Biblios
ISSN 1562-4730 (online)

Requisitos para a valoração de riscos de preservação em repositórios digitais

Grettel Ravelo Díaz
Mayra Marta Mena Mugica
Jorge del Castillo Guevara
Universidad de La Habana – UH, Cuba

REVIEW

Resumen

Objetivo. El presente artículo se propone abordar de manera suscinta algunas consideraciones teóricas en torno a la preservación y la gestión de riesgos en repositorios digitales. En este sentido, se presentan tres experiencias internacionales clave, orientadas a la valoración de riesgos en ambiente digital, para luego ofrecer un conjunto de requisitos generales que deberían tenerse en cuenta para la valoración de riesgos de preservación en repositorios digitales
Método. Se utilizó el análisis documental clásico de una extensa bibliografía especializada sobre el tema que se aborda en este artículo. Asimismo, el análisis documental clásico fue de gran utilidad para la comprensión de las tres experiencias internacionales de valoración de riesgos en repositorios digitales que se presentan.
Resultados. El principal resultado fue un conjunto de diez requisitos generales que deberían tenerse en cuenta para la valoración de riesgos de preservación en repositorios digitales.
Conclusiones. Los resultados obtenidos permiten valorar la confiabilidad, autenticidad e integridad de sus recursos a través de la identificación de amenazas en los componentes de su sistema, su comunidad de usuarios y su ambiente organizacional.

Palabras-claves

Gestión de riesgos; Preservación digital; Repositorio digital.

Requisites for assessing preservation risks on digital repositories

Abstract

Objective. The present article approaches in a succinct way to some theoretical considerations about the preservation and the risk management in digital repositories. In that sense, three key international experiences are presented, in order to assess risks in the digital environment and to offer a set of general requirements that should be taken into account for the assessment of preservation risks in digital repositories.
Method. We used the classic documentary analysis of an extensive specialized bibliography on the subject. Likewise, the classic documentary analysis was very useful for the understanding of the three international experiences of risk assessment in digital repositories that are presented.
Results. The main result was a set of ten general requirements that should be taken into account for the assessment of preservation risks in digital repositories.
Conclusions. The results obtained make it possible to assess the reliability, authenticity and integrity of your resources through the identification of threats in the components of your system, your community of users and your organizational environment.

Keywords

Digital Preservation; Digital Repository; Risk Management.

1 Introducción

Cómo mantener los objetos digitales y preservar su contenido informativo durante su vida útil es una de las interrogantes más frecuentes en la actual sociedad de la información, donde la veracidad de los documentos constituye un aspecto medular para un entorno de trabajo seguro. En el ambiente digital, los aspectos relacionados a la calidad de la información y los documentos se encuentran seriamente amenazados, fundamentalmente, por la manera en que se manifiestan sus componentes en ese entorno. Al decir de Duranti (2010) la principal divergencia con respecto al documento tradicional es que sus componentes se almacenan en diferentes partes del medio y que no existe como objeto físico, al no ser que se genere intencionalmente, además de la multiplicidad de maneras con que se manifiestan los elementos de forma documental.

La creciente producción de información digital y el uso de tecnologías que se encuentran en constantes modificaciones y actualizaciones, requieren eficientes sistemas de gestión, preservación y acceso a los recursos electrónicos. Es por ello que diseñar e implementar estrategias pertinentes de control de amenazas y gestión de riesgos, fundamentalmente en repositorios digitales, se ha convertido en uno de los eslabones principales para la preservación.

La poca “cultura de identificación y valoración de riesgos de preservación digital” en Latinoamérica ha sido una dificultad inquietante dentro de organizaciones que, según Llueca (2014, p. 1), aspiran a sanar sus “jaquecas digitales” de manera permanente. Elementos como la confiabilidad, autenticidad y accesibilidad de los recursos almacenados en repositorios digitales se ven amenazados constantemente por sucesos legales (por incorrecta manipulación, eliminación indiscriminada de información, fraude), medioambientales, tecnológicos, entre otros que, en la mayoría de los casos, no son detectados a tiempo y provocan perjuicios irreparables.

En tal sentido Reed y Gordon (2010) identificaron como aspecto clave el mantenimiento de la integridad de los documentos y la información, principalmente la preservación de aquella que se considera esencial para la organización. La esencia de este enfoque radica en el reconocimiento del valor de esa información como un activo que es parte del capital intelectual de las organizaciones (ISO 30300, 2011; ISO 15489-1, 2016).

