un corpus legal diferenciado del que debe cumplir el contratante del servicio. En otras situaciones, recursos digitales como Webs, recursos derivados de las redes sociales, etc. no están sujetos a un marco legislativo que les favorezca, delimitando sus opciones preservadoras (protección de datos, depósito legal de recursos generados digitales, etc.).

Se precisan políticas de preservación en las organizaciones. No obstante, las cifras hablan por sí solas. Únicamente se computa el 50% el número de entidades que disponen de unidades de preservación activas y de políticas de preservación. En el informe de Enumerate'2014, se registra que del 92% de organizaciones con patrimonio digital, solamente un 34% de ellas desarrollan estrategias de preservación y, únicamente, un 23% (de ese 34%) mantienen estrategias de preservación a largo plazo. Desde la óptica de las unidades de depósitos, buena parte de los no repositorios son certificados para demostrar un grado de confiabilidad aceptable.

1.2 Normalizar procesos e implementar herramientas para el almacenamiento como estrategia

Dada la vulnerabilidad del recurso digital y la complejidad de los entornos de trabajo donde se genera dicho recurso, se precisa normalizar procesos y procedimientos de trabajo, favoreciendo el desarrollo de proyectos preservadores suficientemente regulados. Sin embargo, Enumerate (2014) desvela, como el 48% de las entidades poseedoras de patrimonio digital -y en las que se contemplan estrategias de preservación a largo plazo-, no consultan y aplican normativa alguna. Esto es, del 23% de organizaciones que disponen de esas estrategias, casi la mitad lo hace sin adoptar norma alguna. La preservación exige método y sistematización de las tareas. Su transcendencia es tal que resulta difícil imaginar el desarrollo de esta función sin normalización alguna. En principio, la veracidad del recurso digital exige la aplicación de normas para trabajar seguridad de la información (serie UNE-ISO 27001; ISO/IEC 27036-4:2016, etc.), y protección de datos. Su vulnerabilidad obliga a trabajar riesgos desde el mismo momento de creación del recurso digital (UNE-ISO/TR 18128:2014), de diseñar sistemas de gestión de documentos acordes a las necesidades (UNE-ISO 30300:2011 y UNE-ISO 30301:2011), de regular las aplicaciones donde se generan (UNE-ISO 15489-1:2016) y conocer el tipo de requisitos funcionales y tecnológicos que se precisan (UNE ISO 16175 1-3); de controlar los dispositivos de almacenamiento (UNE-ISO 14721:2015; UNE-ISO 14641-1:2014); y de demostrar grados de confiabilidad sobre los mismos (ISO 16363:2012; ISO/FDIS 17068: 2016); de trabajar de modo normalizado todo tipo de estrategias de preservación, tanto para la digitalización (UNE-ISO 13028:2010), para la conversión y migración (UNE-ISO 13008:2012), como para el despliegue de metadatos desde que surge el recurso (serie ISO 23081 1/3), como en posteriores actuaciones de conservación (PREMIS), u otras normas de preservación a largo plazo (ISO/TR 18492:2005; ISO/TR 15801:2009 Rev.). El factor tecnológico, igualmente incide y

obliga a conocer y controlar los formatos, buena parte de los cuales son productos normalizados.

En preservación, igualmente, es preciso conocer y aplicar herramientas específicas tanto para la ingesta, para la identificación de los ficheros incorporados, así como para su metadescripción para la recuperación posterior de datos e informaciones. Aplicaciones como *DROID, Jhove2, FIFZ, XENA, Extractor, Pronom, FileMaker, Checksum*, etc. vienen siendo empleadas considerando sus diversas funcionalidades de identificación de ficheros, reconocimiento de formatos, caracterización de casas comerciales, derechos legales, control de bytes y de metadatos ante la captura de ficheros, por ejemplo. En esta línea, se precisa también comprender el funcionamiento de normas de metadatos para el encapsulado, de paquetes como lo es METS o para incorporar los metadatos mínimos exigidos de preservación (estándar PREMIS). Al respecto, de los presupuestos observados, en Enumerate (2014) se destaca que un 19% son destinados a la normalización de metadatos.

El hecho de que buena parte de las entidades se conformen de memoria patrimonial híbrida, esto es, no solamente digital, sino que se contemplen materiales analógicos (48%), obliga, igualmente a considerar conocimientos y habilidades, así como a destinar presupuesto para su tratamiento. En consonancia, no se ha producido un incremento presupuestario correlativo.

Por otro lado, la integridad del documento digital exige el control del recurso digital desde el momento de su creación (esto es, en la aplicación de software y sistema en que se crea). Precisa, una estrategia de almacenamiento respetando parámetros definidos (requisitos técnicos y funcionales), tanto en las oficinas, como en los e-depósitos de almacenamiento destinados a su preservación a medio y largo plazo. Este control de las áreas de almacenamiento puede variar y efectuarse con mayor o menor precisión dependiendo de las organizaciones, dado que pueden confluir situaciones diversas de almacenamiento, tales como, la creación del recurso en aplicaciones que no cumplen requisitos técnicos y funcionales que aseguren la integridad, o como entidades donde desde la creación se incluyen disposiciones para asegurar dicha integridad, a situaciones donde el documento no se captura en un determinado repositorio;

Esto es, un repositorio que cumple con todos los requisitos archivísticos y garantías de control posibles. Finalmente, es preciso que se demuestre un control de la integridad. Esta se logra bien mediante demostraciones de confianza, (auditorías atendiendo a normas, tales como aplicaciones de ISO 16363:2012 para un repositorio, o Moreq2, para requisitos), bien

mediante el aseguramiento del cumplimiento de adecuadas contrataciones o auditorías de parte sobre el proveedor de servicios (UNE-ISO 14641-1:2015). En el caso de entornos de *cloud computing*, una lista de verificación para los contratos de servicios en la nube, es una opción recomendad y disponible a través del trabajo de InterPAREs (BUSHEY, G y otros, 2015).

