Revista Española de Documentación Científica
41(1), enero-marzo 2018, e193
ISSN-L:0210-0614. https://doi.org/10.3989/redc.2018.1.467

ESTUDIOS / *RESEARCH STUDIES*

¿Riesgos despejados? Estrategias proactivas como servicio en entornos de *Cloud Computing*

Manuela Moro-Cabero*, Dunia Llanes-Padrón**

*Departamento de Biblioteconomía y Documentación. Facultad de Traducción y Documentación. Universidad de Salamanca, España
Correo-e: moroca@usal.es | ORCID iD: https://orcid.org/0000-0001-5301-1924

**Departamento de Ciencias de la Información. Facultad de Comunicación. Universidad de La Habana, Cuba
Correo-e: dlp@yahoo.es | ORCID iD: https://orcid.org/0000-0001-8639-4706

Recibido: 07-03-2017; 2ª versión: 19-05-2017; Aceptado: 23-05-2017.

Cómo citar este artículo/Citation: Moro-Cabero, M.; Llanes-Padrón, D. (2018). ¿Riesgos despejados? Estrategias proactivas como servicio en entornos de *Cloud Computing*. *Revista Española de Documentación Científica*, 41 (1): e193. https://doi.org/10.3989/redc.2018.1.467

Resumen: Es una realidad insoslayable el incremento del uso de servicios de Cloud Computing en las organizaciones debido a las ventajas que conlleva. Los gestores de documentos deben adoptar una posición proactiva, asesora y comprometida ante el empleo de dichos servicios, caracterizados por cierta opacidad, fundamentada en el desconocimiento de su funcionamiento y regulación, hecho que suscita reticencias para su adopción. En el estudio, de naturaleza descriptiva y sustentado en un notable número de fuentes heterogéneas, se sistematizan las amenazas derivadas de la gestión y almacenamiento en dichos servicios, a la par que se establecen estrategias de actuación, tanto ante la concreción de acuerdos como para su contratación. Su finalidad es la de sensibilizar al profesional sobre su potencial labor asesora y de control para asegurar la continuidad digital y la preservación de los recursos documentales en la nube.

Palabras clave: archivos en la nube; servicios en la nube; riesgos; acuerdos de servicios en la nube; preservación en la nube.

Cleared risks? Proactive strategies as service in Cloud Computing contexts

Abstract: The increasing use of Cloud Computing services at organizations is an undeniable reality nowadays. Record managers must then adopt a proactive and compromised position, giving advice to users. However, as a consequence of lack of knowledge in the function and regulation of the field, the implementation of those services faces no little confrontation. This descriptive essay, supported by a relevant number of heterogeneous resources, systematizes the menaces of managing and storing information with these services. At the same time, the study establishes a set of action-strategies for both reaching and hiring agreements. The objective of the paper is, therefore, to make the professional aware of the potential of these services as assessing and controlling tools, as well as ensuring the digital continuity and the record resources preservation in the Cloud.

Keywords: records in the Cloud; services in the Cloud; Risks; agreement of services in the Cloud; preservation in the Cloud.

1. INTRODUCCIÓN

En la meteorología las nubes aportan gran información sobre los fenómenos que se suceden. La nube en el contexto tecnológico de la información es claramente representativa de las tendencias en los modelos de negocio y en consideraciones de gestión y almacenamiento de datos, información y documentos. Al almacenamiento de los recursos digitales de archivo le es inherente su conservación y su disponibilidad; esto es, su accesibilidad y usabilidad cuando estos se precisen. El empleo de servicios en entornos *Cloud Computing* (CC) comenzó manifestándose cortoplacista en cuanto a los intereses de gestión y de conservación de datos, si bien, dadas las ventajas que presenta y el constante incremento de los recursos nacidos digitales, su contratación resulta atractiva tanto para los productores como para los gestores de dichos recursos.

El gestor de documentos debe comprender tanto el alcance de *posibles cielos encapotados* en el entorno tecnológico del *Cloud Computing*, como las ventajas de contratar dichos servicios, pues ha de aprender a desplegar un conjunto de estrategias, para asesorar en gestión y almacenamiento de los datos. La preocupación del profesional se demuestra en algunos estudios donde se señalan amenazas y se desvelan oportunidades de actuación mediante actuaciones de asesoría y de control (CAARA, 2010; McKemminsh, 2013; Stancic y otros, 2013; Ostrzenski, 2013; Beagrie y otros, 2014).

El interés por comprender y difundir la experiencia en estos entornos se ha incrementado. Estudios (InterPARES3 project, 2013; Palma-Villalón, 2014), monográficos en la revista *The Canadian Journal of Information and Library Science* –CJILS, (2015) y estadísticas (Giannakouris y otros, 2016, ESPAÑA-Instituto Nacional de Estadística, 2016) así lo confirman. Una bibliografía anotada sobre el tema es recopilada bajo el patrocinio de *InterPARES Trust Project* (Bushey, How y McLelland; 2015). Ésta ha sido estructurada en cuatro áreas: enfoque legal de los servicios en la nube[1]; casos jurídicos[2]; perspectiva del servicio *cloud* desde la gestión de documentos electrónicos[3] y gestión de documentos[4]. Por otro lado, el monográfico de CJILS (2015, vol. 39, 2) incluye artículos sobre autenticidad, confiabilidad, portabilidad, continuidad de los datos o contratación. A su vez, el proyecto *InterPARES Trust* para el entorno CC ha generado un marco teórico y metodológico de apoyo para la formulación de políticas, despliegue de procedimientos, adopción de normas y legislaciones para el almacenamiento y acceso de datos y documentos en un entorno de nube (Jansen y Duranti, 2013; Park, 2015)[5].

Es una realidad insoslayable el incremento del uso de estos servicios en las organizaciones (Giannakouris, 2016[6]; Boletín INE, 2016[7]), debido a las ventajas que conlleva, destacando la facilidad para disponer la información en modalidades de servicio marcadas por la dispersión geográfica; la facilidad de uso, la oportunidad de contar con un respaldo de los datos o, en principio, la reducción de costes a la par que se incrementa su transparencia (Oliver y Knight, 2015). Esta disminución (relativa) es demediada por múltiples factores: nivel de servicio acordado, naturaleza y volumen de los recursos a almacenar y gestionar, tecnología requerida, etc. Para el contratante, se produce un cambio en los factores de coste, trabajando volúmenes de datos y servicios de bajada y subida de datos, frente a componentes operativos, de inversión tecnológica o de depreciación en el ciclo de vida (Brown y Fryer, 2014). Desde la e-administración pública, la nube favorece la consulta de una creciente ciberciudadanía. Además, tal y como recoge Borglund (2015), la nube aporta una oportunidad de no disponer de tecnologías informáticas reduciendo la inherente tiranía formativa, dada su obsolescencia[8]. Por otro lado, la seguridad, consustancial y regulada en estos sistemas, es atractiva para centros donde su implementación requiere esfuerzo, competencia y experiencia[9].

En el CC las opciones de servicio, modelos disponibles, fases, tipos, categorías y características son heterogéneas, a menudo, opacas para el gestor de la información y documentación de archivo, dificultando la apreciación del riesgo, las actuaciones derivadas para su mitigación y su apropiado rol asesor.

Considerando esta situación, en el presente estudio se formularon dos objetivos: sistematizar la relación de amenazas derivadas de la gestión y almacenamiento, y establecer estrategias proactivas. Su logro facilitará al gestor documental su labor asesora y de control para asegurar la continuidad digital y la preservación de los recursos documentales en la nube.

Para su alcance, el ensayo de naturaleza descriptiva y analítica se ha basado en la consulta, análisis y sistematización de un notable número de fuentes estadísticas, reglamentarias, normativas y especializadas (publicaciones periódicas, actas de congresos), así como informes y directrices, procedentes de Archivos Nacionales, constituyéndose en sí mismo un repertorio bibliográfico sobre el tema.

El estudio se estructura en cuatro apartados. Uno primero, define modelos, tipos y características de los servicios en entornos CC. El segundo, identifica el alcance y contenidos de las fuentes normativas

que sustentan el marco de servicios CC con la intención de apoyar al lector en su consulta y utilización, en caso necesario. En un tercer enunciado, se categorizan e identifican principales riesgos y, finalmente, se incorpora un acápite en el que se pautan estrategias para su gestión y mitigación.

2. ALCANCE DE LOS SERVICIOS EN UN ENTORNO CLOUD COMPUTING: MODALIDADES, TIPOS Y CATEGORÍAS

El epígrafe define el CC, especifica sus modalidades, tipología, categorías y características, como sigue:

2.1. Concepto

El CC es definido en su norma terminológica (ISO 17788, 2014) como "un paradigma para permitir el acceso en la red a un grupo escalable y flexible de recursos físicos o virtuales compartibles con aprovisionamiento de autoservicio y administración bajo demanda"[10]. Bajo el calificativo de "paradigma", se confirma un "nuevo modo de hacer o de producir", constatándose que la distribución virtual de cualquier recurso compartido que se provee a través de Internet (por el *proveedor del servicio*) delimita el concepto de servicio para el cliente (*contratante* del servicio).

