

2012-06-01

Uso de cloud computing en el Sistema Nacional de Archivos de Colombia: implementación del Plan de Gestión de Documentos Vitales

Ángela Marcela Camacho Vargas

Universidad de Carlos III de Madrid, España, angelamarcelacamacho@gmail.com

Follow this and additional works at: <https://ciencia.lasalle.edu.co/co>

Citación recomendada

Camacho Vargas, Ángela Marcela (2012) "Uso de cloud computing en el Sistema Nacional de Archivos de Colombia: implementación del Plan de Gestión de Documentos Vitales," *Códices*: Iss. 1 , Article 5.

Disponible en:

This Artículo de Investigación is brought to you for free and open access by the Revistas descontinuadas at Ciencia Unisalle. It has been accepted for inclusion in *Códices* by an authorized editor of Ciencia Unisalle. For more information, please contact ciencia@lasalle.edu.co.

Uso de *cloud computing* en el Sistema Nacional de Archivos de Colombia: implementación del Plan de Gestión de Documentos Vitales

Use of Cloud Computing in the National Archives of Colombia:
Implementation of the Vital Document Management

Ángela Marcela Camacho Vargas*

Resumen

El documento presenta cuestiones técnicas acerca del *cloud computing*, tendencia del área de la informática relacionada con el almacenamiento de datos y copias de seguridad de la información. Así mismo, se mencionan instituciones, comités, sistemas, programas y proyectos que requieren articularse en Colombia para implementar una gestión nacional de atención de emergencias y preservación de la información de carácter vital, estableciendo previamente por qué es necesario desarrollar el Programa de Gestión de Documentos Vitales. Finalmente, se plantean cuestionamientos en torno a sistemas que sirven para brindar una solución a las entidades públicas y aquellas que cumplen funciones públicas en todo el país en la atención de emergencias, haciendo uso de la herramienta tecnológica del *cloud computing*. Esta, entre otros beneficios, disminuye los tiempos de búsqueda e impacta favorablemente en la gestión de recuperación de la información en documentos críticos, tan pronto como sea posible, después de un desastre.

Palabras clave: *cloud computing*, documentos vitales, Sistema Nacional de Archivos de Colombia, Archivo General de la Nación de Colombia, estrategias de gobierno en línea, ciudades digitales.

Abstract

The document presents technical issues surrounding cloud computing, computer science area trends related to data storage and backup copies of information. Similarly, there is mention of institutions, committees, systems, programs and projects required in Colombia to implement a national management of emergencies and preservation of vital information, previously established because it was necessary to develop the program to manage vital documents. Finally, it raises questions about systems that work to provide a solution to public entities and those that provide public services throughout the country in emergency care, using the technological tool of cloud computing. This, among other benefits, decreases the search times and positively impacts on the management and retrieval of information in important documents as soon as possible after a disaster.

Keywords: Cloud computing, vital documents, National System of Archives of Colombia, online government strategies, digital cities.

Recibido: 16 de enero del 2012 **Aprobado:** 17 de abril del 2012

* Profesional en Sistemas de Información, Bibliotecología y Archivística de la Universidad de La Salle, Colombia. Estudiante del Máster en Investigación en Documentación, Universidad de Carlos III de Madrid, España. Correo electrónico: angelamarcelacamacho@gmail.com

Introducción

Se ha escrito bastante sobre la gestión de riesgos y de planes de manejo de riesgos. Este documento no tratará de retomar los procedimientos que se deben seguir en estas teorías de la administración, sino ver la aplicación que tiene el uso de herramientas informáticas como el *cloud computing*, integrado a la estrategia de manejo de riesgo y atención de emergencias, concretamente el componente de documentos vitales.

Los riesgos que se identifican en la geografía nacional son de variada naturaleza, pueden ser geológicos, meteorológicos o climatológicos, o pueden ser generados por causas humanas voluntarias o accidentales que ocasionan incendios, inundaciones o contaminación, entre otros factores que alteran, deterioran, dañan o destruyen documentos de archivo o la información contenida en ellos, lo cual representa problemas para la continuidad de la gestión misional o vulnera los derechos de los ciudadanos.

Por ello, lo que se pretende a continuación es abordar el uso del *cloud computing* como alternativa para la gestión de documentos vitales de las entidades colombianas que cumplen funciones públicas, propuesta que está en sinergia con competencias de entidades y programas del Gobierno Nacional colombiano, como lo son: el Programa de Gobierno en Línea (República de Colombia, Ministerio de Tecnologías de la Información y las Comunicaciones, Gobierno en Línea (s. f.)) —liderado por el Ministerio de Tecnologías de la Información y las Comunicaciones—; el Sistema Nacional de Archivos (SNA), coordinado por el Archivo General de la Nación, ente encargado de la política archivística; y el Sistema Nacional para la Atención y Prevención de Desastres (SNAPD), liderado por el Ministerio del Interior y de Justicia.