Es preciso comprender que se ha producido un cambio considerable en los modelos de almacenamiento. Estos son sofisticados y pueden disponer de servicios de red, de seguridad y de servicios operativos comunes. Se precisan depósitos para los recursos electrónicos con diseños que permitan la consulta de los documentos. Razón por lo que, la tradicional sala de consulta o gaveta dispuesta para la consulta con sus dispositivos facilitadores de recuperación, así como los depósitos, han sido transformados en un complejo entorno de almacenamiento y de servicio de ficheros. En este entorno son incorporados paquetes de información remitidos desde las aplicaciones donde se crean (PIT-paquetes de información transferida) y en él son caracterizados para su almacenamiento (PIA-paquetes de información de archivo) y disponibilidad (PIC-paquete de información de consulta), mediante pautas reguladas de almacenamiento para la conservación, gestión de todos los datos y provisión de ficheros atendiendo a demanda.

La norma UNE-ISO 14721:2015 (ISO 2012), regula el diseño normalizado de estos e-depósitos. En ella se reconocen una serie de entidades funcionales que, mediante una red amplia de tareas, capturan los ficheros controlando su ingreso en el depósito (asignación a los PITs, formatos, etiquetado de metadatos de entrada); ubican y relacionan esos ficheros (con otros analógicos y etiquetan su almacenamiento en PIAs), mediante el almacenamiento de los mismos; identifican y preparan para la recuperación (de PIAs a PIC, completando la gestión de datos); se adelantan a posibles cambios tecnológicos, planificando la conservación; disponen para consulta (a través de la funcionalidad de acceso) y administran, en su conjunto la totalidad del repositorio y del servicio de consulta. Resulta curioso observar como el estudio Enumerate (2014) señala que el 31% de las entidades con patrimonio digital dispone de políticas de uso de los recursos, siendo un 42% el porcentaje que mide el uso del recurso, un 85% para los recursos Web y un 32% para recursos derivados de las redes sociales.

Otros servicios de almacenamiento de futuro ineludible son aquellos que han sido trabajados para el almacenamiento a corto y medio plazo en entornos de nube y que con mayor frecuencia son contratados para almacenar a largo plazo. Ellos incorporan las ventajas de un entorno de red (servicios a medida, pago atendiendo a demanda, disponibilidad de recursos y tecnologías, facilidad para disponer de copias de los datos, seguridad, etc.), aunque

en ellos se aprecian, igualmente, numerosos riesgos que deberían ser gestionados (accesibilidad, cumplimiento legal en situaciones transfronterizas, deficiencias funcionales de archivo, descontrol de la geolocalización, etc.), desde posiciones proactivas del profesional con un ejercicio asesor e interventor en grados diversos.

1.3 Fomentar la gestión del riesgo como estrategia

La vulnerabilidad del recurso digital conlleva asociado un requisito de conocimiento de los factores de riesgo vinculados al mismo, así como de su gestión. Entre los factores de riesgo destacamos los siguientes: volumen y variedad de recursos, heterogeneidad de patrimonio histórico, crecimiento exponencial del recurso nacido digital, digitalización retrospectiva cuantiosa, ausencia de sensibilización para la preservación, supeditación tecnológica, marco legal complejo, seguridad de la información dificultosa, inestabilidad de la información digital, incremento de los costes de preservación, complejidad de recursos para preservar, como puede ser la Web profunda, marcada brecha digital, archivo híbrido, etc.

Desde la creación del recurso es preciso identificar requisitos para su gestión y aquel conjunto de riesgos vinculados a su ausencia o a su control. El informe técnico UNE-ISO/TR 18128 (2014) ha sido creado precisamente para ayudar al profesional a identificar áreas de riesgo para los documentos. Sin embargo, en el proceso preservador, se precisa conocer cada categoría de recurso digital existente y los riesgos vinculados a su naturaleza, así como aquellos otros de su almacenamiento. Los métodos y técnicas de evaluación del riesgo deben ser conocidos por el profesional para preservar el recurso.

La apreciación del riesgo es un método complejo y sistémico que exige adquirir, en primer lugar, conciencia del riesgo mismo. Esto es, del peligro al que está expuesto el recurso y del impacto que supone su deterioro o pérdida para una organización. En segundo término, será preciso identificar todos los riesgos, determinar los factores de riesgo, priorizar los riesgos, atendiendo a su impacto, valorarlos, por tanto y establecer un programa para su tratamiento y gestión de resiliencias aprendidas. Este proceso global, de identificación, análisis y evaluación o gestión del riesgo es sistémico, proactivo, dirigido a prevenir pérdidas y a capitalizar oportunidades. Por esta razón, debe de ser contemplado como una herramienta de soporte en la preservación del recurso digital (página web, repositorio, datos en la nube, etc.) y en los procesos de preservación asociados a las estrategias (conversión, migración, digitalización…).

La gestión de riesgos se encuentra normalizada en diferentes entornos y muy trabajada en los repositorios, en los que se incorporan aplicaciones que permiten analizar el riesgo, establecer informes, orientar sobre mitigaciones del mismo e informar sobre posibles riesgos residuales.

El uso de normas para la preservación facilita el reconocimiento de riesgos, dado que son numerosos los criterios y requisitos que en ellas se incluyen y cuyo incumplimiento implica impactos desfavorables. Así, la norma UNE-ISO 14641-1:2015 incluye requisitos mínimos y adicionales que nos orientan sobre sostenibilidad, integridad, seguridad y trazabilidad de la información y su preservación a largo plazo. La norma ISO 16363:2012 aporta confiabilidad a los depósitos a la par que adelanta riesgos, ante el incumplimiento de criterios observados. Otro ejemplo lo hallamos con el seguimiento de la norma ISO 27036-4:2016. Esta regula requisitos para la seguridad de los datos ante servicios contratados en la nube, favoreciendo el almacenamiento de datos. Son numerosas las herramientas que trabajan el reconocimiento del riesgo, como puede ser la empleada en la UE (Unión Europea), conocida como Drambora, para gestionar riesgos en repositorios.