Es por ello que las auditorías basadas en métodos de preservación digital deben ser de primordial interés en organizaciones comprometidas con garantizar un ambiente operacional razonablemente seguro. Por lo tanto, la realización de diagnósticos para detectar cualquier tipo de dificultad en los instrumentos de preservación, facilita tomar decisiones con eficiencia y trazar estrategias acertadas, en aras de ofrecer un ambiente de trabajo en el que las personas puedan confiar.

Sin embargo, esos diagnósticos necesitan tener en cuenta, de antemano, los requisitos necesarios para que los sistemas de almacenamiento puedan gestionar información de calidad. En este trabajo se propone un conjunto de requisitos para la valoración de riesgos de preservación de documentos en repositorios digitales. Para esta propuesta se utilizaron como referencias tres experiencias de gran aceptación en el contexto internacional:

- Trusted Digital Repositories: Attributes and Responsabilities, creado por el Research Libraries Group (RLG).
- Digital Repository Audit Method Based on Risk Assessment, conocido por (DRAMBORA) y creado por el Digital Curation Center (DCC) y el Digital Preservation Europe (DPE).
- Audit and Certification of trustworthy digital Repositories, o Libro Magenta, creado por el Consultative Committee for Space Data Systems (CCSDS).

Las mismas presentan una perspectiva abarcadora, pues toman en cuenta no solo al documento en sí, sino el contexto del que forma parte, la comunidad y todos aquellos elementos que influyen en él. Por otra parte, se basan en un enfoque orientado a la gestión de riesgos como principal proceso en la preservación digital.

Otro elemento a considerer, es que permiten comparar y cuantificar riesgos según el nivel de impacto en el sistema, y establecen las relaciones entre los riesgos y las áreas afectadas. Además, posibilitan la realización de un diagnóstico del estado del repositorio al tomar como indicadores, además del estado de los documentos

digitales, la infraestructura que lo soporta, el personal que lo administra, su documentación legal y regulatoria, la satisfacción de las necesidades de sus usuarios y otros de carácter administrativo como el presupuesto asignado al mantenimiento del repositorio y la infraestructura. También prestan especial atención a los aspectos relacionados con la confiabilidad y la autenticidad de la información, sobre la base de la gestión de riesgos y seguridad del sistema, así como la planificación estratégica.

2 Metodología

Para arribar a la propuesta de requisitos, se realizó un análisis documental, a partir de una extensa revisión bibliográfica, lo cual permitió establecer un marco teórico y conceptual sobre el tema en cuestión, así como identificar las principales experiencias que lograron establecer una relación más sólida entre la preservación digital y la valoración de riesgos. El análisis documental también permitió identificar los aspectos esenciales de las metodologías seleccionadas para el desarrollo de la propuesta.

3 La preservación y gestión de riesgos en repositorios digitales

Existen disímiles criterios sobre lo que es en sí un repositorio digital, pero las nociones encontradas no difieren en su esencia unas de otras. Una de las más acertadas plantea que es un sistema complejo e interrelacionado, que conduce a la gestión de documentos en formato digital y debe contener el tratamiento de los riesgos y su constante monitoreo, planificación y mantenimiento, así como la implementación de estrategias y acciones que permitan llevar a cabo su misión de preservación digital (National Archives and Records Administration, 2007).

Asimismo, el CCSDS (2011) expresa que un repositorio confiable debe permitir la realización periódica de auditorías para evaluar el estado de sus objetos digitales y el sistema sobre el cual se soporta. Tales diagnósticos deben estar basados en modelos o estándares que provean las pautas para la seguridad del sistema y de la información digital, el establecimiento de los roles y responsabilidades del personal encargado del repositorio, el compromiso de los depositantes para la incorporación de recursos y la diseminación adecuada de la información.