2.2. Modelos y tipología

Los *modelos* de servicio (*o de autoservicio*) se reconocen atendiendo a dos enfoques: el de los profesionales TI o el del cliente. Respecto a los primeros, se identifican -considerando la infraestructura de la nube- dos modelos básicos de nube: pública (utilizada por una cantidad desconocida entre sí de clientes y donde el usuario transfiere el control de sus datos, reduciéndose las garantías de calidad del servicio, en cierto modo) y privada (en la que el cliente compra el uso exclusivo de la infraestructura de la nube, bien para empleo remoto, bien en el *sitio* de la nube, siendo administrado por él o por un tercero). La combinación de ambos modelos genera un tercero: nube híbrida (tanto pública, privada como *comunitaria,* empleada por clientes con dos tipos de datos e informaciones, que requieran privacidad en gradientes diferentes). La nube pública supone menor coste que la privada, debido al tipo de garantías en la compra de servicios. La nube híbrida se presenta como una opción intermedia para clientes con requisitos divergentes y recursos heterogéneos en cuanto a su sensibilidad o privacidad requerida. Esta última, donde se mixturan opciones de nube pública y privada es la tendencia. Además, se reconoce, igualmente, el modelo de nube cuya infraestructura beneficia a una comunidad específica que comparte requisitos y relaciones con otra y donde las relaciones son contratadas por uno de los miembros de dicha comunidad (ISO 17788: *community cloud*). Esto es, todos comparten el mismo servicio, permitiendo a los clientes tener conocimiento sobre quién está usando la infraestructura compartida. Hecho que no se produce en la opción pura de nube pública, pero que implica beneficios de coste de nube pública.

Desde un enfoque de cliente, se distinguen tres tipos de servicio de acceso mediante demanda: la provisión de software, de plataformas o de infraestructura. Estas modalidades de servicio pueden adoptarse de modo independiente o adaptarse a las necesidades del cliente, de acuerdo a sus preferencias y usos (*bajo demanda*). Atendiendo al tipo de solicitud y uso se conforma el acuerdo de nivel de servicio y la consiguiente estructura de pago que debe hacerse por los mismos. En cada uno de los servicios principales se reconocen ventajas e inconvenientes. Brevemente se perfilan cada uno de estos tipos, definidos en la norma ISO 17788 (2014).

El modelo *IaaS -Infrastructure as a Service* (enunciado 3.2.24 de la citada norma), permite al contratante alquilar infraestructura mediante la provisión de acceso al hardware (discos duros, servidores, etc.). Por tanto, se facilita la provisión y uso de recursos de procesamiento, almacenamiento y alojamiento masivo en servicios remotos o red. Se trata de la tercerización de equipos usados como soporte de operaciones de negocios: servidores, máquinas virtuales, almacenamiento, componentes de red. En este modelo, el suscriptor no controla la infraestructura de la nube aunque sí tiene el control sobre sistemas, almacenamiento, aplicaciones desplegadas y algunos otros aspectos de cortafuegos, etc. Por tanto, el desarrollador gana control detallado del entorno y aumenta su responsabilidad en su construcción y gestión. Se reconoce un coste constante en el mantenimiento de operaciones. Las categorías que en la norma se vinculan de modo más inmediato a dicho modelo, son las de almacenamiento de datos *(DSaaS- Data Storage as a Service)* y las de disposición de mayor potencia de red *(NaaS-Net Work as a Service).*

El modelo *SaaS -Software as a Service* (apartado 3.2.36, de la norma), permite al contratante el acceso remoto a software alojado en la infraestructura del proveedor. No siempre precisa gestionar licencias y asumir la responsabilidad de actualizaciones. Facilita las transacciones, al estar el software disponible desde varios dispositivos localizados de modo remoto. Un notorio inconveniente es que el suscriptor no controla la infraestructura ni el software. De este modelo la norma determina categorías de servicio centradas en la comunicación, permitiendo la interacción a tiem-

po real (*CaaS-Communication as a Service),* en el almacenamiento de datos *(Dsaas-Data Storage as a Service)* o en facilitar la conectividad y la capacidad de red *(NaaS-Net work as a Service).*

El modelo *Paas -Plataform as a Service* (apartado 3.2.20 de la norma), permite la provisión de alojamiento por el proveedor de servicio en el que el contratante pueda construir su propio software o implementar y ejecutar aplicaciones del cliente. Por lo tanto, se ofertan hardware, SOs, capacidad de red, almacenamiento de datos, sistemas de búsqueda y de disposición geográfica de los datos, facilitando, de este modo que no se produzcan descargas ni se disponga de instalaciones, eliminado obligaciones por parte del contratante de compra, creación y mantenimiento de hardware. Se destaca como particularidad, que es definido por el servicio y para ello se precisa cierto conocimiento de lenguaje de programación o de un conjunto de herramientas específicas. El desarrollador no tiene tanta responsabilidad en el control detallado del entorno, pues no controla la infraestructura, aunque sí las aplicaciones desplegadas por él. Las categorías de servicio que son reguladas en la norma vinculadas a este modelo apoyan la comunicación *(Caas- Communication as a Service),* la provisión de recursos para ejecutar y visualizar software (*ComaaS- Compute as a Service*). También se vinculan el almacenamiento de datos como servicio (*DSaaS- Data Storage as a Service*.) y a la disposición de red (*NaaS-Net Work as a Service*).

La hibridación de tipos y categorías genera una variada oferta de servicio adecuada a las heterogéneas y mutantes necesidades del cliente. Se desconoce(n) el(los) perfil(les) de propuesta(s) contratada(s) por los archiveros, si bien algunos estudios enuncian comportamientos variados: Borglund (2015) especifica, para la realidad sueca, experiencia de *SaaS* combinado con *IaaS*, enfatizando la percepción de los entrevistados sobre la reducida veteranía aún en la aplicabilidad de los modelos para el archivo. Brown y Fryer (2014) reflejan un estudio de caso de nube híbrida (Parlamento de UK), con plataforma tecnológica e infraestructura para el almacenamiento con objetivos de preservación digital a largo plazo, por lo que en principio, parece un modelo *IaaS* con almacenamiento masivo. Los archivos de Estado del *Land* de Bade-Wurtemberg en Alemania, emplean un modelo *SaaS* (Sobczak, 2015). La combinación de *Saas* y *Paas* la hallamos en Archivemática, por ejemplo, en la experiencia seleccionada de almacenamiento de los fondos del Consejo de Bibliotecas Universitarias de las Prairies del Pacífico (Sprout y Jordan, 2015).

2.3. Características

Las características señaladas para estos servicios son las siguientes: A) actuación bajo demanda, a modo de autoservicio a la carta. B) ancho de banda suficiente para facilitar un acceso rápido a la red, desde cualquier dispositivo con acceso a Internet. C) disposición de un conjunto de recursos compartidos por diferentes contratantes, con conectividad desde diversos terminales para múltiples usuarios al mismo tiempo. D) flexibilidad y capacidad de adaptación –incremento, disminución o modificación- de los servicios y disposición de los recursos de modo rápido atendiendo a las necesidades de los usuarios. Esto es, escalabilidad a la carta. E) Servicio medido y pagado de acuerdo a lo utilizado, esto es, capacidad para medir el uso que se hace en almacenamiento, procesamiento, ancho de banda, empleo de dispositivos y aplicaciones, etc., así como de notificar mediante informe el gasto derivado y parametrizado atendiendo a su utilización, actuando con transparencia en la optimización de los recursos y servicios empleados. (Radack 2012).

Para una adecuada valoración de los servicios a convenir, considerando aquellos que se ofertan, sería recomendable conocer marcos de referencia común en los que se delinean elementos integrantes, así como el marco normativo surgido en la regulación del CC, además de aquellos aspectos vinculados a la seguridad, portabilidad y riesgos asociados. Cuanto mayor sea la comprensión de los mismos y sus potenciales interacciones, en mejor posición se dispondrá el archivero para asesorar sobre estos entornos.

3. ECOSISTEMA NORMATIVO

En el siguiente epígrafe se revisa la composición del ecosistema normativo mediante el que se conforma y regulan los entornos CC. Se acomete desde tres enfoques: uno primero, donde se identifican normas para su construcción conceptual, terminológica y arquitectónica; uno segundo, para reflexionar sobre las normas que desarrollan seguridad y regulan actuaciones ante riesgos y, finalmente, un enfoque de análisis normativo desde la perspectiva archivística, considerando aquellas normas que incluyen aspectos que les afectan.

3.1. La construcción conceptual y arquitectónica del entorno CC

El CC está regulado por un ecosistema de normas orientadas a caracterizar y perfilar una terminología básica (ISO/IEC 17788, 2014), a definir su arquitectura de referencia (ISO/IEC 17789, 2014), a facilitar detalles de los acuerdos de servicio (Serie

ISO/IEC 19086-1/4), a mejorar su interoperabilidad y portabilidad (ISO/IEC 19831, 2015 y la futura ISO/IEC 19941[11]), a garantizar los procesos de su seguridad y confidencialidad de la información general y sus controles (ISO/IEC 27018, 2014; ISO/IEC 27017, 2015; ISO/IEC 27036 1/3)), así como a favorecer la apreciación de posibles riesgos de seguridad en la nube (ISO/IEC 27036-4, 2016). Este grupo de normas regulan aspectos del CC considerando múltiples enfoques, tales como el del proveedor del servicio, el del bróker de este tipo de servicios, el del desarrollador y el del cliente. Enfoques que el archivero debe optimizar en su beneficio.

La norma ISO/IEC 17788 (2014) incluye una terminología básica en la que, además de los conceptos clave, se definen términos sobradamente conocidos por los gestores de documentación, tales como los de disponibilidad, confidencialidad, seguridad, integridad interoperabilidad, capacidad de portabilidad, reversibilidad, auditoría, almacenamiento de datos, entre otros.