La implementación de modelos de gestión de riesgos como metodología de trabajo en el sector de la información y documentación, en sus sistemas, procesos, instrumentos básicos y tecnologías, supone adquirir habilidades para la planificación y gestión del riesgo. Es preciso comprender la necesidad de implementar planes de tratamiento del riesgo, registros donde se identifiquen los riesgos, matrices del riesgo donde se nos permita priorizarlos y trabajar su gestión de modo dinámico y retrospectivo, así como informes de riesgo, donde se incluyan lecciones aprendidas.

Además, en cada proyecto vinculado a una o varias estrategias que se recojan en el plan de preservación, el riesgo y su gestión no deben ser obviados. De facto, el hecho mismo de planificar, proyectar, identificar mediante registros y elaborar informes disminuye los riesgos vinculados a la planificación, al diseño y a la implementación de sistemas, procesos y estrategias de conservación.

Así, a modo de ejemplo, si tomamos como referente un proyecto de digitalización, lógicamente son variados los asuntos que han de ser considerados. Comenzaremos por analizar los recursos que serán objeto de migración, su naturaleza, su potencial, las necesidades a las que responden, etc. desde el enfoque selectivo; identificados estos, será preciso conocer las habilidades y competencias necesarias del personal para llevarlo a efecto, los conocimientos tecnológicos, el equipamiento que será empleado en el proceso, así como su disposición; además, deberá establecerse una estimación de costes y una programación

para llevarlo a efecto. Lógicamente, se deben de vincular riesgos asociados a todos estos requisitos.

Se necesitará implementar controles de calidad en imagen (tamaño, profundidad, color), en procesos y en tecnologías, así como sobre el test de validación de la digitalización, la certificación de la misma y calificación de metadatos derivados del proceso. Dichos controles se orientarán a obtener una adecuada digitalización, respondiendo a los requisitos de digitalización y de servicio de la(s) comunidad(es) específica(s) identificada(s). La existencia de una planificación en la que se establezcan fases y se identifiquen tareas, incluidas las de control, resultan fundamentales en la aplicación de cualquier estrategia de preservación.

Múltiples amenazas y variados requisitos observados en la preservación nos invitan a reflexionar sobre nuevos enfoques de trabajo, los cuales acometemos en el siguiente epígrafe.

2 Preservar. Nuevos enfoques de trabajo

En la función preservadora se reconocen heterogéneos enfoques de trabajo. Algunos de ellos, denotan la fragilidad de la función preservadora, mientras que otros son testimonio de su favorable prospectiva.

En primer término, se destaca el enfoque propiamente preservador de la memoria patrimonial digital. Esto es, aquel en el que se subraya la finalidad de conservar el recurso, entendido como objeto de información de utilidad para la organización y para la sociedad. El profesional debe asegurar la memoria patrimonial digital que, en atención a las ratios observadas, (sobre políticas, estrategias, unidades preservadoras, presupuestos, etc.), se demuestra no lograrse con suficiente éxito. En este sentido, se están realizando innumerables esfuerzos en la preservación, tal y como es posible observar a tenor de herramientas y proyectos accesibles en el Registro de herramientas de preservación a largo plazo -COPTR[3] (con un total de 424), si bien, se precisa sensibilizar, formar e incrementar el alcance preservador. Se debe ahondar en la consecución de este objetivo.

Además, buena parte de los recursos digitales precisan demostrar veracidad y mantener una adecuada cadena de custodia. La confiabilidad del recurso digital se alcanza asegurando, entre otros aspectos, su integridad desde su creación, captura, tratamiento y

[3] Community Owned digital Preservation Tool Registry (COPTR)
Accesible en: http://coptr.digipres.org/Main_Page (consultado en: 26/05/2017). Más información, igualmente, sobre recursos y herramientas en el *site* del NSDA, accesible en: https://wiki.diglib.org/NDSA:Digital_Preservation_in_a_Box

conservación a largo plazo. Seguridad, trazabilidad y políticas de protección de datos contribuyen a dotar de autenticidad e integridad el recurso digital. La aplicación de esquemas de seguridad en las organizaciones facilita la veracidad. No obstante, el preservador debe constatarla durante todo el ciclo de vida del recurso, con independencia de su ubicación. Resulta esencial una adecuada gestión desde la creación del recurso para asegurar su cadena de custodia. El preservador deberá vigilar que en aplicaciones y repositorios se incorporen y cumplan determinados requisitos tecnológicos y funcionales, con independencia del modelo de gestión documental y de conservación que la organización disponga, siempre supeditado a un amplio abanico de posibilidades: aplicación con dispositivos de almacenamiento seguros o con deficiencias.

El seguimiento de la veracidad, así como la supeditación del recurso a las obsolescencias tecnológicas y de logiciales, implican una obligada reflexión, en el momento de la valoración y disposición del recurso sobre su conservación. Será obligado identificar necesidades de información de las comunidades de usuarios y conocer el modo en que un recurso digital dado será consultado, utilizado o reutilizado y por quién. Frente a una custodia pasiva de documentos y colecciones, el preservador en un entorno electrónico debe afrontar una custodia dinámica en la que se exige conocer naturaleza del recurso, naturaleza de la comunidad específica de usuarios de dicho recurso, necesidad informativa –cambiante, por regla general, relación de estrategias a desplegar para ese recurso en el tiempo y costes derivados. Este conocimiento le permitirá reflexionar, posicionándolo en sus actuaciones de modo proactivo, sobre la construcción de la memoria patrimonial institucional y social.

Un segundo enfoque más favorable, se deriva del hecho mismo de preservar paquetes de información que son etiquetados para su identificación, ubicación, almacenamiento y recuperación. El profesional se rodea de datos. Preserva objetos de datos etiquetados y sujetos a un incremento de su metanarrativa. Además, a ello contribuyen los gobiernos abiertos y todos los movimientos de *open data*, el potencial de los *big data* en el sector privado, los entornos de *cloud computing*, entre otros, generando nuevas aproximaciones a la economía digital basada en datos. Se trata de un universo digital dispuesto, no sólo para el uso, sino para la reutilización y donde la explotación de datos a corto, medio y largo plazo, resulta altamente rentable. Este nuevo modelo productivo y de gobernanza exige una nueva mirada del profesional de la información, donde el preservador deberá actuar para aconsejar sobre cadenas de custodia, integridad de los datos, así como para su conservación propiamente dicha y disponibilidad, si fuese necesario.