En tal sentido, un repositorio digital confiable debe tener la capacidad de preservar y gestionar recursos digitales auténticos, íntegros y confiables para su acceso, sobre la base de un enfoque de gestión de riesgos, a lo largo del ciclo de vida de tales recursos. Estos elementos se garantizan, según lo sugerido por el DCC/DPE (2007) por medio de: (a) la documentación como evidencia (los objetivos, el diseño, las especificaciones y la implementación del repositorio deben ser apropiadamente documentada), (b) transparencia (expone los riesgos y permite informar a los usuarios y organizaciones afines acerca de las decisiones tomadas respecto al repositorio), (c) competencia (el repositorio debe cumplir con todas las tareas para las que el mismo está diseñado dentro de su contexto), (d) medición (el repositorio puede evaluar la efectividad de la planificación para su preservación y controlar los objetivos y metas por medio de indicadores de confiabilidad).

La preservación es una categoría inevitable en cualquier abordaje sobre los repositorios digitales, toda vez que estos, independientemente del tipo de información que contengan o los procesos a los que tributen, deberían tener la capacidad de preservar sus recursos informacionales de manera segura a lo largo del tiempo. Sin embargo, este es un tema verdaderamente complejo, por lo que autores como Proscovia (2013) incisten en la necesidad de un acercamiento holístico y proactivo sobre este proceso.

Desde la perspectiva de la gestión documental, la preservación, en específico, en ambiente digital, según Rothenberg (1995, c.p. Candás, 2006, p. 128), está relacionada con "…un conjunto de procesos dirigidos a conservar la información en formato digital cuyo propósito es permitir a los usuarios la recuperación, el acceso, la interpretación y el entendimiento de los documentos de forma significativa y válida."

Por su parte, Candás (2006, p. 128) la entiende como "…un conjunto de actividades, entre las que se incluye la conservación, y que están destinadas a que un objeto perdure el mayor tiempo posible en su estado original, preocupándonos no sólo por el mantenimiento del objeto, sino también (y principalmente) por su contenido informativo."

Como bien afirma el precitado autor, la preservación en ambiente digital estará orientada no solo al objeto físico, o sea, al soporte, toda vez que este solo forma parte del contexto tecnológico de los documentos, a diferencia de lo que ocurre en un entorno físico, sino que debe prestar mayor atención a la información contenida en él. El desafío radica en cómo crear y mantener información digital presumiblemente auténtica y confiable, garantizar su diseminación, disponibilidad y acceso a lo largo del tiempo. Para ello, se hace necesario acudir a un proceso de comprensión y manejo de eventos que pueden constituir amenazas a la identidad de las organizaciones, así como al cumplimiento de sus objetivos y metas: se refiere a la gestión de riesgos (CIMA, 2008).

Esos eventos que constituyen amenazas se consideran, propiamente, riesgos. La norma ISO 31000 (2009, p. 1) los define como "…un efecto de incertidumbre sobre los objetivos…" Esta noción incluye aquellos relacionados con la tecnología, los efectos climatológicos, el desconocimiento, entre otros. Delgado (2011, p. 63) desde un enfoque basado en estudios de identificación y valoración de riesgos argumenta que su gestión permite "…prevenir pérdidas, mejorar el funcionamiento de las actividades de una organización, la calidad de sus productos y servicios, así como su seguridad". Precisamente, la gestión de los riesgos puede considerarse un subsistema en el marco de la preservación de información en ambiente digital. En torno a esta apreciación Gilliland (2000, p. 38) apunta que la gestión de riesgos "tiene implicaciones para ponderar el riesgo en términos de asegurar la fiabilidad y la autenticidad, así como la correcta eliminación y preservación de la información digital". En este sentido Lemieux (2010) ha insistido en la importancia de abordar esta categoría en relación con la gestión documental, para enfrentar riesgos relacionados con eventos no deseados como fraude y corrupción, lo cual puede conllevar al fracaso organizacional. Es por ello que la preservación, desde el ámbito de la gestión documental, es un proceso esencial en la gestión de riesgos relacionados con el manejo y uso de la información que se genera en formato digital.

En esta línea de pensamiento, el DCC/DPE (2007) asegura que la preservación digital es hoy día frecuentemente definida como un ejercicio de gestión de riesgos donde el propósito es convertir la incertidumbre acerca del mantenimiento de la usabilidad de los objetos digitales auténticos dentro de riesgos cuantificables. Esta visión es apropiada y oportuna al mismo tiempo, toda vez que si la preservación digital tiene como objetivo mantener la presunción de la veracidad de la información a lo largo del tiempo, el tratamiento de aquellos factores que suponen una amenaza en este sentido debe estar, necesariamente, implícito en toda política, estrategia o proceso de preservación digital.