El *cloud computing*

¿Qué es el *cloud computing*? Se trata de un modelo informático del que se empezó a hablar desde el año 2008 (Joyanes, 2010), con el cual se busca que los datos y aplicaciones se repartan en diferentes servidores. Dado que en español aún no hay uniformidad

en el término, se puede encontrar información con los siguientes títulos: “computación en la nube” o “informática en la nube” (Joyanes, 2010).

De acuerdo con lo indicado por Joyanes (2010), todavía no se encuentra una definición estándar para el concepto que encierra tener información electrónica en nubes o repartida entre computadores; sin embargo, la Agencia del Departamento de Comercio de los Estados Unidos (NIST, por sus siglas en inglés), tiene una sección dedicada a generar estándares para las tecnologías de la información, que es el Centro de Recursos de Seguridad en Computadores (Computer Security Resource Center-CSRC), que ha definido la computación en nube como:

un modelo para facilitar el acceso bajo demanda a recursos informáticos fiables –por ejemplo: redes, servidores, almacenamiento, aplicaciones, servicios– que pueden ser proporcionados rápidamente con el mínimo esfuerzo de gestión o mediante la interacción de un proveedor de servicios.

Los computadores con funciones de servidor que soportarán la nube son pertenencia de las tradicionales compañías informáticas y de servicios de Internet como Google, Microsoft, IBM, Dell, Oracle o Amazon, entre otras empresas que desean crear sus propios centros de datos para disposición de sus empleados o investigadores (Joyanes, 2010).

Dos años después de haberse lanzado el concepto, ya se han analizado los beneficios y riesgos que trae consigo la implementación de esta tecnología en las empresas y para los usuarios. A continuación se presenta los que mencionó Ignacio Llorente (2011), experto de la Unión Europea en *cloud computing*, el pasado 31 de mayo de 2011, en el VII Foro Computing, acerca de la Sociedad de la Información:

- Beneficios:
 - Ahorro de costos
 - Agilidad y capacidad elástica e instantánea
 - Comodidad por la externalización de la gestión de la infraestructura

- Calidad percibida en el uso del servicio
 - Eficiencia, derivada de la inversión de tiempo en el servicio pero no en infraestructura
 - Innovación: este es el aspecto más importante, porque supone una nueva forma de proporcionar el servicio o nuevos servicios
- Riesgos:
 - Falta de control y desconocimiento de la gestión interna del proveedor
 - Dependencia del proveedor: riesgo de cierre e imposibilidad de migrar a otro proveedor
 - Disponibilidad del servicio
 - Variaciones del rendimiento
 - Cuellos de botella en la transmisión de datos. Aplicaciones que requieran gran cantidad de datos y poco procesamiento
 - Licencias: modelos de licencia que no están preparadas para su uso en *cloud*

En cuanto a los beneficios se puede añadir que se evitará la instalación de aplicaciones en el computador de los usuarios, no será obligatorio cambiar o actualizar computadores y servidores y se podrá acceder constantemente a la información disponible en los servidores de Internet. Y respecto a los riesgos surgen otros interrogantes: ¿cómo será el trato en la privacidad de los usuarios?, ¿cuáles serán las políticas y los sistemas de protección de datos?

Muchos analistas ya se han manifestado ante los riesgos, en particular haciendo referencia a la seguridad en la nube y la necesidad de que surjan rápidamente estándares de seguridad informática en el uso de esta tecnología e invitando a los usuarios potenciales a que se evalúe si vale la pena asumir el riesgo de depositar los documentos e información de carácter “vital” para las instituciones.

Así se puede observar en la opinión que recopiló la empresa española Colt, a través de la aplicación de una encuesta a personas vinculadas con la gestión informática de instituciones europeas, como lo señala Bonilla (2011), al resaltar que “la seguridad en sí misma ya no es una cuestión que preocupe tanto, sino más bien los riesgos empresariales asociados de la transición interna de las TI a un servicio basado en nube”. También menciona que los empresarios prefieren infraestructuras privadas, antes que públicas, con el fin de priorizar la seguridad, aun teniendo que disminuir los beneficios de escalabilidad y ahorro de costos.

Con la creciente masa de información, son muchos los recursos informáticos que se requieren para el almacenamiento y procesamiento de los datos electrónicos no estructurados que representan grandes volúmenes de información, o lo que ya es conocido como *big data*.