Una actuación proactiva, dinámica, sostenible del preservador, sólo es posible si el preservador comprende que debe trabajar de modo colaborativo con diversos profesionales, con una finalidad clara: asegurar el recurso digital desde su creación y mantenerlo disponible en el tiempo para cuando se precise su uso y reutilización. El profesional de la información ha de actuar con estrategia para identificar el recurso, conocer su naturaleza, identificar la comunidad de usuarios presente y futura, establecer estudios de prospectiva sobre sus necesidades informativas de uso y reutilización del recurso, así como de mudanzas y avances tecnológicos para preservarlo en entornos tecnológicos, de tal modo que sea conservado sin pérdida en el grado de disponibilidad: accesibilidad, uso y reutilización. Este tipo de acciones no puede acometerlo de modo aislado, sino que debe participar del conocimiento de tecnólogos, de legisladores, estadísticos, documentalistas y archiveros, de los productores de los recursos etc.

La complejidad de amenazas y enfoques obligan a repensar el propio concepto de conservación. Para ello, se ha generado el siguiente epígrafe.

3 El ABC de la preservación proactiva del recurso digital

Debe entenderse a la preservación como un todo sistémico conformado por una serie de partes que la integran y se encuentran estrechamente relacionadas. En primer lugar, preservar incluye la idea de *conservar* recursos digitales pero también, recursos analógicos (documentos y colecciones). De los primeros, son numerosas las categorías establecidas: documentos de office, documentos de entornos web, de social media, de aplicaciones de oficina para gestión presupuestaria, contable, de recursos humanos, etc., documentos geoespaciales, audiovisuales, etc. Esta enumeración contribuye a comprender la complejidad de preservar la *variedad* de recursos. Dichos recursos son almacenados en repositorios con diferentes funcionalidades y requisitos tecnológicos que pueden ser e-depósitos vinculados a aplicaciones documentales, a aplicaciones de gestión documental, a unidades de almacenamiento creadas para almacenar a largo plazo o, incluso, a unidades de almacenamiento en la nube con situaciones de almacenamiento distribuido. La conservación física alcanza, por tanto, a documentos y colecciones tangibles, como a recursos digitales de naturaleza heterogénea que son almacenados en e-depósitos y *data centers*.

En segundo término, y para *asegurar veracidad,* el concepto de preservar debe vincularse con el de seguridad de la información. La veracidad e integridad de los recursos y el

valor de su cadena de custodia implican construir seguridad desde la creación del recurso mismo.

En tercer lugar, y dada la obsolescencia tecnológica, preservar significa también investigar sobre *prospectiva tecnológica* para identificar tendencias y, de este modo, facilitar la selección de estrategias y la coordinación de costes de preservación, pero además, para poder asegurar la conservación a largo plazo.

En cuarto término, preservar lleva asociado la idea de *disponibilidad*. Se conserva para disponer la información contenida en los recursos cuando sea precisada. Acceso, uso y reutilización deben ser asociados a la preservación. No es posible determinar una estrategia o una combinación de ellas sin apartarse del concepto de disponibilidad.

Finalmente, preservar supone, igualmente, coordinar las estrategias preservadoras y establecer, atendiendo a los requisitos de aquellas seleccionadas, planes de preservación sostenibles para la organización.

Como es posible observar, la función preservadora ha incrementado su peso frente a otras funciones de gestión y conservación documental. Resulta evidente su sombra alargada hasta el propio proceso creativo del recurso mismo. En una retrospectiva, pudiéramos señalar que progresivamente, la función creadora y de tratamiento del documento ha decrecido en favor de la preservadora, cuya importancia se ha acrecentado. La necesidad de identificar la naturaleza de los recursos, las características del entorno tecnológico donde se crean, capturan, acceden y almacenan los datos y objetos de datos, las comunidades de usuarios y sus cambiantes necesidades informativas, los riesgos a los que se someten ante incumplimientos y deficiencias en requisitos funcionales y tecnológicos, ha supuesto revisar el concepto de “appraisal”, estrechamente vinculado a la preservación, dado que no es posible valorar y adoptar decisiones de disposición sin considerar estrategias y costes de preservación.

En la función preservadora se reúnen y concilian dos tipos de intereses de cualquier organización. Las entidades tienen la necesidad de preservar los documentos para sus intereses inmediatos, esto es, para su uso y reutilización en las actividades de negocio. Esto es, se trabaja, desde la óptica preservadora para facilitar la continuidad digital, asegurando que el recurso esté accesible, disponible en todo momento cuándo y cómo se precise.

Por otro lado, se dispone de los recursos para el futuro, asegurando que prevalezca la memoria patrimonial institucional y social; Como es factible observar, parecieran, en cierta forma, intereses contrapuestos. Se trata de dar respuesta a otro tipo de intereses en los que el

recurso ha de ser conservado para su uso y reutilización (si fuera el caso) a largo plazo. De ahí, que Thurston caracterice dicha profesión como una función que sufra cierta esquizofrenia o bipolaridad, trabajando en el presente con recursos del pasado y del presente para sustentar el presente y construir el futuro.

Ante este esfuerzo conciliador, se reconocen dos objetivos en la preservación: el primero se focaliza en conservar la información que está sujeta a constante mudanza, dado que, igualmente, las necesidades de los usuarios no son estables. El segundo se centra en garantizar la accesibilidad y usabilidad del recurso digital mismo, en el tiempo, así como el de las tecnologías, con independencia de formatos, soportes y medias empleados desde su creación hasta su almacenamiento en repositorios permanentes.