4 Experiencias internacionales de preservación digital y gestión de riesgos

Antes de abordar las tres experiencias que se presentan en este trabajo, resulta necesario tener en cuenta el modelo de referencia conocido como Open Archival Information System (OAIS) desarrollado por la National Aeronautics and Space Administration (NASA) y convertido en norma ISO 14721 en el año 2003, para la especificación de requisitos y responsabilidades en torno a un sistema de archivo abierto, para la preservación a largo plazo de objetos digitales en una comunidad determinada.

Este modelo es la base sobre la cual estas se han desarrollado las experiencias que se abordan en este artículo (Audit and Certification of trustworthy digital Repositories, Trusted Digital Repositories: Attributes and Responsabilities y Digital Repository Audit Method Based on Risk Assessment). Ciertamente, el modelo presenta un conjunto de características que lo hacen apropiado para su utilización en diferentes aplicaciones orientadas a la preservación en ambientes digitales. Entre ellas, cabe destacar su concepción de "archivo" desde una perspectiva amplia toda vez que abarca diferentes tipos de ítems de información. Por otra parte, se orienta específicamente hacia la preservación a largo plazo. Otro elemento a considerar es su definición como sistema abierto, lo cual permite su utilización con independencia del sistema de almacenamiento.

El Open Archival Information System es un modelo de referencia creado con el objetivo de gestionar y preservar a largo plazo una cantidad concreta de materiales digitales y sus contenidos; ha sido adoptado en el ámbito global como "la iniciativa más completa para los grandes programas de preservación a largo plazo" (Rivera, 2009, p. 13).

Muchas herramientas y proyectos de preservación digital se han elaborado sobre la base de este modelo debido a que provee un vocabulario común para la discusión de los resultados acerca de lo que es el "archivo digital",

una descripción comprensiva de las partes funcionales y los roles de un archivo digital y no tiene restricciones para su implementación, es decir, permite que cada institución lo adecue a sus necesidades y realidad.

4.1 Trusted Digital Repositories: Attributes and Responsibilities

Creado por el RLG-OCLC en el año 2002, con el objetivo de investigar acerca de los atributos de un repositorio digital para organizaciones de investigación, establece un consenso sobre las características y las responsabilidades de los repositorios digitales confiables a larga escala, así como colecciones heterogéneas de diversas organizaciones. Propone, en un primer momento, definiciones de repositorios confiables en diferentes escenarios como bibliotecas nacionales o universitarias, museos, revistas virtuales e instituciones culturales pequeñas a partir de las colecciones que preservan y el contenido de los materiales. Con el propósito de adoptar una visión estándar de los principales atributos y responsabilidades de los repositorios digitales, el mismo se divide en: (1) Atributos de un Repositorio Digital Confiable, (2) Responsabilidades de un Repositorio Digital Confiable y (3) Certificación de Repositorios Digitales Confiables.

Esta experiencia, que es considera un reporte técnico, facilita la comprensión de las principales responsabilidades y los atributos de un repositorio y del personal encargado de su funcionamiento para mantener la confiabilidad de sus materiales. Aunque no hace un énfasis particular en la gestión de riesgos, propone que este debe ser llevado a la práctica en las instituciones a través de los planes de contingencia, de preservación y de seguridad del sistema.

El RLG esclarece los deberes del repositorio sobre la base del cumplimiento de los requisitos administrativos para la implementación de estrategias que reporten mejoras o modifiquen las funciones y operaciones del sistema; toma en consideración la viabilidad organizacional respecto a las políticas y procedimientos de preservación, almacenamiento y acceso a los recursos digitales; prioriza la superación del personal encargado; mantiene el balance de las inversiones, los beneficios y los gastos en los procesos de actualización de los componentes del sistema y sus recursos de información; y documenta todas las tareas y acciones realizadas por el repositorio para brindar evidencia y transparencia a la comunidad.

Al mismo tiempo, ofrece parámetros para distinguir si un repositorio ha establecido correctamente las responsabilidades de preservación de colecciones y sobre la gestión de los materiales digitales, desde la creación hasta el mantenimiento constante durante su ciclo de vida, sobre las operaciones a partir de su marco legal, sobre el control de los recursos, la disponibilidad de los mismos y la identificación de los usuarios. Además, hace referencia al cumplimiento de códigos de buenas prácticas y de normas establecidas por su comunidad, lo cual permitiría su certificación ante cualquier institución o estándar internacional.