La serie ISO 19086 proporciona a clientes y proveedores las herramientas necesarias para elaborar un marco eficiente de servicio (acuerdo de servicio *Cloud* –CSA) centrado en la concreción de sus niveles de servicio (SLAs), mediante la construcción de acuerdos, la fijación de niveles, la formulación de objetivos, la regulación de requisitos principales a considerar sobre la conformidad de objetivos y calidad del SLA (parte 3); regula, asimismo, el modelo métrico que permite la medición de los objetivos de calidad (parte 2), incluido un acuerdo de nivel considerando los requisitos y objetivos de calidad en el área de la seguridad y la privacidad (parte 4). Para tal fin, ha sido estructurada en 4 partes, siendo la primera la única editada (ISO 19086-1, 2016), mientras que las partes restantes se hallan en estadios intermedios de concreción, para su publicación[12]. La primera parte explica la interconexión de las restantes. Define contenidos principales de un SLA (servicios cubiertos, conceptos o definiciones, controles, así como roles y responsabilidades) y sus áreas de contenido (figura 2 de la norma), todas ellas relevantes para la gestión de la información y los documentos como se apreciará en el enunciado cuatro.

3.2. El marco regulador de la seguridad de la información y protección de datos

La norma ISO/IEC 27036-1/3: regula la seguridad de la información y otros aspectos vinculados a protección de datos personales y privacidad, requeridos al proveedor. Estructurada en tres partes, éstas se dirigen a casuísticas y situaciones en las que se pueden especificar arreglos de seguridad. En ella, no se trabajaron factores de continuidad de negocio, dado que estos se incluyen en la norma ISO/IEC 27031 (2011)[13]. La cuarta parte (ISO/IEC 27036-4 (2016), versa sobre riesgos de adquisición y provisión de los servicios vinculados a la Seguridad de la Información (SI) en entornos de CC. Esta última parte posibilita su visibilidad para servicios en nube pública, privada e híbrida, si bien no es una guía pensada para su apreciación y mitigación, únicamente, describe directrices que apoya la gestión de la SI en estos entornos.

Para el análisis y gestión del riesgo resultan de mayor utilidad la norma ISO/IEC 27002 (2013) y la norma ISO/IEC 27017 (2015). Esta última, regula la seguridad en los servicios en la nube (enunciados 5 al 18) basándose en los controles de ISO 27002 (2013)[14]. En ella, se especifican, tanto desde el enfoque del cliente del servicio CC como desde el proveedor, políticas, organización, recursos humanos, gestión, control del acceso, criptografía, seguridad del entorno y seguridad física, de las operaciones, de la comunicación, del desarrollo y mantenimiento sobre la seguridad de la información en un entorno CC. Incorpora apartados sobre gestión de incidencias en SI, aspectos de SI y de la gestión de la continuidad de negocios, así como sobre el cumplimiento con la regulación contractual y del entorno legal. La norma dispone de dos anexos. A destacar, el primero, Anexo A, en el que se aporta un set de controles de SI en el servicio de CC.

En esta línea, la ISO/IEC 27018 (2014), regula la seguridad en protección de datos considerando los contratos de proveedores de servicios y clientes como base para el cumplimiento de los requisitos establecidos por la legislación sobre la información personal identificable (PII). Se entiende que dichos requisitos variarán atendiendo a la jurisdicción legal. Por ello, es importante conocer -y valorar en el momento de firmar los acuerdos- si los proveedores de servicios se auxiliarán de subcontratas o de opciones de internacionalización en sus servicios. En estos casos, el marco legal sobre protección de datos varía (Park, 2015).

En España, la guía sobre utilización de servicios en la nube (Ministerio de Presidencia, 2014) unifica requisitos de seguridad, requisitos vinculados a datos personales y contratación, detallando interrogantes para los datos personales y explicaciones para cada parte constitutiva del contrato (desde el enfoque de seguridad). Así mismo, la Comisión Europea (2014) ha editado una Guía de referencia para la contratación de niveles de servicio, donde se incluyen recomendaciones de objetivos de servicio para seguridad, gestión de datos y protección de datos personales, así como objetivos de calidad, claramente orientativos.

3.3. Abordaje desde la perspectiva Archivística

La gestión de la información de archivo electrónico es regulada en la norma UNE-ISO 14641-1 (2015), donde se incluyen elementos definitorios y caracterizadores de la preservación de la información y sistemas de información de Archivo Electrónico a largo plazo. Se sistematiza la búsqueda de información, accesibilidad y usabilidad de la misma, así como el concepto de "tercera parte de confianza" prestadora de servicios de archivo. Además, se regula el contenido de contratos de externalización y las características aplicables a un caso de subcontratación. Esta norma se dirige tanto a organizaciones que se encuentran implementando un sistema de información, como a aquellas otras que ofrecen tecnologías de la información y se configuren como editores de programas que busquen desarrollar sistemas, así como a aquellas que ofrezcan servicios de archivo de documentos de terceros (y donde el entorno CC puede operar). Si bien, se centra en datos de documentos capturados que no pueden alterarse (ni borrarse, ni cambiarse por otros nuevos). Algunas de sus recomendaciones son fundamentales, como la de revisar elementos técnicos contratados; perfiles de los sistemas de archivado para aquellas personas que van a acceder a la información e interactuar con ella; procedimientos operacionales,[15] ante la restitución de ficheros, la eliminación, el establecimiento de contratos, las actuaciones previas -ante la contratación de servicios de archivo por terceras partes de confianza-, o incluso, la evaluación, entre otros elementos.

De igual modo, la norma UNE-ISO 14721 (2015) apoya un diseño de repositorios de ficheros en acceso abierto, cuya confiabilidad puede evaluarse mediante la norma ISO 16363:2012. Esta norma puede emplearse para perfilar criterios en el almacenamiento y funcionalidad de las entidades de captura, de gestión de los datos, de planificación de la conservación, del almacenamiento y administración del mismo. A su vez, la norma ISO 17068:2012 aporta metodología para verificar por tercera parte (contratante u otro) la confianza en repositorios digitales (del proveedor del servicio). Por ende, es de utilidad para que el cliente que ha contratado un servicio obtenga ciertas garantías sobre cómo se realiza dicha gestión (sobre servicios de almacenamiento contratados, personas y sistemas que se encargan de asegurar los recursos digitales). De este modo, la parte contratante puede verificar un grado de seguridad sobre su proveedor.

Conviene recordar que en gestión de documentos se dispone de una norma sobre apreciación del riesgo para los documentos (UNE-ISO/TR 18128, 2014) en la que se reconocen áreas de incertidumbre que afectan al entorno tecnológico, a las amenazas de seguridad externa, a las mudanzas acaecidas en la organización, a la sostenibilidad y continuidad, entre otras, con aspectos tales como cambios: a) ante la adopción de nuevas tecnologías de modo transversal en la organización y la sociedad; b) en la propiedad, transferencia y traslado de los documentos en la organización, c) en la propiedad como resultado de migraciones forzosas, acuerdos de acceso, transferencia y migración; d) en los términos en los contratos de servicios con terceros, que afecten a la interoperabilidad entre sistemas, sobre las compatibilidades con plataformas y aplicaciones, etc. Por otro lado, la norma ISO 15489-1:2016, al definir un documento autorizado, perfila implícitamente posibles amenazas, ante su incumplimiento. De momento, no existe una norma específica que desde los intereses del gestor documental se regule la gestión, almacenamiento y preservación de ficheros, si bien existe un Grupo de trabajo (ISO/TC 46-SC11/WG17 *Records in the cloud*) que se encuentra desarrollando junto con el ISO/TC 154/WG6 de Aplicaciones de gestión de documentos para Procesos, elementos de datos y documentos en el comercio, la industria y la administración, un proyecto específico (*Information and Documentation*. *Records management in cloud: Issues and concerns*) cuya confirmación contribuiría a facilitar la tarea del gestor en este campo.

4. LA APRECIACIÓN DE RIESGOS COMO SERVICIO

Del conjunto de lecturas realizadas, se deduce una notable preocupación ante la diversidad de amenazas. Los riesgos son percibidos por tecnólogos, normalizadores y archiveros. Para los tecnólogos informáticos, las amenazas que caracterizan el entorno CC se centran en seguridad, tanto para infraestructuras, plataforma de softwares como para servicios de gestión y almacenamiento de los datos. Seguidamente, se detallan las preocupaciones más destacadas y reiteradas: el acceso a los datos, su control o gestión de identidades de usuarios, el cifrado y la comunicación de los datos cifrados, su integridad, el cumplimiento de los requisitos mínimos de seguridad y la propia seguridad física requerida en los centros de datos. Especialmente, se subraya la preocupación por alcanzar seguridad en las infraestructuras de la nube y plataformas, considerando aspectos tales como la vulnerabilidad de la red, problemas de portabilidad (migración) y otros factores que afectan directamente a los propios datos sobre: autenticidad, bloqueos, procedencia, eliminación, pérdida, privacidad, etc. Así mismo, los tecnólogos perciben posibles amenazas ante audi-

toría y control de los datos (deficiencias), sobre rastreabilidad de las operaciones, o la propia ubicación de los datos en situaciones transfronterizas respecto a su compatibilidad jurisdiccional. Los riesgos sobre accesibilidad son contundentes en estadísticas de La Unión Europea de los veintiocho, donde para el 2014 se confirmó que el 35% de las empresas tuvieron problemas de acceso a un software o a datos almacenados (Eurostat, 2016[16]).

La normativa específica sobre entornos CC, igualmente, incorpora el riesgo. En ISO 19086-1, aparecen conceptos definidos tales como continuidad de negocio, recuperación ante desastres, resiliencia y compensación. La continuidad de negocio es el elemento base sobre el que se imbrica la idea de continuidad digital, donde precisamente se defiende la "disponibilidad" de la información, su "accesibilidad" y "usabilidad" en el tiempo, al considerar riesgos en apertura de ficheros, riesgos en el conocimiento de su localización, en comprensión de la información y en su manejo deficiente o insuficiente para el trabajo diario o la verificación de hechos. La accesibilidad, orientada a la usabilidad, es referida en la norma a todo tipo de "capacidades del usuario", subrayando que "busca alcanzar niveles de efectividad, eficiencia y satisfacción (…) considerando el contexto especificado de uso" (ISO 19086.1 concepto. Notas 1 y 2).