Considerando que buena parte de los países, aún no han elaborado una política de preservación, ni mantienen una "filosofía de la preservación" de aplicación a largo plazo, carecen de una infraestructura de preservación y aún mantienen marcos legales poco favorables a ella, urge establecer y consolidar colaboraciones internacionales que permitan sensibilizar e informar y apoyen el desarrollo y despliegue de acciones preservadoras. En esta línea, la carta de la preservación de la Unesco (2003)[4], adoptada por Brasil al portugués, revisada en Moscú (2011), Vancouver (2012) y Varsovia (2015)[5] en declaraciones diversas, señala la necesidad de: 1-Establecer políticas de preservación. 2- Informar sobre los riesgos e impacto de no preservar. 3- Formar y establecer políticas educativas donde se incluya la preservación. 4-Promove investigaciones que favorezcan y apoyen la preservación de recursos. 5- Promover la colaboración internacional. 6- Impulsar esfuerzos comunes que permitan reducir gastos en preservación; y 7- Establecer alianzas en la industria TIC, impulsando formatos abiertos, software libre, licencias multiusuarios, etc.

Además, se debe sensibilizar al personal, consolidar alianzas, para incrementar las colaboraciones, planificar las acciones preservadoras, mediante planes y proyectos, normalizar los procesos derivados de la función preservadora, y, finalmente, mantener y asegurar unidades administrativas de preservación que permitan aportar continuidad al hecho preservador. Lógicamente, ante cualquier ausencia de recursos presupuestarios suficientes, se debería ser muy selectivos con los recursos que serán preservados, atendiendo a estrategias a

[4] UNESCO. Carta para la preservación del patrimonio digital. [Paris]: UNESCO, 2003. Disponible en: <http://www.arquivonacional.gov.br/conarq/cam_tec_doc_ele/preservacao/cartapreservacao.asp>

[5] Recomendación relativa a la preservación del patrimonio documental comprendido el patrimonio digital y acceso al mismo. Disponible en: http://portal.unesco.org/es/ev.php-URL_ID=49358&URL_DO=DO_TOPIC&URL_SECTION=201.html

combinar, necesidades de las comunidades de usuarios presentes y futuros y costes disponibles, trabajando sin alejarse de conceptos de realidad, factibilidad y sostenibilidad.

Se debería impulsar la búsqueda de alianzas y colaboraciones para reducir gastos, capacidades y esfuerzos, sin perjuicio de asegurar el recurso y sus garantías de integridad y disponibilidad, siempre sin alejarse de un criterio facilitador en la selección del recurso que ha de ser preservado, esto es, de fácil recopilación, selección y preservación.

Para finalizar este epígrafe, subrayamos los aspectos que confluyen en una nueva conceptualización de la función. Esto es, se ha producido una mudanza del objeto a conservar; la cual ha supuesto incrementar su complejidad, debido a su variedad, volatilidad, necesidad de demostrar veracidad y, en general, su vulnerabilidad. Se ha producido una variación en el área y modo de almacenamiento. Se ha pasado de un almacenamiento físico, tangible y caracterizado por las limitaciones perimetrales de un depósito reconocible a la vista, a un modelo de almacenamiento lógico, en ocasiones virtual, en otro casos con cierta fisicidad (data centers), y caracterizado por la ausencia de perímetros, así como la presencia de capacidad de almacenamiento en medidas casi inmensurables de bytes. Se ha producido un cambio patente, donde la Ley de Moore y la de Kryder han favorecido el procesamiento –y por tanto la rapidez en generar más información- y el almacenamiento, abaratando costes tecnológicos y de almacenamiento, a la par que se reducen tamaños de capacidades de almacenamiento a pulgadas.

Debido a estas mutaciones, no es posible afrontar una preservación pasiva, atendiendo a que, con actuaciones benignas mediante el control de los indicadores medioambientales y la intervención restauradora en aquellas ocasiones en que fuese necesario, serán suficientes. Lejos de esa idea, las transformaciones sufridas exigen actuaciones proactivas que aseguren no sólo la conservación del recurso mismo, sino su disponibilidad en el tiempo. La finalidad de conservar para disponer se mantiene, pero no es posible afrontarla con los anteriores fundamentos, principios, métodos y técnicas y, por supuesto, con los conocimientos tradicionales con los que se afrontaba la conservación del recurso físico. En idéntica línea, tampoco es posible asumirla con los presupuestos de antaño y, debido al coste que supone, sin criterios de sostenibilidad (Cruz Mundet, 2015).

Considerando estos cambios, lógicamente, se precisan nuevos métodos. Se ofrece una introducción en el siguiente epígrafe.

4 Preservar significa planificar y actuar

Planificar la preservación exige una investigación exhaustiva sobre los recursos digitales sujetos a preservación, sobre el entorno tecnológico en el que se crean, gestionan o/y almacenan dichos recursos, sobre las necesidades de información que los productores o usuarios, en último término prevén necesitar, sobre los recursos presupuestarios, de infraestructuras y de capacidades personales disponibles en la organización para la que se pretende trazar el plan. Básicamente, la elaboración de un plan implica dar respuesta a un considerable número de interrogantes, tales como: ¿Qué categorías y volumen de recursos debo preservar? ¿Cuál es su naturaleza? ¿Cuáles son esenciales para el funcionamiento de la organización? ¿Qué pretendo conservar del conjunto de recursos o contenidos identificados? ¿Cómo los estoy conservando en el presente? ¿Cómo puedo asegurarlos en el futuro? ¿A qué tipo de contingencias y riesgos están expuestos? ¿Qué protección será la más conveniente ante factores de riesgo elevados? ¿Qué medidas de protección puedo desplegar para mitigar el impacto? ¿De qué dispongo para su adecuado almacenamiento y procesamiento? ¿Qué necesito para su adecuado almacenamiento? ¿Están los recursos suficientemente identificados? ¿Disponen de metadatos de conservación? ¿Puedo conocer cuáles son los datos técnicos del entorno en el que se almacenan? ¿Quién los consultará? ¿Para qué necesito los recursos? ¿Qué tipo de acceso preveo que es necesario? ¿Cuáles deben ser reutilizados? ¿Dispongo de capacidad para afrontar la conservación con garantías? ¿Dispongo de presupuestos suficientes? ¿Los agentes implicados en el proceso demuestran competencias para su ejecución? ¿Cuál es la tendencia tecnológica de almacenamiento?