4.2 Digital Repository Audit Method Based on Risk Assessment (DRAMBORA)

El método DRAMBORA, fue publicado en el año 2007, y constituye una de las herramientas claves de auditoría para repositorios digitales basada en la gestión de riesgos. Sus creadores, el Centro de Curaduría Digital y el comité de Preservación Digital de Europa, facilitan a los administradores y personal interno un conjunto de instrumentos, habilidades y conocimientos para llevar a cabo auditorías adaptables al contexto en el cual se encuentra insertado el repositorio digital. Este método, contó con un conjunto de auditorías pilotos en un rango diverso de organizaciones que incluyó bibliotecas nacionales, bases de datos científicas, archivos de datos culturales y de herencia en Europa. Además, posibilita la valoración de las capacidades de los repositorios, identificar sus debilidades y reconocer sus fortalezas a través de la valoración y la cuantificación de los riesgos de preservación digital.

El método en cuestión divide el análisis en seis etapas imprescindibles, comienza por la identificación del contexto organizacional, la documentación de las políticas y la estructura regulatoria por las que se rige el repositorio, la identificación de las actividades, valores y propietarios del repositorio, la identificación de los riesgos, la valoración de los riesgos, y concluye con la gestión de los riesgos para la posterior toma de decisiones y el diseño de las estrategias. Ello proporciona un patrón organizado para la detección de amenazas y la solución de los problemas.

4.3 Audit and Certification of Trustworthy digital Repositories

El Libro Magenta, como también se le conoce, se considera una "recomendación práctica" propuesta por el CCSDS en el año 2011, que proporciona directrices para la identificación de problemas en los contenidos y componentes de los repositorios digitales. Está basado en el Modelo de Referencia OAIS y constituye un proceso de auditoría y certificación para la estimación de confiabilidad de los repositorios. Escoge como referencia principal la metodología Trustworthy Repositories Audit and Certification Criteria: criteria & checklist (TRAC) del RLG que aporta una visión más actualizada de la misma respecto a los cambios en la tecnología y en las llamadas "comunidades designadas" cuya definición es tomada de OAIS (CCSDS, 2002, p. 10) y no es más que "un grupo identificado de consumidores potenciales que son capaces de entender un conjunto particular de información". La misma está dividida en tres partes principales: (1) Infraestructura organizacional, (2) Gestión de objetos digitales y (3) Infraestructura y gestión de riesgos de seguridad.

Este instrumento de auditoría y certificación permite crear una visión más abarcadora acerca de la función del repositorio, parte del comportamiento organizacional, la sustentabilidad financiera, la experiencia y las habilidades del personal encargado de la administración y gestión de los objetos digitales, desde el momento de la adquisición y la creación de los metadatos hasta el almacenamiento y la planificación de estrategias de preservación. Asigna a cada sector de la organización los indicadores que deben ser analizados en el proceso de auditoría y qué parámetros se deben cumplir para garantizar la confiabilidad del repositorio.

Asimismo, centra su atención en la relación que se establece entre el repositorio y todas las partes que intervienen en su funcionamiento, lo cual delimita así el rol del productor, del contribuidor, del administrador y del usuario, y le otorga mayor importancia a la existencia y conservación de contratos, acuerdos legales de depósito y derechos de propiedad intelectual. Explica, además, la necesidad de los planes de contingencia y de preservación para la gestión de los riesgos de infraestructura técnica del sistema en general y plantea que la solución eficaz para obtener una visión anticipada de estimación de riesgos es la auditoría y la revisión regular del estado financiero, las habilidades del personal y las prácticas de gestión de los objetos digitales, a través de herramientas como DRAMBORA o de expertos internos o externos a la organización.

5 Propuesta de requisitos para la valoración de riesgos de preservación en repositorios digitales

La siguiente propuesta tomó como punto de referencia las tres experiencias presentadas en el acápite anterior. El análisis minucioso de cada una de ellas permitió crear un conjunto de 10 requisitos generales que deberían tenerse en cuenta en todo proceso de valoración de riesgos de preservación en ambientes digitales.