Para los archiveros, la gestión del riesgo no es un asunto baladí en sus sistemas de gestión y preservación de documentos electrónicos. Ya se ha señalado como la norma UNE-ISO/TR 18128 (2014) identifica áreas y factores de riesgo, e incorpora metodología para la apreciación basada en la serie de normas ISO 31000 (Gestión del riesgo).

Para los gestores de los documentos, estos entornos CC, han generado (y generan) cierta desconfianza. Ejemplo de ello, es la aportación de Goh y Sengsavang (2016), quienes muestran las barreras percibidas por archiveros e informáticos. En orden de importancia exponen las siguientes: protección de datos personales (92.86%), propiedad y custodia de los datos/documentos (88,09%), seguridad de la IT (85,72%), inviolabilidad de los datos (80,96%) y la aplicabilidad de las leyes locales en protección de la información personal (73.81%). Curiosamente, al destacar los autores la percepción de los archiveros frente a los informáticos, destacan: la (in)seguridad de la información y la (des)protección de datos personales. Por el contrario, los informáticos otorgan mayor peso a las derivadas de la propiedad y custodia de los documentos y de la incertidumbre sobre la aplicabilidad de legislaciones locales[17].

En esta línea, Beagrie y otros (2014) al referirse a seguridad, especialmente en aquella información sensible, comercial o con datos personales, remarcan que los proveedores CC pueden incluir, tanto en los servicios que ofrecen como en los centros de datos que gestionan, niveles de seguridad muy elevados, dado que son certificados mediante la serie ISO 27001, además de incorporar normas específicas para los entornos CC, que trabajan la seguridad de los datos, tal y como se ha reseñado.

De facto, la norma ISO 17788 (2014) entiende por *Seguridad de la información* "la preservación de la confidencialidad, integridad y disponibilidad de la información" a la que deben añadirse, atendiendo a la nota que acompaña al término definido, otras propiedades como la autenticidad, responsabilidad, no rechazo y fiabilidad. Estos aspectos conforman, igualmente, la definición del documento autorizado (UNE-ISO 15489-1, 2016). Remarcamos como la disponibilidad del documento significa que éste puede ser localizado, recuperado, presentado e interpretado, matices que se destacan en continuidad digital.

La seguridad constituye una de las cuatro categorías de requisitos que, para los sistemas de información, especifica la norma UNE-ISO 14641-1 (2015). Señala entre los requisitos mínimos: la identificación de personas y de procesos que acceden, la realización de copias de seguridad, el control de las actividades de acceso y la continuidad en los accesos; y entre los adicionales: la recuperación de formatos distintos de los formatos de acceso a los originales. Así mismo, establece categorías para la trazabilidad de las acciones, para la integridad de los datos y para la preservación de los mismos.

Junto a la seguridad de la información, la confidencialidad, *a priori* es la que mayores reservas suscita entre los profesionales de la información para no incumplir la legislación sobre protección de datos, tal y como especifica Ostrzenski (2013). A este tenor, Cotino-Hueso (2015) diferencia 3 categorías de riesgos: aquellos vinculados a la falta de control de datos (disponibilidad, portabilidad, integración, confidencialidad, cadena de subcontratación); los derivados de un deficiente aislamiento de los datos en entornos multiusuarios; o los producidos por insuficiente transparencia sobre el potencial de amenazas comunicadas a los contratantes y sobre el posicionamiento de datos, entre otros.

Estudios, informes y recomendaciones de algunos archiveros y Archivos en los que han sido analizados riesgos en la gestión de la información en la nube (CAARA, 2010; McKemmish, 2013; PROV, 2013; Beagrie y otros, 2014; Government of South Australia, 2015), confirman cierta preocupación a la par que permiten identificar una serie de amenazas sobre las que se debería actuar para mitigar

su alcance. Concretamente, McKemmish (2013) se plantea hasta siete categorías de riesgos aportando información para actuar, tanto desde la perspectiva del contratante como del proveedor de servicios. Algunas de ellas se aglutinan bajo el paraguas de riesgos derivados de la g*estión y almacenamiento de los datos*: seguimiento durante el ciclo de vida y sin garantías de continuidad digital; otras bajo la amenaza de *seguridad de los datos*, protección de derechos y seguridad de plataformas y softwares. De igual modo, subraya riesgos de índole *legal y buen gobierno:* incompatibilidades jurisdiccionales y geolocalizaciones transfronterizas, de transparencia (informes ante incidentes, comunicaciones sobre remedios adoptados…) y gobernabilidad. Finalmente, la autora de este ensayo señala el riesgo *de ausencia de consideración de los requisitos de GDE* en la gestión y almacenamiento de datos. En esta línea enumerativa, los riesgos visualizados por CAARA (2010), PROV (2013) y los archivos de South Australia (2015) coinciden con algunos de los anteriores expuestos (protección de datos, almacenamiento en otra jurisdicción, funcionalidades de GDE, pérdida de datos); Además, profundizan en riesgos sobre el *acceso* a los datos y su *disponibilidad*, motivado por causas heterogéneas[18]. De igual modo, en los estudios se señalan posibles dificultades en la *portabilidad* (migración de datos) de un sistema a otro (proveedor y cliente). La *portabilidad, continuidad y sostenibilidad* son los aspectos constructivos de una preservación permanente y viable, tal y como demuestran Stancic y otros (2015) para documentos firmados electrónicamente y en los que aportan soluciones diversas, de utilidad para experimentar.

Encontramos en las directrices de UK (Beagrie y otros, 2014) excelentes detalles sobre los riesgos derivados de a*spectos legales* en cuanto a gestión, preservación y acceso a los archivos, discerniendo entre los coincidentes con procesos de externalización de funciones, de los específicos al entorno CC, planteados entre proveedores y contratantes, o considerando obligaciones de derecho de terceras partes –como gobiernos y clientes- o los derivados de los contractos y niveles de acuerdos establecidos entre proveedor y archivo. Sobre obligaciones de terceras partes se especifican aspectos de cumplimiento de derechos de autor, licencias de uso, reproducción de archivos o copias, permisos y autorizaciones, etc. Al respecto, se destacan riesgos vinculados a externalización y subcontratas, a la virtualización (seguridad en equipos compartidos, pérdida de control de la localización de los datos, acceso, multi-*cloud*, etc.), autonomía tecnológica (adaptación de servicios a necesidades, por ejemplo) y a la deslocalización (competencia jurisdiccional para seleccionar y ejecutar la legislación pertinente).

En la actualidad, la *conformación del acuerdo de servicio,* en sí mismo, debe considerarse un riesgo elevado, debido al *desconocimiento* que el profesional pueda tener sobre el mismo, y cuya carencia competencial impide adoptar posiciones proactivas. Además, en el proceso de contratación de los servicios deberían de contemplarse todos los riesgos posibles, con anterioridad a la firma del contrato de servicio. Máxime, considerando que se trata de entornos caracterizados por el cambio continuado, debido a la obsolescencia tecnológica y *valorando las necesidades presentes y futuras de los usuarios* de los datos. Por tanto, atendiendo al tipo de necesidades, deberían de identificarse posibles riesgos vinculados a la conservación y provisión de datos más allá de su vida "activa" o aquella limitada a la ejecución de la actividad de negocio. Finalmente, atendiendo a los intereses de preservación, sería importante identificar riesgos de pérdida o de destrucción o corrupción de datos derivada de *presupuestos financieros insuficientes* para la contratación, así como, aquel conjunto de riesgos provocados por ausencia o *deficiencias de planificación de estrategias de éxito y de auditorías específicas* de control.

Los requisitos especificados en normas ISO, cuyo incumplimiento puede redundar en riesgos, así como el conjunto de amenazas señaladas, invitan a considerar actuaciones planificadas que favorezcan rápidas recuperaciones ante incidentes de consideración.

5. ESTRATEGIAS COMO SERVICIO

En el epígrafe se presentan estrategias y escenarios de actuación de alcance general, así como las específicas para actuar ante el ciclo de vida de los datos en el entorno de la nube.

5.1. Pluralidad de estrategias y escenarios

Algunos autores (Oliver y Knight, 2015; Beagrie y otros, 2014) adelantan las siguientes estrategias de preservación que se deben respetar:

a) Sobrepasar intereses cortoplacistas de diversidad de agentes - de productores (vida útil administrativa), proveedores (interés económico) y tecnólogos (grado de obsolescencia)-, para preservar los recursos digitales almacenados en la nube.

b) Intervención de control y asesoría del gestor de documentos.

   a) Ante acuerdos o pautas para la gestión o mitigación de riesgos sobre corrupción, pérdida o destrucción de datos, basadas en informes financieros.

b) Ante estrategias de cierre de contrato con el proveedor y devolución de datos.

El enfoque de una preservación sostenible debe prevalecer en entornos de incertidumbre. Este es el caso de los entornos CC. El cambio en la práctica archivística en estos entornos ha sido analizado por Stancic y otros (2013) destacando cuatro escenarios clave:

1. Escenario I- Proveedores de servicios responsables en la práctica de la gestión y conservación de los documentos. No intervención de productores y archiveros.
2. Escenario II- Productores de información, invierten esfuerzos en un control adicional de aquellos servicios no estandarizados.
3. Escenario III- Servicios normalizados. Productores de documentos seleccionan proveedores de servicios, atendiendo al nivel de cumplimiento de requisitos.
4. Escenario IV-La Comunidad de archiveros es sensible y activa asegurando el cumplimiento de normas e influye en su implementación por parte de los proveedores de servicios y en su exigencia por parte de los productores.