Excesivos interrogantes que exigen respuestas bien reflexionadas y por ello, es posible establecer las siguientes fases (VOUTSSÁS, 2012):

- Fase de Identificación de contenidos a preservar (categorías, tipologías, naturaleza, volumen, formatos, elementos descriptivos asociados, etc.).
- Fase de selección de los contenidos que serán conservados (considerando necesidades informativas, presupuestos disponibles, tecnologías existentes o disponibles, capacidades para llevarlo a efecto, etc.).
- Fase de determinación de los plazos de almacenamiento para los contenidos (considerando uso y valores de los documentos).
- Fase de estudio del entorno tecnológico donde se crean, almacenan y conservan los recursos digitales.

- Fase de evaluación de la capacidad y potencialidad para el almacenamiento de contenidos a medio y largo plazo: considerando capacidades de almacenamiento en repositorios, de copias de seguridad y replicados y de opciones de almacenamiento en la nube o de otra naturaleza colaborativa.
- Fase de determinación de riesgos a los que están sometidos los recursos (en atención a la categoría del recurso, identificación de riesgos, gestión y tratamiento de los mismos, desde un enfoque sostenible del tratamiento del riesgo y del impacto producido ante ausencia de tratamiento).
- Fase de protección de los contenidos ante contingencias: incluye el desarrollo de planes de continuidad digital, de planes de tratamiento y mitigación del riesgo y de acuerdos en la devolución de datos almacenados en la nube, ante la finalización del contrato, o ante contingencias vinculadas a la nube, entre otros.
- Fase de identificación de estrategias más adecuadas para la preservación del recurso, incluidas posibles combinaciones para asegurar el recurso desde su creación.
- Fase de gestión e implementación de los requisitos necesarios para almacenar y proteger los recursos, en atención a las estrategias adoptadas y a los avances de la tecnología.
- Fase de estudio de la disponibilidad de los recursos y su marco legal (gestión de licencias por distribución de recursos sujetos a derechos de propiedad intelectual, de propiedad comercial y de protección de datos.
- Fase de programación de la implementación del plan (para cada uno de los recursos trabajados en el plan de preservación).
- Fase de coordinación, si así fuera, de los recursos analógicos con digitales (en Archivos híbridos).
- Fase de evaluación de resultados y estudio de resiliencias.

Para algunas de las estrategias que han sido normalizadas se regulan fases y tareas con gran detalle, muy especialmente, dada su importancia en la preservación y su uso, para la digitalización, para la conversión y migración. Tanto la norma UNE-ISO 13008: 2012, como la UNE-ISO 13028:2010, incluyen proyectos bien detallados.

A menudo, no disponemos de capacidad para desarrollar con el detalle requerido un plan de conservación. No obstante, La NDSA (*National Digital Stewardship Alliance*) establece niveles[6] de actuación básicos mediatizados por cinco factores. Dichos factores responden a los siguientes 5 aspectos clave para la preservación: control de formatos, veracidad e integridad

[6] Accesibles en: http://ndsa.org/activities/levels-of-digital-preservation/ (Fecha de consulta: 29/05/2017)

del recurso, control de metadatos del recurso, seguridad de la información y control del almacenamiento del recurso. Analizamos el alcance de estos aspectos, seguidamente.

1- Control de formatos

Se podría considerar al formato como un intermediario entre el objeto de datos y la información. De ahí su importancia. La obsolescencia de aplicaciones genera innumerables formatos desconocidos o no identificados. El problema que afronta el preservador es doble: la variedad de formatos (se trata de miles) y su obsolescencia. Hecho que puede derivar (y así acontece) en el desconocimiento de los formatos. Así, pues, si disponemos del objeto de datos y de la información de representación de ese objeto, podremos controlar su obsolescencia y gestionarla. Esto es, reconocer su estructura. Además, los formatos varían en atención a las versiones y a los sistemas operativos o/y aplicaciones con los que se opere.

Los formatos expresan el paso del tiempo intergeneracional de entornos electrónicos. Incluso los formatos abiertos están sujetos a numerosos cambios. Como preservadores, debemos, por tanto, conocer sus propiedades, sus riesgos, su viabilidad de migración, etc. Además, de investigar su identificación y potencial en la conversión y migración.

Se debería alcanzar progresivamente lo siguiente:

a) Protección de los recursos digitales mediante el control de un set limitado de formatos para cada categoría de recurso, a ser posible, formatos abiertos (libres de licencias). Tanto el NARA[7], como la Library of Congress[8], disponen de información sobre los formatos más aconsejables, considerando riesgos y avances y de modo actualizado.
b) Identificación de formatos, mediante la elaboración de un inventario de los mismos. Esta tarea requiere ubicar el formato en la oficina y máquina, conocer su versión, sus propiedades y características. Identificar la compañía si el formato es propietario, tanto el desarrollador como el mantenedor actual. Conocer su versatilidad y utilidad (a través de sus propiedades y estimación de vida), conocer opciones para la conversión, softwares que lo abre, lo visualiza, lo archiva, permite consulta, interactuación, etc. Saber dónde ha sido o está siendo mantenido. Aprender a seleccionar los más adecuados atendiendo a una serie de criterios. Conocer si es avalado por un estándar, Etc.

[7] Disponible en: http://www.archives.gov/records-mgmt/policy/transfer-guidance-tables.html#scannedtext
[8] Disponible en: https://www.loc.gov/preservation/resources/rfs/TOC.html

c) Validación de formatos, generando un perfil de cada formato y trabajando su viabilidad mediante herramientas de validación y de caracterización. Un perfil de formato describe tanto el formato preferido como el aceptado y en él se incorpora información numerosa sobre ambos formatos. Se incluyen elementos como riesgos y mitigación, licencias, etc.
d) Gestión del cambio de formatos, ante avances tecnológicos o de aplicaciones, mediante el empleo de estrategias de conversión, migración o emulación.