Alrededor del *cloud computing* y los *big data* se encuentra la tendencia en la informática, como se observó en Las Vegas, Estados Unidos en mayo de 2011, en el evento de EMC World 2011 (Adeva, 2011). Así mismo, desde el año 2010 se empezaron a ver compañías que ofrecen el servicio de *cloud storage* (Mandianes, 2010), brindando a sus usuarios capacidades de almacenamiento hasta de 5 TB, soluciones que a través del uso de la plataforma en la red y de un servicio compartido mejoran la escalabilidad de los procesos y suponen a mediano plazo una disminución de costos, al mismo tiempo que un aumento en las facilidades de consulta y gestión.

Si bien es necesario evaluar las condiciones del servicio, como se hace con cualquier contrato o compra de servicios, no hay que dejar que el pánico cunda en torno a la seguridad informática, pues el riesgo de pérdida, sustracción o alteración de información siempre ha estado latente. Aunque sea la misma empresa la que provea el almacenamiento de los datos, no se debe pasar por alto que los servicios de *cloud computing* son ofrecidos por empresas multinacionales con infraestructura que desborda en seguridad con el fin de ganarse la confianza de los usuarios. Por ello, seguramente, no tardarán en mejorar y aumentar los sistemas que protejan a la nube con la mayor seguridad.

.....
 “Con la
 creciente masa
 de información,
 son muchos
 los recursos
 informáticos que
 se requieren
 para el
 almacenamiento
 y procesamiento
 de los datos
 electrónicos no
 estructurados
 que representan
 grandes
 volúmenes de
 información,
 o lo que ya es
 conocido como
big data”.

.....
“El daño o
pérdida de los
documentos
puede ser
causado por
desastres
derivados de
amenazas
geológicas como
terremotos,
tsunamis,
erupciones
volcánicas o
deslizamientos
de tierra, o
de amenazas
climáticas
como ciclones o
inundaciones”.
.....

Importancia de establecer un plan de manejo de riesgo y la gestión de documentos vitales

Es necesario empezar por indicar a qué se considera documentos vitales o esenciales. De acuerdo con lo señalado por el Archivo Nacional de los Estados Unidos, es aquella información que se necesita para realizar las actividades bajo condiciones no normales o de emergencia (única e irremplazable) y reanudar las actividades normales después, así como la información necesaria para identificar cuáles son los documentos más importantes de la institución que se encuentran relacionados con los derechos legales y financieros de las personas que pueden ser afectadas por las acciones de la entidad y con el funcionamiento propio de esta. Entonces, los documentos vitales se asocian a los registros que permiten la operación de emergencia y aquellos necesarios para proteger los derechos (United States of America, National Archives, 1999).

Estos documentos vitales poseen un valor intrínseco legal, intelectual o económico. Algunos de ellos pueden ser registros de la constitución de la entidad, títulos, pagarés, garantías, pólizas, contratos, fórmulas, licencias, objetos culturales, documentos de identificación personal o historias clínicas. No se trata de proteger los documentos históricos o de carácter patrimonial —esta suele ser una percepción equivocada—, sino de identificar la información que es vital y puede estar asociada con servicios de salud, educación, economía, etc., registrada en soportes de todo tipo.

El daño o pérdida de los documentos puede ser causado por desastres derivados de amenazas geológicas como terremotos, tsunamis, erupciones volcánicas o deslizamientos de tierra, o de amenazas climáticas como ciclones o inundaciones. En los años 2010 y 2011 los desastres a causa de estos fenómenos naturales aumentaron, dando paso a pérdidas de todo tipo, como se puede constatar por informes, noticias y registros de terremotos, tsunamis, inundaciones y erupciones volcánicas. Entre estos fenómenos se desatacaron los siguientes:

- Terremoto de Haití, enero del 2010 (Universidad de Puerto Rico, 2010)

- Terremoto y tsunami en Chile, febrero del 2010 (Barrientos, 2010)
- Terremoto de Indonesia, enero del 2011 (Universitam, 2011)
- Terremoto y tsunami de Japón, marzo del 2011 (Japón, un lustro para salir a flote, 21 de marzo del 2011)
- Inundaciones en Colombia, 2010-2011 (Organización de las Naciones Unidas, 2011)

La historia de Colombia recordará las consecuencias desastrosas de la ola invernal enfrentada entre el 2010 y el 2011. En cuanto a la actividad sísmica, el Instituto Agustín Codazzi (República de Colombia, Instituto Colombiano de Geología y Minería-Ingeominas, s. f.) señala que en todo el territorio existe una continua ocurrencia de eventos sísmicos que reflejan la dinámica posible de generar sismos de gran magnitud, considerando que en Colombia, al estar situada en el extremo noroccidental de Sudamérica, confluyen varias placas tectónicas, entre ellas las de Nazca, Caribe y Suramericana, y también se tienen registros del siglo xx de eventos tsunámicos generados por aguas del océano Pacífico.