Desconocemos cuantitativamente el grado de inmersión de estos escenarios en la práctica de las organizaciones. Goh y Sengsavang (2016), subrayan en su estudio como la mitad de las organizaciones que contrataron dichos servicios carecían de una política para la externalización de transferencia y gestión de documentos transferidos, recayendo las decisiones sobre la contratación de estos servicios en los Departamentos de informática (76%), frente a un 10% de participación de archiveros. Lógicamente, de este escenario, pueden derivarse riesgos de gestión y de continuidad digital, en la medida en que el proveedor desconozca requisitos de gestión del documento electrónico (GDE) o no esté interesado económicamente en aportar "a priori" niveles de servicio a costes elevados.

El segundo escenario (intervención de control de la organización contratante), precisa de asesoría especializada en GDE, dado que es necesaria para identificar los requisitos a normalizar y para avanzar en la mitigación de posibles riesgos.[19]

En el tercer escenario (de servicio normalizado), confluyen oferta de servicio normalizado y potenciales riesgos en GDE para la organización contratante del servicio, por lo que la asesoría y el control resultan imprescindibles. Estudios sobre experiencias demuestran actuaciones dispares. Goh y Sengsavang (2016) especifican como un 26.19% negocia niveles de servicio y no acepta el contrato ofertado por el proveedor, un 16.67% no lo negocia y un 28.57% lo desconoce, por lo que se deduce su ausencia en dicha negociación.[20].

El cuarto escenario debe estimarse ideal, donde el archivero se adelanta sensibilizando a la organización sobre la necesidad de efectuar acuerdos de nivel de servicio (SLAs) provechosos y respetuosos con la gestión de sus datos; por tanto, actuando de modo activo en la mejora de un marco común de servicios para el que previamente ha analizado los requisitos mínimos de servicio en un contexto CC.

La realidad desde la óptica de gestión documental, ha sido reflejada por Stancic y otros (2013) en el análisis de un proveedor de servicios operativo en cincuenta y ocho países, (alcance global) en el que se destaca la existencia de información sensible, como: documentación sobre personal, datos confidenciales de clientes, información confidencial o secreta vinculada a productos, textos y otros formatos con derechos de autor. Se manifiesta la cesión que realizan las organizaciones a empresas desconocidas de documentación sujeta al cumplimiento de un estricto marco legal. Sitúan en riesgo su imagen, su nivel de competitividad, su reputación comercial, su gobernanza, etc.

5.2. Acciones vinculadas al ciclo de vida de los datos

A la luz de estas situaciones, los autores recomiendan actuaciones comprometidas, intermediarias entre proveedores y clientes, mediante asesoría calificada como Archivando 2.0 y que McKemmish (2013) adjetiva de Archivos 3.0. Estas, pueden ejercerse atendiendo a la secuencia del ciclo de vida de adopción de un servicio, considerando sus principales etapas que dan respuesta a dónde, cuándo, cómo y con qué actuar. Esto es, a la identificación de localizaciones, tiempos, métodos e instrumentos específicos y que se resumen en el ciclo como:

a) Acciones previas a la firma de un SLA, identificando requisitos a cumplir (cuyo incumplimiento deriva en riesgo) en la organización contratante y comparando la oferta mostrada por el proveedor, atendiendo a estas necesidades identificadas.

b) Consolidación y mantenimiento de los compromisos de servicio contratados, mediante acuerdo, verificando la calidad de los objetivos de servicio reflejados en los acuerdos; en su caso, ajustando los acuerdos considerando las nuevas necesidades; y finalmente, analizando incidencias y hechos sobrevenidos, así como aspectos de recuperación ante desastres.

c) Detalles de rescisión del contrato de servicio (bien por finalización o/y actualización del acuerdo).

La fase previa de identificación de requisitos debería, además de trabajar aquellos requisitos funcionales y técnicos de GDE, contrastar cuáles de ellos no se hallan reflejados en el acuerdo estándar o, si estuvieran, su grado de compatibilidad respecto a los exigidos en cuanto a existencia y cumplimiento del marco legal del contratante del servicio. Exige, por tanto, la creación de un listado de requisitos a cumplir por la entidad, sobre el que se verificarán amenazas, valorando ofertas y legalidad de los proveedores de servicios. La labor asesora se sustenta en el análisis del conjunto de ofertas que mejor respondan a los requisitos de la organización y, además, conlleven costes más aceptables en caso de incremento de las prestaciones, sin olvidar los requisitos preceptivos ante la rescisión del servicio.

Lógicamente, todo esfuerzo por sistematizar requisitos alcanza notable valor. Algunos Archivos contribuyen a esta tarea (Archivos de UK, por ejemplo), tabulando un conjunto de ellos, para contrastar requisitos de tipo legal y contractual. Sobre los primeros, cita los vinculados a la custodia de los datos (de mantenimiento y gestión, de seguridad, de cumplimiento), al acceso (derechos), a la transferencia y disposición de los datos (destrucción y transferencia), a los derechos de propiedad intelectual (derechos del depositante, del proveedor y de terceras partes) y finalmente, a la protección de datos personales (jurisdicciones, derechos de los individuos, acceso para uso de datos exentos, infracciones).

A menudo, hallamos orientaciones en normas que pueden servirnos de guía. Tal es el caso de la norma UNE-ISO 14641-1 (2015), donde se especifican actuaciones previas a la contratación del servicio de archivos (permanentes) de una tercera parte de confianza, recomendando verificar si el proveedor del servicio es capaz de cumplir tres aspectos clave, entre otros, que son: capacidad de cumplimiento de requisitos mínimos de archivo (integridad, disponibilidad, fiabilidad, autenticidad, etc.), compatibilidad de las políticas de gestión y de los procedimientos de seguridad con los acordados por la organización.

Por otro lado, en la fase intermedia de un ciclo de servicio sería aconsejable que el archivero –ante su rol asesor- verificase la conformidad del cumplimiento de las estipulaciones convenidas (siempre desde la óptica del cumplimiento de los requisitos de funcionalidad, técnicos, de seguridad, confidencialidad, portabilidad, continuidad etc. de los datos e informaciones) vinculadas a los objetivos de servicio, atendiendo a las modificaciones acaecidas o sobrevenidas, esencialmente en cuanto a accesibilidad, usabilidad, portabilidad, etc. Los elementos de un acuerdo de nivel de servicio son estipulados en diversas fuentes: norma ISO 19086-1 (2016); Guía de la Comisión Europea para normalizar los SLA (2014); directrices del PRO of Victoria (2013); Guía de Seguridad en CC (España. Ministerio de Presidencia: 2014).

El modelo de referencia común ofertado por el proveedor debería describir (siguiendo las indicaciones de la norma ISO 19086-1) el acuerdo de servicio en la nube para facilitar una comprensión común de las partes y el SLA, así como para determinar el nivel del servicio contratado. Su consulta contribuirá a conocer el tipo de tramitaciones a realizar, atributos que caracterizan el SLA, objetivos de nivel de servicio que se ofertan y se aceptan, directrices y mejores prácticas. Lo idóneo, sería poder consultar el acuerdo de servicio marco en el *site* del proveedor. El SLA, suele formar parte del mismo por lo que favorece su localización.

Un acuerdo de servicio es definido como un acuerdo documentado sobre el servicio establecido entre dos partes (proveedor y contratante del servicio) que como se ha detallado, puede constar de uno o más documentos, sobre los servicios establecidos (ISO 19086-1:2016). Suele disponer de documentos definitorios de términos empleados en todos los servicios, explicativos de obligaciones y descriptivos sobre la finalización del servicio. Acompañan otros adicionales para el acuerdo específico, SLA. No siempre los proveedores aportan esta documentación diferenciada, tal y como McLelland y otros (2014) muestran en el análisis de contratos. Resulta esencial conocer el contenido regulado en la norma sobre las partes de los acuerdos (SLA) para trabajar la apreciación de riesgos. Es una oportunidad para su mitigación, dado que en ellos se incluyen tanto objetivos fijados (cuantitativos y medibles mediante rangos), como elementos cualitativos (lista enumerada de aspectos constatables mediante interpretación humana o sobre su existencia o no existencia) de los servicios acordados: apoyos, niveles de rendimiento, recuperación de desastres, propiedades y acceso a los datos, etc.

De hecho, en dicha norma se especifican áreas de contenido de los SLA que, tanto proveedores como contratantes de servicios, deberían conformar, consultar y acordar respectivamente. Su enumeración es suficientemente aclaratoria de su relevancia: seguridad de la información, disponibilidad, accesibilidad, apoyo al servicio Cloud, terminación del servicio, gobernanza, cambios de servicio, fiabilidad del servicio, rendimiento del servicio, certi-

ficaciones, gestión de datos y protección de datos personales. Con frecuencia, los contratos, cambian muy rápidamente por lo que debe quedar definido el modo de comunicación por parte del proveedor y sus actuaciones.

Analizados de modo general (Baset,2012; Gulia y Sood,2013; Pan y Mitchell,2015) y, desde un enfoque documental (McLelland y otros, 2014; Bushey, Demoulin y McLelland, 2015) los contenidos de un SLA, se percibe coincidencia, -tal y como se señala en la norma- sobre la necesidad de incluir en el acuerdo (o de consultar en la propuesta de acuerdo) detalles sobre el rendimiento del servicio contratado (garantías, duración, granularidad, exclusiones, control de incumplimiento, informes y acreditaciones). Se incide además en la observancia de la terminología, de las limitaciones y responsabilidades de proveedores y contratantes. Resulta aconsejable demarcar contenidos mínimos, así como valorar o incorporar soluciones ante situaciones de pérdida, desastre o incumplimiento. De igual forma, deberían regularse contenidos sobre la notificación de informes y sobre actuaciones ante la finalización o actualización del acuerdo ante devoluciones de datos, modificación de los servicios y responsabilidades derivadas. La ETSI (2012) propone en su informe técnico para evaluar requisitos de calidad de los SLAs los siguientes: rapidez, precisión complementada por fidelidad, disponibilidad, confiabilidad, seguridad, simplicidad, flexibilidad, capacidad y usabilidad.