5.1 Establecer los objetivos, metas, visión y misión del repositorio

Para solucionar las denominadas amenazas en la reputación de la entidad y su repositorio, es imprescindible que los miembros de la organización y la comunidad de usuarios conozcan su papel, lo que implica conocimiento acerca del tipo de repositorio, y qué se espera de él, los objetivos que se propone a corto, mediano y largo plazo para desarrollar una adecuada estrategia que permita alcanzarlos de manera eficiente. Sobre la base de estos aspectos se hace posible definir los servicios del repositorio, su alcance y desempeño, para lo cual es necesario incluir dentro de sus principales metas el compromiso de llevar a cabo la preservación a largo plazo para el acceso a sus recursos digitales.

5.2 Identificar y designar su comunidad de usuarios, recursos y productores

Es necesario tener total claridad respecto al tipo de usuario para el que estará diseñado, y sus necesidades de información. En tal sentido se hace necesario conocer además: qué información le interesa transmitir, tipos de recursos a adquirir, cuáles serán sus principales productores y proveedores, ya sean instituciones o individuos en correspondencia con sus temáticas de interés, y qué otras organizaciones afines poseen un repositorio con información similar. Esto permite solucionar problemas relacionados con las expectativas del usuario respecto a la búsqueda y el acceso a la información que necesita, la disponibilidad de recursos actualizados y el pleno conocimiento de aquellos objetos digitales que componen el repositorio y el control de la producción científica en los procesos de adquisición e incorporación.

5.3 Apoyar financieramente el repositorio por la organización u otras instituciones vinculadas

Debido a la evolución constante de la infraestructura tecnológica y de las crecientes necesidades de información e intereses de los usuarios, es primordial contar con una base financiera que permita la actualización y mantenimiento de los componentes del software. Esto contribuye a que no se detenga el proceso de incorporación de nuevos materiales de diversos tipos o formatos, así como la renovación de infraestructura obsoleta, lo cual garantiza mantener en funcionamiento constante el repositorio.

5.4 Conocer el marco regulatorio y los requerimientos legales del repositorio

El desconocimiento del marco regulatorio, de las disposiciones legales y administrativas que forman parte del ambiente jurídico del repositorio, ponen en riesgo el comportamiento del personal y del propio usuario. El repositorio debe ajustarse a las regulaciones establecidas en el país o localidad donde está insertado, cumplir con las normas nacionales e internacionales que de alguna manera están relacionadas con las funciones que realiza, así como con las normativas internas de la organización y los compromisos éticos para el manejo de la información. Los repositorios institucionales se encuentran embebidos en un entramado de reglas de funcionamiento en las cuales se establecen requisitos de obligatorio cumplimiento. Por otra parte, es necesario contar con manuales y procedimientos sobre el uso y funcionamiento del sistema en cuestión.

5.5 Determinar el personal administrativo y de apoyo requerido

El personal que interviene en cada uno de los procesos del repositorio, desde su diseño, creación, adquisición de recursos, mantenimiento y gestión de los mismos, debe contar con las competencias y habilidades esenciales para el manejo del mismo. La capacitación constante debería estar incluida en los planes de desarrollo de los especialistas. También debe conocer y cumplir con las normas técnicas, regulaciones y códigos de ética profesional.

5.6 Definir los procesos de forma precisa, así como las acciones por cada proceso

Este requisito se orienta a todos los procesos que van, desde la adquisición de los recursos, hasta el acceso a los mismos. A partir del análisis de las herramientas estudiadas se recomienda tener en cuenta los procesos siguientes: adquisición, incorporación, almacenamiento, preservación, gestión de metadatos, acceso y diseminación. Es necesario definir los requisitos para cada uno de ellos. Por ejemplo: en la adquisición se debe determinar qué información necesita el repositorio y su orientación hacia su comunidad de usuarios. Esto permitirá una adecuada selección de los recursos que serán insertados. La incorporación, el almacenamiento, la preservación y la gestión de metadatos son procesos muy relacionados, de los cuales se derivará la capacidad del repositorio de mantener la veracidad de la información.

Es imprescindible contar con una estrategia para la gestión de metadatos. De este aspecto depende, en mayor medida, que pueda cumplir su funcionalidad y combatir amenazas que podrían surgir como la destrucción y duplicidad de documentos, almacenamiento incorrecto, entre otras. Todo repositorio debería definir de antemano sus perfiles de acceso, según las responsabilidades y competencias de cada usuario. Finalmente, la diseminación dependerá del conocimiento exhaustivo de las necesidades de su comunidad para ofrecer información pertinente, oportuna, relevante y actualizada.