Ante el conocimiento de estas condiciones es preciso preguntarse: ¿Hay un plan de atención de emergencias y de documentos vitales en las instituciones colombianas? En caso de que alguna institución conteste de manera afirmativa, las siguientes preguntas serán: ¿Es adecuado el plan de atención y recuperación por desastres?, ¿el país está preparado para seguir funcionando en el menor tiempo posible luego de ocurrido un desastre?

Quien escribe estas páginas considera que en el sistema de archivos de entidades públicas en Colombia no está preparado para atender un desastre tipo huracán Katrina (United States of America, Department of Commerce, 2005). Lo que queda de esto son las lecciones aprendidas por otras naciones, entre otros aspectos, en lo concerniente a la recuperación de la información y documentación que permita la activación de las instituciones que cumplen funciones públicas.

Para atender una situación de emergencia es necesario contar con información oportuna, suficiente y actualizada. Por ello se

requiere constantemente establecer o verificar la pertinencia del Programa de Documentos Vitales. A este respecto hay que responder a los siguientes interrogantes: ¿Cuáles son los procesos vitales de la institución?, ¿cuáles son los documentos vitales para soportar y reactivar estos procesos?, ¿dónde se conservan, con qué frecuencia se actualizan y en que soporte se cuentan los documentos vitales?, ¿quiénes son los responsables de generar y conservar la información vital?, ¿dónde guardar los documentos vitales?, ¿hasta cuándo guardarlos o en qué modo se actualizan?, ¿cómo acceder para recuperar la información vital para el funcionamiento de la institución?, ¿cuánto cuesta conservar la información vital?

Se debe detallar la información acerca de la documentación que se va a tratar de carácter vital (Muñoz de Solano y Palacios, 2006), con el fin de planificar el sistema de preservación de dicha información y controlar los riesgos a los que está expuesta. A este efecto, una guía que puede ayudar en la metodología para obtener esta información es la implementada por el portal de administración electrónico del Gobierno Español y documentada con la denominación de Magerit: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas (Gobierno de España, s. f.).

Las entidades públicas en la cadena de establecer un programa de documentos vitales en Colombia

El Programa de Documentos Vitales no debe planificarse e implementarse por separado; debe estar articulado con otros planes de atención de emergencias. En el caso de Colombia, debe concordar con los lineamientos del SNAPD (República de Colombia, Ministerio del Interior y de Justicia, s. f.), y otros sistemas del orden central y locales en cada departamento y municipio del territorio nacional.

En el caso de la ciudad de Bogotá, es el Fondo de Prevención y Atención de Emergencias (Fopae), entidad de la Alcaldía Mayor de Bogotá, la entidad encargada de diseñar e implementar el “Plan Distrital de Prevención y Atención de Emergencias del Distrito

Capital” (Alcaldía Mayor de Bogotá, 2010). En este plan se han determinado los riesgos y escenarios de daños y se ha establecido la integración con otros planes de instituciones distritales en caso de requerirse atención de emergencias; sin embargo, falta incluir un programa de documentos vitales para la salvaguarda de información de las entidades distritales.

En mayo del 2010 se publicaba un artículo (Zapata, 2010) que daba detalles de una encuesta aplicada por el Archivo Distrital a las entidades de la Alcaldía Mayor de Bogotá, y a las varias preguntas que se formularon en torno a los mecanismos establecidos para realizar el plan de protección de los documentos vitales, a fin de dar continuidad a la gestión de la entidades públicas distritales, las respuestas evidenciaron, en la mayoría de las entidades, la existencia del plan de continuidad de sus actividades; sin embargo, esto se encuentra asociado con el área de sistemas, la cual tradicionalmente ha demostrado mayor conciencia sobre la necesidad de proteger los activos de información, a lo cual se suman las competencias y conocimientos de los ingenieros de sistemas en materia de seguridad de la información.

En el momento de la encuesta (año 2009) se señaló que para proteger la información se realizan copias de seguridad informática y digitalización almacenadas en soportes como el DVD y los discos duros, siendo estos los mecanismos señalados como más utilizados, seguidos de la microfilmación.

En la misma encuesta se buscó identificar el rol de los archivistas o de los responsables de la gestión documental, ante el establecimiento de programas de documentos vitales, y se evidenció la carencia de dicho plan en la mayoría de las instituciones distritales. Esto deja ver que ni “el personal de archivo ni las mismas entidades tienen certeza del objetivo de este programa, y que los planes de continuidad del negocio, no consideran el programa de documentos vitales como un componente de dicho plan”, como lo afirma Zapata (2010) en su artículo.