En la Guía de los Archivos Nacionales de Reino Unido (Beagrie y otros, 2014), se ha sistematizado la siguiente relación de elementos a valorar: disponibilidad, rendimiento, funcionabilidad, externalización, protección de datos, seguridad, control y auditoría, propiedad de los datos y de los metadatos, localización geográfica, disposición de los datos, portabilidad, gestión del cambio, cambios en los términos y condiciones de servicio, identificación y resolución de problemas, infracciones, recuperación ante desastres, mediación ante disputas, terminación del contrato, cambios producidos en el estatus del proveedor o mediador del servicio, renovaciones del contrato, costes y legislación. Bushey y otros (2016), han elaborado una lista de verificación para contratos de servicios CC, en la que proponen 68 interrogantes (agrupados en 8 apartados), dotados de una escala[21], en la que se consideran los siguientes aspectos: convenio; propiedad de la información; disponibilidad, recuperación y uso; almacenamiento de datos y preservación; retención y disposición de datos; seguridad, confidencialidad y privacidad; ubicación de los datos y flujo de datos transfronterizos; y, finalmente, terminación del contrato. Dicha guía es altamente aconsejable.

Además del acuerdo de servicio marco y el SLA, el servicio ofertado/aceptado puede conformarse de una base documental amplia que refleja acuerdos de suscripción, acuerdo de procesador, acuerdo de nivel de privacidad e incluir determinadas políticas adoptadas en torno a la privacidad, uso, seguridad, continuidad de negocio y el plan de recuperación de desastres.

La tercera fase del ciclo debería enfocarse, bien a la continuidad digital de la información, bien al aseguramiento de la preservación de los datos, ante la actualización del acuerdo o ante la finalización del mismo (formatos compatibles, migraciones, devolución de datos, borrado en la nube, reversibilidad, tal y como se concretó, metadatos recuperables, comprensibles, etc.). La portabilidad de los ficheros (capacidad de migración de una nube a otra) tendría que estar negociada con anterioridad a la firma del SLA, tanto para fases intermedias –caso de subcontratación de servicios por el prestador- así como para la etapa final. Igualmente, se deberían perfilar las condiciones de renovación del servicio, verificando -en el momento de la rescisión- el cumplimiento de lo acordado en la contratación del servicio y mejorando, en su caso, las clausulas y contenidos del nuevo acuerdo, resultado del estudio de resiliencia. Todas las actuaciones derivadas de la segunda y tercera fase deben de quedar reflejadas en la documentación resultante de los acuerdos o estar sujetas a revisión.

La importancia de participar en la negociación del contrato es tal que confirmamos con Bushey, Demoulin y McLelland (2015) la necesidad de actuar de modo proactivo para alcanzar habilidades y negociaciones que mejoren el rendimiento en estos entornos, dado que tal como señalan dichos autores, la firma de un SLA debe entenderse como "un eslabón en la cadena del proceso de gestión de calidad. Para obtener una alta calidad de servicio se requiere diligencia en la selección del servicio, negociando un contrato equilibrado y otros procedimientos"[22]. Esto es, centrándose en las relaciones establecidas de confianza entre proveedor y cliente, tanto en el momento de decidir el contrato como en su implementación, determinación y actuación del ciclo de vida. McLelland y otros (2014) analizan el empleo de modelos económicos para la toma de decisiones, ante la firma de un contrato de servicio en la nube.

Numerosos son los archiveros que destacan el potencial rol asesor del archivero en la compra de servicios CC (Askhoj y otros, 2011; McKemmist, 2013; Stancic y otros, 2013), incorporándolo al ejercicio profesional desde un enfoque positivo y subrayando la necesidad de ser formados en esta temática. Con esta finalidad, Oliver y Knight (2015), proponen la adquisición de habilidades y

competencias sobre estos entornos. Al respecto, Borglund (2015) enfatiza la prioridad de ahondar en competencias sobre tecnologías de la información, -tanto para los entornos Web como para la seguridad de la información-, así como en la preservación a largo plazo. Igualmente, redunda en la necesidad de adquirir la competencia para el diseño de acuerdos de servicios.

Para finalizar, señalar que Guo y otros (2015) observan estos entornos, como una oportunidad para el archivero, al conferirle el rol de garante de la autenticidad e integridad del documento, percibiéndolo como mediador del servicio de almacenamiento comercial entre los recursos de datos producidos desde el sector privado y almacenados en el sector público (o en el privado), dadas las competencias destacadas y demostradas del archivero en el logro de *documentos auténticos*.

6. CONCLUSIONES

Se ha constatado el interés creciente en el uso de servicios CC en las organizaciones europeas, con comportamientos desiguales de su empleo entre sus países integrantes, situándose España en una ratio del 20% frente a Finlandia con 57%. Esto es, una de cada cinco empresas lo utiliza. Han sido destacadas las principales ventajas asociadas a los servicios CC, tanto en organizaciones, como en centros de archivo. Los estudios demuestran como los profesionales perciben claramente su utilidad en centros con moderados recursos, señalando, además experiencias efectivas para otro tipo de centros y con necesidades de almacenamiento de datos, no sólo cortoplacistas sino a más largo plazo.

A su vez, han sido identificados un buen número de riesgos, percibidos por profesionales de la información y, en cierto modo, algunos de ellos contrastados en su experiencia con servicios contratados. Se ha demostrado un enfoque polimorfo en la observancia del riesgo, como acontece con seguridad de los datos, constatándose amenazada en este entorno o, por el contrario, asegurada. En similares circunstancias, se ubica la sostenibilidad económica (factible o desorbitada). Existe coincidencia en identificar riesgos derivados de privacidad de datos personales, portabilidad, acuerdos de servicio y formación tecnológica y legal.

La concreción de los servicios es cada vez más consistente, sistematizada y regulada, a tenor del marco normativo, incluidos algunos factores de riesgo, tales como: fundamentación, cuidado terminológico, seguridad, protección de datos y privacidad, integridad, alcance e intervención en los acuerdos, entre otros.

El hecho de que el trabajo sobre el recurso digital de estos entornos CC se ejecute sobre un objeto *multifacetado* (poliforme), *diversificado* (requisitos heterogéneos de variados contextos económico-sociales-culturales) y *dinámico*, (cambio tecnológico continuado así como a las expectativas de las comunidades que producen, mantienen y conservan dichos recursos), tal y como es calificado por Jansen y Duranti (2013), obliga al profesional a generar estrategias para abordar con sostenibilidad la problemática derivada de esta nueva situación, conduciéndola como una oportunidad de trabajo y de generación de nuevas expectativas para obtener mejores rendimientos. Se invita al profesional a adoptar una actitud proactiva en el proceso de contratación de servicios, un compromiso en la adquisición de los conocimientos y competencias tecnológicas y legales requeridas, desplegando la habitual resiliencia que ha demostrado poseer ante los entornos electrónicos. La opacidad de la nube dificulta una adecuada intervención. Coincidimos con, Oliver y Knight (2015) en que se debería investigar el uso potencial de dichos servicios, sopesando la necesaria inversión económica requerida a corto plazo, los beneficios que a largo plazo reportan, así como el impacto y responsabilidad que ello implica desde la perspectiva de almacenamiento y conservación en el tiempo.

El ensayo basado en la consulta de normas, ensayos y directrices, fruto del interés del archivero y tecnólogo por estos entornos CC, debe contrastarse con otros nuevos donde sean identificados factores limitadores y potenciadores, normalizados procesos y se difundan experiencias (el número de ellos es aún reducido). De este modo, las percepciones y valoraciones sobre su uso contribuirán a (in)formar a la comunidad de profesionales interesados. Igualmente, sería recomendable el análisis de los proveedores de servicios por y para los especialistas. En esta línea, interesa consultar la guía de UK (Beagrie y otros, 2014) en la que se incorporan ejemplos de cumplimiento de determinados criterios por parte de proveedores de servicios generales y especializados[23]. Ahondar en este tipo de estudios facilitará las decisiones de los profesionales en procesos asesores.

Ante todo, se debe evitar todo tipo de brechas críticas para la gestión y preservación de los documentos. De facto, al propio Archivo le es inherente la autenticidad de los documentos, siendo garante de confianza plena sobre la misma. Guo y otros (2015) subrayan esta condición definitoria del archivo en su triple acepción de *transparencia*, lograda mediante profesionales imparciales, confiables que actúan como intermediarios, de *su seguridad*, evitando cualquier alteración o daño

accidental o deliberado, y *estabilidad*, ante una adecuada identificación y representación de los contextos de producción de la información. Acepciones que son total o parcialmente delegadas en terceros (proveedores de servicios). Por lo tanto, nos reafirmamos en la prioridad de adoptar una actitud proactiva ante los entornos CC. La asunción de este compromiso facilitará la adquisición de la confianza necesaria para actuar con la competencia debida, dado que, sin lugar a dudas, dichos entornos son un futuro ineludible.

7. AGRADECIMIENTOS

Este trabajo ha sido financiado por la Agencia Financiadora Coimbra Group Universities (Referencia CG- 477.488.939- Convocatoria 2017-Llanes-Padrón), por su programa de becas para profesores e investigadores de Latinoamérica, del que ha sido beneficiaria Doña Dunia Llanes Padrón.