5.7 Implementar estrategias de preservación

Se deben implementar programas y estrategias de preservación digital. Estas deberán estar orientadas, no solo al mantenimiento del *hardware*, o sea, de los dispositivos físicos, sino a la preservación de la información que se gestiona en las bases de datos, así como de sus metadatos, los cuales deberán tener un peso importante en cualquier estrategia de preservación digital toda vez que los mismos permiten, además de la recuperación de la información, la representación de sus contextos de creación.

Se tendrán en cuenta los requisitos para la creación, captura, manejo y control de la información, además de contar con procedimientos para la pérdida, corrupción y su manipulación indebida. La obsolescencia tecnológica debe ser un aspecto a considerar a la hora de elaborar procedimientos y políticas de preservación. Por otra parte, los planes de contingencia y de preservación deben estar orientados a la salvaguarda de los recursos digitales y deben reflejar los resultados que provienen del chequeo periódico de la organización, para poner en

práctica las estrategias en caso de amenazas debido a fenómenos naturales o de seguridad digital, que puedan provocar la interrupción accidental del sistema.

5.8 Establecer las estrategias de identificación y gestión de riesgos

Se considera que la única manera de identificar los riesgos de preservación en un sistema es el monitoreo constante del estado de los recursos y los componentes. Esta estrategia de control también puede estar reflejada en el plan de preservación de la organización, tomando como apoyo las herramientas que existen para la cuantificación de los mismos, como por ejemplo DRAMBORA. Este chequeo para la detección de riesgos potenciales dentro del sistema se realiza con el objetivo de evitar afectaciones en su funcionamiento, a partir de soluciones concretas para cada tipo de riesgo identificado, sobre la base de las propuestas que plantean las metodologías para la mitigación de los riesgos de preservación digital y la seguridad informática.

5.9 Realizar auditorías frecuentes a la organización y al sistema

Las auditorías permiten conocer el estado de funcionamiento del sistema, verificar si responde a los intereses de su comunidad y si se están cumpliendo los objetivos planteados. Asimismo, ofrece resultados que contribuyen a la modificación o trasformación de los servicios, la evaluación de los recursos, del personal, del estado de los componentes del sistema, de la manipulación de los objetos, de la calidad de los servicios y permite la búsqueda de soluciones y la toma de decisiones ante cualquier problema que presente la organización. Las auditorías pueden ser tanto internas como externas, pues ambas cumplen un importante papel en este sentido.

5.10 Proveer el acceso transparente a sus recursos y su documentación normativa

La transparencia en estos sistemas de información es vital para brindar un entorno de intercambio en el que las personas puedan confiar. Un ambiente de opacidad y asimetría informacional podría crear un marco para la corrupción administrativa, por medio del ocultamiento o eliminación documental para beneficio personal. Sobre esta línea de pensamiento se hace necesario minimizar la incertidumbre que genera un sistema que manipula información de carácter público de forma inadecuada, para garantizar la responsabilidad en cuanto a la gestión del repositorio.

Un aspecto clave, por tanto, es el acceso a la información, sin esto no es posible saber si el repositorio cumple a cabalidad con los objetivos para el cual ha sido diseñado e implementado. Tampoco será posible conocer si respeta los requisitos que se establecen en las normativas jurídicas del país o localidad, así como de otras regulaciones, normas técnicas y códigos de buenas prácticas.

Se hace necesario tener pleno conocimiento sobre su misión, visión, objetivos y metas y todos sus recursos digitales disponibles, así como otros temas de interés para el usuario y el personal respecto a la identidad de los productores, las organizaciones asociadas y principales inversores, las organizaciones valoradas como competencias y el acceso al fondo documental de la organización. También es necesario tener plena claridad sobre cada uno de los procesos llevados a cabo por el repositorio, y la documentación que surja como resultado de los mismos.

6 Consideraciones finales

Los problemas asociados con la dificultad de preservar la veracidad de la información generada y mantenida en repositorios digitales suponen diversos tipos de riesgos para las organizaciones, relacionados fundamentalmente con la tecnología, el personal y las dificultades financieras, entre otros; por lo que la gestión de los mismos debería ser una prioridad para aquellas instituciones que utilizan este tipo de recursos de información.