Esta tendencia parece ser constante entre los archivistas de América Latina, aunque los “principios que dieron origen al Programa de Documentos Vitales son anterior a la formulación de las políticas de seguridad de la información surgidas de la informática”

(Zapata, 2010), con origen en el último cuarto del siglo xx cuando la Organización de las Naciones Unidas para la Educación la Ciencia y la Cultura (Unesco), al publicar en 1986 los estudios RAMP (Records and Archives Management Programme), incorporó en el Programa de Gestión de Documentos el Subprograma de Gestión de Documentos Vitales (o Esenciales).

El Programa de Documentos Vitales debe estar integrado con el Programa de Gestión Documental (PGD). Así lo ha considerado el Archivo General de la Nación, ente rector de la política archivística en Colombia, dirigiéndose a las entidades públicas y privadas que cumplen funciones públicas, sin importar su naturaleza orgánico-funcional (República de Colombia, Ministerio de Cultura, Archivo General de la Nación-AGN, s. f.) A este efecto, se ha establecido un marco legal, conceptual y técnico, así como una orientación que brinda el Sistema Nacional de Archivos de Colombia (SNA), el cual está conformado por las instituciones archivísticas que cumplen funciones públicas y las entidades privadas que deseen pertenecer al sistema, a las cuales se les debe proporcionar orientación sobre organización, manejo, preservación, conservación, servicio y control de los archivos (República de Colombia, AGN, 2011).

Fue así como en abril del 2001 el Archivo General de la Nación, a causa de la afectación de los archivos por la ola invernal en todo el país, realizó observaciones para la preservación de la documentación, recordando lo que ya había señalado en otros documentos en cuanto a las instalaciones de unidades y depósitos para el almacenamiento de archivos, así como la prestación de una atención primaria en caso de que se haya afectado la documentación. Además, mencionó su alcance y dejó ver la preocupación del Gobierno. En todo esto se percibe la necesidad de establecer un programa de documentos vitales en el territorio nacional:

Teniendo presente que la prioridad del Gobierno Nacional es la asistencia humanitaria de esta emergencia, pero que también existen otras áreas que deben ser consideradas por parte de las entidades, se hace necesario tomar medidas preventivas y correctivas para la protección de los documentos producidos por Gobernaciones, Alcaldías y entidades públicas y privadas con funciones públicas de

los órdenes departamental, distrital y municipal, pues su preservación afecta de modo directo los derechos de los ciudadanos, a futuro. (República de Colombia, AGN, 29 de abril del 2011)

Adicionalmente, entre las entidades que se necesita que se articulen para la formulación e implementación del Programa de Documentos Vitales, se encuentra el Ministerio de las Tecnologías de Información y las Comunicaciones (s. f.), que tiene a cargo la coordinación de la estrategia de Gobierno en Línea, y este a su vez del Programa de Agenda de Conectividad, que tiene participación en la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública, a la cual también debería pertenecer el Archivo General de la Nación (República de Colombia, AGN, s. f.).

El propósito de dicha comisión es el de definir estrategias y políticas para la producción de la información necesaria y lograr así una óptima generación de bienes y servicios públicos por parte del Estado. Además, en sus objetivos señala la eliminación de la duplicidad de la información, optimización e intercambio y uso de tecnologías de la información y las comunicaciones en la administración pública (República de Colombia, AGN, s. f.). Para esto último resulta importante la aparición de la tecnología de *cloud computing* como herramienta para la conservación y recuperación de documentos. Esta tecnología siendo un servicio público en el mundo, será al mismo tiempo tan privada como lo establezcan los términos contractuales y los sistemas de seguridad que se desarrollen en el área de la informática. Puede considerarse su uso en caso de atención de emergencia.

La tecnología *cloud computing* puede ser aplicada al Programa de Documentos Vitales

Elaborar e implementar el programa de documentos vitales es una labor multidisciplinar en la cual se requiere convergencia en diferentes etapas del proyecto de los conocimientos de archivistas, historiadores, restauradores, ingenieros de sistemas, administradores, ingenieros industriales, abogados, economistas, estadísticos, gestores de bases de datos y sistemas de información, gestores de conocimiento, analistas de gestión del riesgo y,

en general, todos aquellos que por su experiencia o competencia se especialicen en la gestión de documentos e información y la gestión de riesgos, de modo que se puedan analizar las alternativas para la preservación de los documentos y archivos electrónicos (Zapata, 2010).