2- Veracidad e integridad del recurso

La integridad del recurso exige un continuado seguimiento desde la creación del recurso digital y el mantenimiento de dispositivos que aseguren la información. No obstante, es posible observar diferentes niveles de actuación, que son los siguientes.

a) Para proteger la información, se precisan acciones inmediatas a la creación del recurso, o al menos, ante la captura del mismo en un repositorio con garantías funcionales de gestión documental. Controlando volumen y metadatos del recurso y ante deficiencias detectadas, completando el etiquetado asociado a dicho recurso, con la creación de etiquetas que verifiquen la autenticidad de la información e integridad.
b) .El conocimiento del grado de veracidad debe realizarse mediante el control de aquellos recursos en su captura, asegurando que los originales no puedan ser modificados y controlando cualquier opción de ataque de virus informático para aquellos recursos supeditados a un alto riesgo.
c) En el repositorio o bien, en las aplicaciones donde se almacenan los recursos, debe establecerse un nivel de control de dichos recursos. En primer lugar, en el momento mismo de la ingesta, el control debe hacerse efectivo mediante operaciones de c*hecksum* y de validación de metadatos; aunque también, una vez ubicados en el repositorio, para asegurar su integridad y veracidad mediante informes periódicos. Además, se debería contar con dispositivos para detectar datos corruptos o posibles ataques.
d) Desde la óptica de reposición ante cualquier contingencia, la unidad de preservación debería asegurar el contenido replicado, encontrándose en condiciones de reponerlo en caso de corrupción o para dar respuesta a eventos específicos.

3 - Seguridad de la información

Se considera a la seguridad de la información estrechamente vinculada a la integridad y veracidad del recurso digital. Para su logro, deben implementarse esquemas nacionales de seguridad y aplicaciones que cumplan requisitos mínimos y que de algún modo nos permitan hablar de seguridad. Sin lugar a dudas, para su logro se trabaja de modo

denodado, sin embargo, la piratería informática, se esfuerza con idéntico ritmo. Por esta razón se produce una paradoja. A mayores esfuerzos, mayores prestaciones de seguridad, pero no es posible confirmar, mayores éxitos. No obstante, se debería trabajar sobre esta materia persiguiendo varios niveles de logro.

a) El primero, vinculado a la protección del recurso, exige identificar el recurso desde la perspectiva de usos, permisos y usuarios, facilitando o restringiendo su acceso, en atención a los niveles de acceso identificados y de restricciones delimitadas: consultar, modificar, eliminar o reutilizar pueden ser parámetros que debamos de emplear, agrupando a los usuarios en categorías precisas para lectura o consulta, modificación o interactuación con el recurso, eliminación o borrado del mismo, etc.
b) En segundo lugar, se hace necesario controlar a las categorías de usuarios y de tecnólogos para identificar quién tiene o no acceso a recursos y en qué modalidad.
c) Finalmente, se debería disponer de planes de actuación ante incumplimiento de seguridad de la información, además de considerar el control de permisos de actuación específica como puede ser el del preservador, el del informático, el de la entidad externalizada con la que trabajamos, etc.

4 - Gestión de metadatos

La gestión de metadatos es considerada una estrategia de preservación. Esto es, se debe de partir de que un objeto de datos sin la información de contenido no puede ser considerado un recurso autorizado u oficial. Recordemos que todo paquete de información (a transferir, a archivar o a consultar) debe de disponer de un amplio etiquetado que le identifique, que nos informe sobre qué es, quién es, cómo es, qué dice, con qué se ha creado, cuál ha sido su vida, dónde se ubica, por quién ha sido modificado, cuánto ha sido modificado, consultado, etc. En fin, el paquete de información de archivo ha de disponer de información suficiente para ser considerado documento autorizado, incluida aquella específica para su conservación (procedencia, fijeza. legal, tecnológica, etc.). Se debe de trabajar persiguiendo lo siguiente:

a) Por cada recurso digital, disponer de etiquetado suficiente para su localización e identificación, así como para organizar una copia de seguridad del mismo.
b) Trabajar para almacenar un conjunto de metadatos de naturaleza administrativa, tecnológica y aquellos vinculados a su historial de eventos y transformaciones sufridas (de conversión de formatos, de migración, de digitalización, de acceso, de modificación, etc.)

c) Se debe trabajar para gestionar aquellos metadatos técnicos y administrativos vinculados a su situación una vez ubicados en un e-depósito. Estos nos informarán sobre su situación actual, la cual será la base para trabajar otros avances tecnológicos y evitar, de este modo la obsolescencia del recurso.
d) El nivel máximo de seguridad de un fichero es que disponga de los metadatos de preservación, así como aquellos vinculados a la identificación del fichero o paquete de información, considerado como paquete de Archivo, ubicado en un repositorio. Al respecto, PREMIS es el estándar que mejor se adapta a su control y gestión.

5 - Almacenamiento y ubicación del recurso digital

El control del almacenamiento del recurso digital se realiza mediante depósitos electrónicos que cumplan determinadas garantías. El diseño de un depósito está normalizado mediante la norma UNE-ISO 14721:2015 (ISO: 2012) y su confiabilidad es posible verificarla mediante la norma ISO 16363:2012 (UNE-ISO: 2017). No obstante, y dada la vulnerabilidad y fragilidad del recurso es necesario adoptar ciertas garantías para su preservación. Para aquellos datos ubicados en aplicaciones donde se crean deberían considerarse requisitos funcionales y tecnológicos que permitan asegurar su almacenamiento y controlar su ubicación. Estas son las siguientes acciones que se deberían considerar.

a) Actuación de protección del recurso digital, mediante la existencia de dos copias, manteniendo original y réplica. Si se dispone de un e-depósito, puede contarse con otro distribuido, asegurando su copia. A menudo, cuando los recursos se ubican en servidores en las oficinas de negocio, la réplica en la nube puede ser una solución.
b) Un nivel de mayor seguridad es aquel que permite contar con una copia de seguridad o réplica de los contenidos en una ubicación geográficamente diferente. El entorno tecnológico de la nube o repositorios distribuidos en otras centros, vienen siendo las opciones más empleadas.
c) Un nivel de control mayor de los contenidos almacenados se consigue si se dispone de planes de prevención y de actuación ante desastres. Esto facilita el despliegue rápido de acciones para la recuperación ante cualquier contingencia, activando dispositivos y alertas ante cualquier obsolescencia de formatos, soportes, etc. Al respecto.
d) Finalmente, para aquellos recursos calificados de esenciales, sería preciso disponer de un plan de almacenamiento de máxima seguridad con 3 replicaciones en ubicaciones diferenciadas, así como planes activados de actuación ante desastres.