Con la constante evolución de las tecnologías, el incremento de la producción documental y los crecientes intereses y necesidades de información de las comunidades de usuarios, la valoración de riesgos ha sido una solución para algunas organizaciones que han comprendido la necesidad de aplicarla, con el objetivo de garantizar un ambiente de trabajo en el que sea posible confiar. Por ello, la implementación de estrategias de preservación basadas en auditorías para la valoración de riesgos en repositorios digitales es, actualmente, un proceso que necesita ser introducido y generalizado a nivel internacional, a partir de experiencias que se consideran clave en este sentido.

Como resultado del análisis realizado a tres experiencias internacionales de auditoría de repositorios digitales y un conjunto de indicadores aportados por ellas, se han identificado diez requisitos generales para la valoración de riesgos de preservación digital aplicables a cualquier contexto social. Estos permiten valorar la confiabilidad,

autenticidad e integridad de sus recursos a través de la identificación de amenazas en los componentes de su sistema, su comunidad de usuarios y su ambiente organizacional.

Referencias

Candás, J. (2006). El papel de los metadatos en la preservación digital. *El profesional de la Información, 15* (2), 126-136.

Chartered Institute of Management Accountants CIMA. (2008). *Fraud Risk Management: A Guide to good practice.* Australia: H. Doody.

Consultative Committee for Space Data Systems CCSDS. (2002). *Reference Model for an Open Archival Information System (OAIS). Estados Unidos.*

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

Delgado, A. (2011). Normativa de referencia. *Administración de documentos y archivos: Textos fundamentales* (pp. 37- 65). España: Coordinadora de Asociaciones de Archiveros CAA.

Digital Curation Centre DCC /Digital Preservation Europe DPE. (2007). *Digital Repository Audit Method Based on Risk Assessment (DRAMBORA) 1.* Holanda.

Duranti, L. (2010). Concept and principles for the management of electronic records, or records management theory is archival diplomatics. *Record Management Journal*, 20 (1), 78-95.

Gilliland-Swetland, A. (2000). *Un paradigma perdurable, nuevas oportunidades: el valor de la perspectiva archivística en el entorno digital* (A. Delgado, Trad.). Washington, EE.UU.: Council on Library and Information Resources

ISO 31000 (2009) Risk management: Principles and guidelines.

ISO 30300 (2011) Information and documentation—management system for records—fundamentals and vocabulary.

ISO 15489-1 (2016) Information and documentation—records management—concepts and principles.

Lemieux, V. (2010). The records-risk nexus: exploring the relationship between records and risk. *Records Management Journal*, 20 (2), 199-216

Llueca, C. (2014). Preservación digital. *Revista Española de Documentación Científica, 37* (1).

National Archives and Records Administration. (2007). *Trustworthy Repositories Audit & Certification: Criteria and Checklist*. EE.UU.: Research Library Group RLG.

Proscovia, S. (2013). Enterprise content management and records continuum model as strategies for long-term preservation of digital information. *Records Management Journal*, 23 (3), 159-176

Rivera, M.A. (2009). Directrices para la creación de un programa de preservación digital. *Serie Bibliotecología y Gestión de Información*, no. 43. Universidad Tecnológica Metropolitana

Research Library Group RLG. (2002). *Trusted Digital Repositories: Attributes and Responsibilities*. EE.UU.

Datos de los autores

Grettel Ravelo Díaz

Licenciada em Ciencias de la Información y maestrante en Bibliotecología y Ciencias de la Información en la Facultad de Comunicación de la Universidad de La Habana. Especialista en Procesamiento y Análisis de Información de la Empresa de Servicios de Información para el Transporte.

grettel@inf.sitrans.transnet.cu

Mayra Marta Mena Mugica

Doctora en Ciencias de la Información y profesora titular de la Facultad de Comunicación de la Universidad de La Habana.

mmena@infomed.sld.cu; mmena@fcom.uh.cu

Jorge del Castillo Guevara

Licenciado em Ciencias de la Información y maestrante en Estudios Políticos y Sociales. Profesor asistente y Doctorante en Ciencias de la Información en la Facultad de Comunicación de la Universidad de La Habana.

guevara@fcom.uh.cu

Recibido - Received: 2017-07-18

Aceitado - Accepted: 2018-12-14