Como lo indica la Norma ISO 15489 al referirse a las competencias que deben tener los gestores de documentos, que si bien ni la primera ni en la segunda parte indica una profesión específica, por ser una norma internacional que debe acoplarse a la situación de varios países y contextos de desarrollo, este profesional tiene entre otras funciones: “g) Definir medidas de contingencia con el fin de evitar situaciones de riesgo y participar en la elaboración del plan de gestión de desastres, especificando los documentos vitales para la continuidad de las actividades de la organización” (Alonso, García Alsina y Lloveras i Moreno, 2008).

Esto conlleva retos y oportunidades para los profesionales de la gestión de la información —la preservación de la documentación no solo debe estar a cargo de sectores privilegiados del medio empresarial— y, además, requiere trabajar con personal calificado para el tratamiento adecuado de los activos de información que son la razón principal de la archivística.

Es por ello que varios autores se han referido a la necesidad y forma que debe considerarse para la conservación de información en las empresas, como lo señalan Esteban Navarro y Navarro Bonilla al hablar de tres retos para la preservación de información en formato electrónico:

- 1) creación de depósitos de conservación adecuados y seguros, tanto físico-lógicos (discos compactos, videodiscos digitales, etc.) para los originales y las copias, como contenedores y almacenes de estos depósitos;
- 2) adopción de nuevas medidas de prevención del deterioro ya que el soporte de lo digital es más vulnerable al paso del tiempo que el papel;
- 3) garantizar a lo largo del tiempo el acceso y la legibilidad de la información contenida en los soportes, haciendo frente a la obsolescencia técnica de los depósitos, del hardware y del software (Esteban Navarro y Navarro Bonilla, 2003, p. 276).

Con lo anterior los autores en mención aluden a que la estrategia para gestionar los retos mencionados debe estar registrada en un

programa de intervención que considere el plan de conservación preventiva contra agentes de deterioro, virus informáticos y obsolescencia de sistemas informáticos, que además debe indicar las medidas de seguridad física-lógica y de actuación ante desastres.

Hacer preservación de información a través de soportes como discos compactos, DVD o discos duros ubicados en la misma área de la empresa no es lo recomendable. Entre las tendencias del mercado informático y la evolución de herramientas tecnológicas se han desarrollado áreas de negocio especializada en *back up*, las cuales ya empiezan a ofrecer el uso del *cloud computing* como tecnología que brinda solución a los problemas de almacenamiento y acceso a la información electrónica y que se convertirá en una alternativa de solución para el desarrollo de los programas de documentos vitales, haciendo que bajen los costos de infraestructuras tecnológicas (*hardware*, *software* y actualizaciones de aplicaciones) y permitiendo el acceso a la información desde cualquier lugar del planeta, con los debidos perfiles de usuarios y contando con el soporte y garantías que ofrecen los gigantes de la informática que desarrollan esta área de negocio.

Así lo señalan varias empresas, entre las que se encuentra Gartner, al exponer las principales tendencias para el mercado del *backup*: “1) Soluciones de hardware basadas en disco; 2) Soluciones que incluyan capacidades de backup para servidores virtualizados; 3) Disminución del tiempo preciso para hacer el backup y para la recuperación de la información; 4) Demanda del modelo ‘cloud’ para backup y recuperación, sobre todo para dispositivos portátiles y de escritorio y oficinas remotas” (Gartner, 2011).

La empresa española dedicada a la tecnología de gestión de información, EMC, también está interesada en la prestación de los servicios de *backup* y recuperación ante desastres. En 2008 —época en que surgió el termino de *cloud computing*—, creó una división especializada, específica para esta área, a la que se denominó Backup & Recovery Solutions (BRS). Esta también ofrece servicios integrados de NetWorker y ha hecho alianzas estratégicas con empresas especializadas en *backup* como Ermestel, IPM, Omega, Peripherals, Powernet y Prosoll (La virtualización y la deduplicación están impulsando el *backup* de nueva generación, 2011).

En mayo del 2011 en el evento de Las Vegas de EMC World, se explicó cómo ofrecer “tecnologías para la realización de *backups*, permite a los usuarios disponer de la capacidad, la escalabilidad y el rendimiento requerido para almacenar y proteger con eficacia grandes conjuntos de datos” (Información siempre segura y disponible, 2011), *big data*, obteniendo en un solo sistema almacenamiento, replicación, encriptado, automatización de servicios en la red, para atender la recuperación de desastres, la protección de datos de oficinas remotas y la consolidación de cintas de múltiples sitios (Información siempre segura y disponible, 2011).