5 A modo de conclusión

Se han señalado suficientes amenazas para preocuparse por la preservación, tanto desde la óptica de dar mayor importancia a la parte por el todo (digitalización, tecnologías, etc.) como a la de formar y normalizar en preservación.

La vulnerabilidad del recurso exige trabajar con métodos y técnicas de gestión del riesgo y adoptar principios de cooperación para investigar y actuar.

La naturaleza y alcance preservador han mutado respecto al concepto tradicional de conservar, debido a la mudanza en el objeto y en el entorno de trabajo, aunque también, a los cambios percibidos en el usuario, tanto desde el enfoque de sus necesidades informativas, como desde el propiamente delimitador de cada comunidad específica en el tiempo.

La planificación, sistematización de los procesos, programación de acciones preservadoras y desarrollo de instrumentos es esencial para lograr una preservación sostenible.

Finalmente, mediante la sensibilización, información y formación será posible disponer de un profesional capacitado con un perfil necesario para un nicho de mercado en alza en la Agenda digital de los Estados.

Bibliografía

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN (AENOR)**. UNE ISO 30300 Información y documentación. Sistemas de gestión para los documentos. Fundamentos y vocabulario**. Madrid, 2011. (NBRS ISO 30300:2016)

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN (AENOR)**. UNE ISO 30301 Información y documentación. Sistemas de gestión para los documentos. Requisitos**. Madrid, 2011. (NBRS ISO 30301:2016)

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN (AENOR)**. UNE-ISO/TR 18128 Información y documentación. Apreciación del riesgo en procesos y sistemas de gestión documental**. Madrid. 2014.

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN (AENOR)**. UNE-ISO/TR 14721 Sistemas de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS). Modelo de referencia**. Madrid.2015.

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN (AENOR)**. UNE-ISO 14641-1 Archivo electrónico. Parte 1: Especificaciones para el diseño y funcionamiento de un sistema de información para la preservación de información digital**. Madrid.2015.

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN (AENOR)**. UNE-ISO 15489-1 Información y documentación. Gestión de documentos. Parte 1: Conceptos y principios;** Madrid.2016
.

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN (AENOR)**. UNE ISO 16175-1 Información y Documentación—Principios y requisitos funcionales para los documentos en entornos de oficina electrónica. Parte 1. Principios.** Madrid. 2012

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN (AENOR)**. UNE-ISO ISO 16175-2 Información y Documentación- Principios y requisitos funcionales para documentos en entornos de oficina electrónica. Parte 2: Directrices y requisitos funcionales para sistemas que gestionan documentos electrónicos.** Madrid. 2012

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN (AENOR)**. UNE-ISO 16175-3 Información y Documentación- Principios y requisitos funcionales para documentos en entornos de oficina electrónica. Parte 3 Directrices y requisitos funcionales para documentos electrónicos**. Madrid. 2013

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN (AENOR)**. UNE-ISO 23081-1 Información y Documentación. Procesos de gestión para los documentos. Metadatos para los documentos. Parte 1- Principios.** Madrid. 2006

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN (AENOR)**. UNE-ISO 13028 Información y documentación. Procesos de conversión y migración de documentos digitales** Madrid. 2012

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN (AENOR)**. UNE-ISO 13008 Información y documentación. Proceso de digitalización**. Madrid: 2010.

BUSHEY, G., DEMOULIN, M., HOW, E. y MCLELLAND, R. Lista de verificación para los contratos de servicio en la nube. Versión final. 2016. Accesible en: <https://interparestrust.org/assets/public/dissemination/ABAITRUSTNA14_FINAL_checklist_julio-29_2016TRAD.AB_.pdf>.

ENUMERATE **Survey Report on Digitization in European Cultural Heritage Institutions**. Comisión Europea. (*Elaborado por STROEKER, N. y VOGELS, R.*). 2014. Accesible en: <http://www.enumerate.eu/fileadmin/ENUMERATE/documents/ENUMERATE-Digitisation-Survey-2014.pdf>

CRUZ MUNDEZ, J.R. y DÍAZ CARRERA, C. **Los costes de la preservación digital permanente**. Gijón: TREA, 2016.

ESPAÑA. Dirección de Tecnologías de la Información y Comunicación. **Código de Administración Electrónica**. Madrid. Boletín Oficial del Estado. 2016.

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN (ISO). ISO/IEC 27036-4 **Information technology. Security techniques. Information security for supplier relationships. Part 4: Guidelines for security of cloud services.** Ginebra.2016.

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN (ISO). **ISO/16363 Space data and information transfer systems. Audit and certification of trustworthy digital repositories**. Ginebra, 2012.

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN (ISO **ISO/TR 17068 Information and documentation - Trusted third party repository for digital records.** Ginebra, 2012.

ORGANIZACIÓN INTERNACIONAL DE NORMALIZACIÓN (ISO). **ISO/27001 Information technology- Security techniques- Information security management systems- Requirements**. Ginebra, 2013 (2015 cor.)

TERMENS, M. **Preservación digital.** Barcelona: Editorial UOC; 2013.

THURSTON, A.: Keynote. Digitization and Preservation. Proceedings of the Memory of the World in the Digital Age: Digitization and Preservation. En **International conference on permanent access to digital documentary heritage***,* 26-28 September 2012. Vancouver, UBC. Canada. Edited by Luciana Duranti and Elizabeth Shaffer (UNESCO, 2013), pp. 31-37.

VOUTSSÁS M. J. **Cómo preservar mi patrimonio digital.** México: UNAM, IIBI. 2013.