ACKNOWLEDGEMENTS

The Coimbra Group Universities (Reference: CG-477.488.939, Brochure 2017-LLanes-Padrón) Financing Agency has funded this work through its scholarship program for academics and researchers from Latin America, which has granted Mrs. Dunia Llanes Padrón.

8. NOTAS

1. Con bibliografía selecta datada entre el 2009 y 2014 sobre asuntos tales como: complejidad de la nube, privacidad de datos, compendio de normas que afectan en la UE, contratos de servicios, derechos de propiedad, protección de datos, seguridad y jurisdicciones.
2. Concretamente, tres casos sobre jurisdicciones, protección de datos y compensación por daños de vulneración de la protección de datos del 2012.
3. Se trata de bibliografía editada entre 2010 y 2014 con asuntos del tipo: tecnología componente, terminología empleada por proveedores de servicios en sus contratos, elementos a considerar ante un contrato, cambios en los servicios, escenarios de utilización, riesgos de seguridad, presentación de servicios y riesgos asociados al Cloud Computing, almacenamiento, directrices y guías de algunas Agencias gubernamentales y Archivos, gobernanza, seguridad, análisis teórico, entre otros.
4. En la que se reúne bibliografía sobre principios de gestión de documentos y normalización, tal como disposiciones de ARMA; de ISO para gestión, ISO:15489,2001; para requisitos funcionales: Moreq2010; y para repositorios: ISO 14721,2012.
5. Fruto de ello, es la colección de informes que se han focalizado en el almacenamiento en infraestructura CC [Informe EU08], (Stancic y otros , 2016); modelos económicos para el almacenamiento en la nube [Informe EU20] (McLeod y Gormly, 2016); análisis de términos en contratos (informe NA10), (Hackett y otros, 2014); listado de verificación para contratos de servicios CC [informe NA14] (Bushey y otros, 2016); estudios históricos de servicios en la nube [informe NA11] (Leverich y otros, 2015); además de la bibliografía anotada, anteriormente citada. Información accesible en: https://interparestrust.org/trust/about_research/studies.
6. En esta línea, la compra realizada por las empresas de servicios en la nube mediante la red Internet, en diciembre de 2016, representa un 23% para la UE de los 15, un 20% en la zona euro y un 21% para las empresas de los 28, destacando países como Finlandia con un 57% o Dinamarca con un 42%. En España, la ratio es sensiblemente inferior, con un 18%. En el Boletín del INE, se confirma que una de cada cinco empresas españolas compra algún servicio CC, siendo un 73.7% de ellas las que prefieren hacerlo desde servidores compartidos.
7. En cuanto al sector, es el de las TICs y aquel de actividades vinculadas a la Información y Comunicación los más destacados con un 58% y un 57% respectivamente. Sobre servicios, el 71.2% de empresas con más de 10 empleados tienen contratado el correo electrónico, el 68.7% servicios de ficheros, el 59,6% servidores de bases de datos de la empresa y un 38.5% servicios de software office (procesadores de texto, hojas de cálculo…) Geográficamente, son Madrid (27.4%) y Cataluña (25.6%) las comunidades autónomas con mayores porcentajes de compra de servicios.
8. Goh y Sengsavang (2016) muestran como los intereses por la contratación de estos servicios se apuntalan en criterios como escalabilidad, disponibilidad, ahorro de costes, facilidad en el despliegue y flexibilidad creciente. En la Guía de los Archivos de Reino Unido (2014) se añaden potencial para el empleo en archivos pequeños con bajos presupuestos (almacenamiento de datos) y para disponer de múltiples respaldos y copias de un modo económico en diferentes geolocalizaciones; destacando el potencial que representan las demostraciones accesibles para algunos de ellos, proporcionada por proveedores emergentes.
9. Si bien, esta queda expuesta a terceros y, por esta razón, parece menos protegida a como se venía trabajando desde la organización.

10. Enunciado 3.2.5 de *cloud computing (*traducción propia de autoras*): Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administrtion on-demand.*

11. La norma ISO/IEC 19941 se encuentra en debate internacional (modo DIS) y es específica para regular la interoperabilidad y portabilidad en un entorno de nube. Su edición está prevista en el presente año.

12. A data de remisión de este estudio, su situación es como sigue: Parte 2, fase borrador -WD; Parte 3, fase de discusión internacional -DIS, Parte 4- fase de discusión nacional- CD.

13. En ella se describen conceptos, principios, procesos y métodos para identificar todos los aspectos y el diseño sobre la continuidad de negocio en las TIC, incluyendo actuaciones ante eventos e incidentes y ante cualquier interrupción relacionada que pudiera afectar a las funciones críticas de la organización.

14. A su vez, se considera una recomendación de la Unión de Telecomunicaciones Internacional del sector de normalización de telecomunicaciones, bajo el código ITU-X.1631.

15. Para la creación, asignación o cambio de formatos, asignación de metadatos, para la captura, duplicación y réplica, copias de seguridad, encriptado digital, etc.

16. *Cloud computing services*. Eurostat. 2016. Accesible en: http://ec.europa.eu/eurostat/documents/2995521/6208098/4-09122014-APEN.pdf/627ddf4f-730a-46ca-856b-32532d8325c5

17. Se comprenden estas preocupaciones, al considerar los resultados del estudio presentado, donde la mitad de las organizaciones encuestadas (40,48%) carecen de políticas sobre externalización, transferencia y procesamiento de datos por terceros, frente a un 40,48% que sí dispone de ellas.

18. Tales como: el acceso no autorizado, dada la falta de privacidad y seguridad de la información ante entornos compartidos; el surgimiento de problemas de acceso a los datos, ante la ausencia de control de los datos o pérdida de propiedad de los mismos o del control de la infraestructura; la subcontratación de servicios por el proveedor de servicios, debido al ancho de banda contratado o a la bajada del rendimiento en la transmisión de los datos, vía Internet, entre otros. Su *disponibilidad* puede verse comprometida ante múltiples copias de respaldo en diferentes localizaciones.

19. Goh y Sengsavang indican para su estudio de caso ratios significativas para la asesoría parcial (50%) y detallada (21.43%).

20. Estas ratios se agravan cuando la pregunta se realiza sobre el grado de intervención en el borrador del acuerdo, incrementándose el porcentaje de respuestas de no participación (38.10%).

21. Mediante la que se confirma, se comprueba su ausencia o una percepción deficiente.

22. (…) "one link in the chain of the quality management process. To obtain high service quality requires due diligence in the selection of service, negotiating a balanced contract and other procedures.

23. Los criterios valorados en 11 proveedores sobre capacidades y precios son: elección de localizaciones, velocidad en el acceso, grado de adopción, costes, seguridad y migración de datos. Se agrupan en 4 rangos: integridad de los datos, confiabilidad, escalabilidad, disposición y portabilidad, disponibilidad, propiedad de los datos, funcionalidad preservadora y costes.

9. REFERENCIAS

Askhoj, J.; Sugimoto, S.; Nagamori, M. (2011). Preserving records in the cloud. *Records Management Journal*, 21 (3), 175-187. https://doi.org/10.1108/09565691111186858

Asociación Española de Normalización (2014). *UNE-ISO/TR 18128 Información y documentación Apreciación del riesgo en procesos y sistemas de gestión documental.* Madrid.

Asociación Española de Normalización (2015). *UNE-ISO/TR 14721 Sistema de transferencia de datos e información espaciales. Sistema abierto de información de archivo (OAIS). Modelo de referencia.* Madrid.

Asociación Española de Normalización (2015). 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.

Asociación Española de Normalización (2016). *UNE-ISO 15489*-1 *Información y documentación. Gestión de documentos. Parte 1: Conceptos y principios*. Madrid.

Baset, S. (2012). Cloud SLAs: Present and Future. *ACM SIGOPS Operating Systems Review,* 46 (2), 57-66. https://doi.org/10.1145/2331576.2331586

Beagrie, N.; Charlesworth, A.; Miller, P. (2014). *Guidance on Cloud Storage and Digital Preservation*, 40 p. Londres: The National Archives of United Kingdom. Accesible en: http://www.nationalarchives.gov.uk/documents/archives/cloud-storage-guidance.pdf

Borglund, E. (2015). What about trust in the cloud? Archivist'wiews on Trust. *CJILS* 39 (2), 114-127. https://doi.org/10.1353/ils.2015.0017

Brown A.; Fryer, Ch. (2014). Achieving sustainable digital preservation in the cloud. *Arxius I industries Culturals*,

Girona, del 11 al 15 de octubre. Accesible en: http://www.girona.cat/web/ica2014/ponents/textos/id87.pdf

Bushey, J.; How, E.; McLelland, R. (2015). Trust in Cloud Service Contracts. Annotated Bibliography. *InterPARES Trust Project. Research Report*, 19 p. Accesible en: https://interparestrust.org/assets/public/dissemination/NA14_20150505_CloudServiceContracts_NAWorkshop5_AnnotatedBibliography.pdf

Bushey, J.; Demoulin, M.; McLelland, R.(2015). Cloud Service Contracts: an issue of Trust. *CJILS*, 39 (2), 128-153. https://doi.org/10.1353/ils.2015.0009

Bushey, J.; Demoulin, M.; How, E.; McLelland R. (2016). Lista de verificación para los contratos de servicio en la nube. Versión final. Accesible en: https://interparestrust.org/assets/public/dissemination/ABAITRUSTNA14_FINAL_checklist_julio-29_2016TRAD.AB_.pdf

CAARA-Council of Australasian Archives and Records Authorities. (2010). *ADRI. Advice on managing the recordkeeping risks associated with cloud computing. V.1.0* Accesible en: http://www.sro.wa.gov.au/sites/default/files/adri_cloud_computing.pdf

CAIS -Canadian Association for Information Science (2015). *The Canadian Journal of Information and Library Science*. Toronto: University of Toronto Press.