De acuerdo con lo que mencionó Alfonso Veloza (2011), directivo de investigación de Gartner, “las ciudades están invirtiendo en nuevos servicios municipales, en los que las nuevas plataformas cloud jugaran un papel muy importante integrando todos los servicios y constituyendo así las Smart cities”. Estas ciudades inteligentes serán las urbes del futuro e integrarán programas que disminuyan los desplazamientos; aumenten la eficiencia en teletrabajo; realicen monitorización de las emisiones de carbono; permitan la ubicación, la sostenibilidad y la inclusión social en la prestación de servicios públicos como transporte, educación, salud, seguridad, comunicación u otros servicios locales como alumbrado, sistemas de urgencias, etc., que hacen parte del concepto.

Sin embargo, el sector público realizará la migración al *cloud* de manera más pausada que el sector privado, “debido principalmente a la falta de cualificación interna y las dudas sobre la seguridad de los datos” (Sector público y la nube, 2011), aunque como menciona Albert Delgado (2011) al referirse a la desconfianza que se percibe respecto a la seguridad del *cloud*, “las empresas medianas y pequeñas van a tener más seguridad en un entorno cloud público que la que tienen ahora y sin embargo desconfían”.

Tanto en el sector público como en el sector privado se perciben ventajas en la implementación del *cloud computing*, entre las que se mencionan ahorro de costos, flexibilidad, aumento de la eficiencia y escalabilidad. En las entidades públicas las preocupaciones más importantes giran en torno a la fiabilidad y a la pérdida del control operativo (Delgado, 2011). También se consideran inhibidores para adoptar el *cloud* las características de

seguridad en datos e infraestructura, el rendimiento y la disponibilidad de la información (Inseguridad de la nube, s. f., tratándose de un “modelo no diseñado para las variaciones de volumen, la reversión de servicios, el cambio de proveedores y una endeble política de seguridad ambiental” (Delgado, 2011).

Ante la posibilidad de implementar el Programa de Documentos Vitales de toda la nación haciendo uso del *cloud computing*, deben considerarse entre las dificultades de los municipios para desarrollar el programa en mención, la preparación que tienen los funcionarios públicos para realizar la identificación de los tipos documentales vitales y la disponibilidad económica para sostener la tecnología requerida en estos programas. Respecto al segundo aspecto, el ahorro en costos es otro beneficio que tiene adoptar como modelo de solución el uso compartido de los recursos del *cloud computing* para las instituciones del Gobierno colombiano.

Algunos preguntarán: ¿Cómo pretender desarrollar un programa de documentos vitales sin previamente haber organizado los archivos físicos? Ante las múltiples respuestas que pueden seguir, cabe preguntarse antes: ¿Será necesario tener los archivos organizados para identificar los documentos vitales de las instituciones y de las personas?, ¿se requiere destinar recursos (económicos, humanos, tecnológicos) para programas de atención de emergencias antes que cubrir las necesidades de la gestión cotidiana? En las posibles respuestas que se puedan suscitar vale la pena considerar que los desastres no ocurren cuando todo está bajo control. En caso de ocurrencia de una emergencia no habrá que preocuparse por la gestión cotidiana y, en cambio, sí será necesario aumentar los esfuerzos para recuperar lo vital y así poder reanudar los servicios o demostrar los derechos de personas e instituciones. Así que mientras en la organización se obtienen los niveles ideales, se podrá rescatar lo vital.

Si la iniciativa de gestión parte del nivel central y es replicada para dar cobertura en todos los niveles del Estado, se obtendrá un beneficio común sin generar un gasto que se aumente pagando por separado millones de pesos por cada institución, departamento o municipio, sino una inversión para proporcionar seguridad de la información, continuidad del negocio y respaldo a los derechos de los ciudadanos e instituciones.

.....
“Los usuarios
del sistema
de gestión de
documentos
vitales pueden
acceder a la
información
y realizar
actividades
de captura,
administración
y difusión de
los documentos
con mayor o
menor grado
de dominio, de
acuerdo con
el perfil de
usuarios que se
les asigne”.
.....

El *cloud computing* sirve para muchas aplicaciones, tantas como sean contratadas con el proveedor, pero el objetivo de este documento se centra en el uso del *cloud* en programas de documentos vitales de entidades que cumplan funciones públicas. Por esta razón, a continuación se presentan algunas características que deben considerarse en el diseño de la propuesta e implementación.

¿Cómo puede ser el esquema? Para el programa de documentos vitales se puede adquirir un servicio de acceso al *cloud* de tipo “nube pública”, en la que al servicio ofrecido por el proveedor tienen acceso varios clientes (Joyanes Aguilar, 2010), que serán las entidades que hacen parte del Sistema Nacional de Archivos, con licencia para usar una “infraestructura como servicios (IaaS)” (Joyanes Aguilar, 2010). De esta manera, tendrán acceso al servicio de almacenamiento y servidores, que se complementa con el uso de paquetes de “software como servicios (SaaS)” (Joyanes Aguilar, 2010) que permitan acceder a aplicaciones sin importar el lugar o el equipo a través del cual se ingrese, y se implementaría de modo escalable por sectores, regiones y niveles del orden nacional.