Comisión Europea (2014). *Cloud Services level Agreement Standardisation Guidelines.* Bruselas. Accesible en: https://ec.europa.eu/digital-single-market/en/news/cloud-service-level-agreement-standardisation-guidelines

Cotino-Hueso, L. (2015). Algunas cuestiones clave de protección de datos en la nube. Hacia una regulación nebulosa. *Revista Catalana de Dret Públic,* 51, 86-103.

European Telecommunications Standards Institute (2012). *ETSI/ TR 103 125. V1.1.1 Cloud. SLAs for cloud services*. Accesible en: http://www.etsi.org/deliver/etsi_tr/103100_103199/103125/01.01.01_60/tr_103125v010101p.pdf

Giannakouris, K; Smhily, M. (2016). Cloud Computing for business yet to go mainstream in the EU. *Eurostat. Cloud computing-Statistics on the use by enterprises*. Accesible en: http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises

Goh, E.; Sengsavang, E. (2016). Survey results on the use of cloud services for records management purposes by international organizations. *InterPARES Trust Project. Research Report,* 24 p. Accesible en: https://interparestrust.org/assets/public/dissemination/TR01_20160928_RMinIOs_TRWorkshop7_SurveyReport_Final.pdf

Government of South Australia (2015). *Cloud Computing and Records Management. Guideline. V.1.* State of Records of South Australia, Accesible en: http://government.archives.sa.gov.au/sites/default/files/20150706%20Cloud%20Computing%20and%20Records%20Management%20Final%20V1.pdf

Gulia, P.; Sood, S. (2013). Comparative Analysis of Present Day Clouds Using Service Level Agreements. *International Journal of Computer Applications,* 71 (3). Accesible en: http://research.ijcaonline.org/volume71/number3/pxc3888603.pdf

Guo, W.; Fan, Y. W.; Li, D. (2015). Archives as a trusted thier party in maintaining and preserving digital records in the cloud environment. *Record Management Journal*, 26 (2), 170-184. https://doi.org/10.1108/RMJ-07-2015-0028

Hackett, Y.; McLelland, R.; Hurley, G. (2016). Contrat terms with Cloud Service Providers. Final. V.3. *Interpares Trust Project. Final Report*. https://interparestrust.org/assets/public/dissemination/NA10_20160130_ContractTerms_InternationalPlenary3_FinalReport_Final.pdf

InterPares 3Project. (2013). *Modulo 8*. *Introducción al cómputo en la nube*. Accesible en: http://interpares.org/ip3/display_file.cfm?doc=ip3_canada_gs12_module_8_sp.pdf

Instituto Nacional de Estadística (2016). Servicios en la nube. *Cifras INE. Boletín informativo*, enero. Accesible en: http://www.ine.es/ss/Satellite?L=es_ES&c=INECifrasINE_C&cid=1259949557512&p=12547351165 67&pagename=ProductosYServicios%2FPYSLayout

Jansen, A.; Duranti, L. (2013). The InterPARES Trust Project- Trust and Digital Records in an Increasingly Networked Society. *INfuture, 2013 The Future of Information Science:"Information Governance"*, pp. 63-68. Zagreb: University of Zagreb.

Leverich, M.; Nalliah, K.; Suderman, J. (2015). Historical Study of Cloud-based Services. Final.2.0. *Interpares Trust Project. Research Report*. https://interparestrust.org/assets/public/dissemination/NA11_20150109_HistoricalStudyCloudServices_InternationalPlenary2_Report_Final.pdf

McKemmish, S. (2013). Recordkeeping and Archiving in the Cloud. Is There a Silver Lining? *Actas INfuture, 2013 The Future of Information Science: "Information Governance"*, pp. 17-29. Zagreb: University of Zagreb. Accesible en: http://infoz.ffzg.hr/INFuture/2013/papers/1-02%20McKemmish,%20Recordkeeping%20and%20Archiving%20in%20the%20Cloud.pdf

McLelland, R.; Hurey, G.; Hackett, Y.; Collins, D. (2014). Agreements between Cloud Service Providers and their Clients: A Review of Contract Terms. *Arxius i Industries Culturals,* Girona, del 11 al 15 de octubre. Accesible en http://www.girona.cat/web/ica2014/cat/comunicacions.php

McLeod, J.; Gormly, B. (2016). Economic models for cloud storage decision-making: An investigation into the use of economic models for making decisions about using the cloud for records storage. *Interpares Trust Project. Research Final Report*. Accesible en: https://interparestrust.org/assets/public/dissemination/EU20_20160609_CloudEconomicModels_EUWorkshop8_FinalReport.pdf

Ministerio de la Presidencia. (2014) *Guía de seguridad de las TIC (CCN-STIC-823). Utilización de servicios en la nube.* Madrid: Centro Criptológico Nacional. Accesible en: https://www.ccn-cert.cni.es/series-ccn-stic/800-

guia-esquema-nacional-de-seguridad/541-ccn-stic-823-seguridad-en-entornos-cloud/file.html

Oliver, G.; Knight, S. (2015). Storage is a Strategic Issue: Digital Preservation in the Cloud. *D-Lib Magazine. The Magazine of Digital Lirary Research*, 21 (3/4). Disponible en: http://www.dlib.org/dlib/march15/oliver/03oliver.html

Organización Internacional de Normalización (2011). *ISO/IEC 27031 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*. Ginebra.

Organización Internacional de Normalización (2012). *ISO/TR 17068 Information and documentation - Trusted third party repository for digital records.* Ginebra.

Organización Internacional de Normalización (2012). *ISO/16363 Space data and information transfer systems. Audit and certification of trustworthy digital repositories*. Ginebra. (UNE-ISO: 2017).

Organización Internacional de Normalización (2013). *ISO/IEC 27002. Information technology. Security techniques. Code of pratice for information Security Controls*. Ginebra.

Organización Internacional de Normalización (2014). *ISO/IEC 17788 Information Technology. Cloud computing-over views and vocabulary. Ginebra*.

Organización Internacional de Normalización (2014). *ISO/IEC 17789 Information Technology. Cloud computing-Reference arquitecture*. Ginebra.

Organización Internacional de Normalización (2014). ISO/IEC 27018 *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.* Ginebra.

Organización Internacional de Normalización (2015). ISO/IEC 27017 *Information technology. Security techniques. Code of practice information security controls based in ISO/IEC 27002 for cloud services*. Ginebra.

Organización Internacional de Normalización (2015). ISO/IEC 19831 *Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based Protocol — An Interface for Managing Cloud Infrasructure*. Ginebra.

Organización Internacional de Normalización (2016). ISO/IEC DIS 19086-1 *Information technology — Cloud computing — Service level agreement (SLA) framework — Part 1. Overview and concepts.* Ginebra.

Organización Internacional de Normalización (2016). ISO/IEC 27036-4 *Information technology. Security techniques. Information security for supplier relationships. Part 4: Guidelines for security of cloud services*. Ginebra.

Ostrzenski, V. (2013). Cloud Computing and Risk: a look at the EU and the aplication of the Data Protection Directive to cloud computing. *Infopreneurship Journal*, 1 (1), 29-38. Accesible en: http://eprints.rclis.org/20201/1/Cloud%20Computing%20and%20Risk%2C%20InfoJour%201%281%29%20pp.29-38%20.pdf

Palma-Villalón, M. V. (2014). La computación en la nube en Europa y en España: una oportunidad de negocio. *Revista Transformación Digital.* Accesible en: http://www.revistatransformaciondigital.com/2014/03/18/httpwww-revistagestiondocumental-com20140317la-computacion-en-la-nube-en-europa-y-en-espana-una-oportunidad-de-negocio/

Pan, W.; Mitchell, G. (2015). Software as a Service (SaaS) Quality Management and Service Level Agreement. *Infuture 2015: e-Institutions-Openness, Accessibility and preservation.* pp 225-234. Zagreb: University of Zagreb. https://doi.org/10.17234/INFUTURE.2015.26

Park, E. (2015). Legal compliance and technical capability for privacy-sensitive data protection in the cloud. *Infuture 2015: e-Institutions-Openness, Accessibility and preservation.* pp 131-133. Zagreb: University of Zagreb. https://doi.org/10.17234/INFUTURE.2015.15

PROV. Public Records Office of Victoria (2013). *Guideline. Cloud Computing Decision Making Version Number: 1.0.* Accesible en: https://www.prov.vic.gov.au/recordkeeping-government/document-library/cloud-g2-cloud-computing-tools-guideline

Radack, Sh. (2012). Cloud computing: a review of features, benefits, and risks, and recommendations for secure, efficient implementations. *ITL Bulletin, Junio*. Accesible en: http://csrc.nist.gov/publications/nistbul/june-2012_itl-bulletin.pdf

Sobczak, A. (2015). Public cloud archives: dream or reality? *CJILS*, 39 (2), 228-234. https://doi.org/10.1353/ils.2015.0014

Sprout, B.; Jordan, M. (2015). Archivemática as a service: COPPUL`S shared digital preservation platform. *CJILS,* 39 (2), 235-244. https://doi.org/10.1353/ils.2015.0016

Stancic, H.; Rajh, A.; Milosevic, Y. (2013). Archiving-as-a-Service. Influence of Cloud Computing on the Archival Theory and Practice. En: Duranti, L.; Shaffer, E. (eds.). *The Memory of the World in the Digital Age: Digitization and Preservation*. UNESCO, 108-125. https://www.researchgate.net/publication/310452684

Stancic, H.; Rajh, A.; Brzica, H. (2015). Archival Cloud Services: portability, continuity, and sustainability. Aspects of long-term preservation of electronically signed records. *CJILS*, 39 (2), 210-227. https://doi.org/10.1353/ils.2015.0012