Tradicionalmente y como medida de seguridad informática y respaldo de la información, se implementan sistemas que requieren la generación de copias para almacenarse en uno o varios servidores ubicados en lugares diferentes al centro de producción, que en materia de atención de desastres debería estar en ubicado en otra ciudad o país, lo cual será más fácil y accesible a través de los servicios ofrecidos en el *cloud computing*.

Los usuarios del sistema de gestión de documentos vitales pueden acceder a la información y realizar actividades de captura, administración y difusión de los documentos con mayor o menor grado de dominio, de acuerdo con el perfil de usuarios que se les asigne. No se trata de subir todo, es necesario seleccionar los temas estratégicos o vitales por áreas de gestión en los sectores de gobierno (alcaldías, gobernaciones), salud y educación, entre otros, y así mismo desarrollar las estrategias de implementación.

En la etapa de diagnóstico y formulación del programa se identificarán entidades que ya posean bases de datos y documentación

vital de los ciudadanos en medio digital y con sistemas de seguridad, como lo puede ser la Registraduría Nacional del Estado Civil con la información de documentos de identidad en Colombia, o las historias clínicas de algunos centros de salud o entidades prestadoras de atención médica, que en caso de atención de emergencias y recuperación de desastres podrían acceder a la información desde un dispositivo móvil con acceso a red.

Algunas consideraciones finales tienen que ver con identificar los documentos vitales comunes a las entidades públicas, o aquellas que cumplen funciones públicas en Colombia, y los documentos vitales misionales de cada institución; establecer si se requiere declarar a través de la normatividad nacional algunos tipos documentales como de carácter vital; y posteriormente, por sectores de la función pública, implementar las estrategias de selección y tratamiento para ser incorporadas en el *cloud*.

En cuanto a escoger al proveedor del servicio, será necesario responder entre otras las preguntas que se presentan a continuación, de acuerdo con un informe especial de *Business Week* del 2008, presentado por Harry Lewis, donde se señalan las cuestiones que deben hacerse antes de confiar los datos de una institución a un proveedor externo (Joyanes Aguilar, 2010):

- ¿Quién puede ver los datos? ¿Cómo se garantiza la privacidad?
- ¿Qué pasa si no se paga la factura mensual, anual? ¿Se pueden borrar bruscamente todos los datos del cliente por este motivo?
- ¿Se hacen más copias de seguridad de los datos? ¿Qué sucede si se pierden? ¿Existe un contrato de garantía?
- ¿Cómo se garantiza el uso de información privilegiada?
- ¿Cómo tratará al usuario la “nube” ante hábitos normales? ¿Se puede discriminar por razón de raza, sexo, religión, nacionalidad? ¿Se puede fingir el *copyright*? ¿Qué sucede con la licencia *copyleft* de Creative Commons?
- ¿Cuál es el control de acceso? ¿Cómo manejar las contraseñas, problemas en el uso?
- ¿Desea que sus empleados reciban publicidad con su correo-e u otras herramientas ofimáticas?

- ¿Cuál será la estrategia de salida de la nube? ¿Cómo se realizará la migración en ambas direcciones? ¿Cómo se recuperan datos almacenados?, etc.

A las cuales se pueden agregar estas:

- Si se modifica o actualiza constantemente el documento declarado como vital, ¿con qué periodicidad y hasta cuántas veces se puede acceder a la nube para reemplazar el nuevo documento?
- ¿Qué medidas de seguridad, acceso y auditoria de los datos se implementarán?
- ¿Dónde se localizarán los datos almacenados?
- Si la emergencia no ocurre en territorio del cliente, sino donde el proveedor del servicio tiene ubicados sus servidores, ¿cómo atenderá el proveedor ante tiempos de caída del servicio? y ¿Estará preparado el proveedor para la atención de desastres en su propia compañía sin que afecten la gestión del cliente?
- ¿Cuánta capacidad se destinará para cada municipio en su almacenamiento?
- ¿Quién debe declarar los documentos vitales en la nube?
- ¿Cuáles herramientas de visualización de datos se proveerían si se requiere acceder a la información en caso de emergencia?

Finalmente, debe ser un ejercicio continuo medir el retorno de inversión. Para ello es necesario recolectar información de costos, éxito de adopción, mantenimiento, formación previa, durante y después de la implementación de un programa de documentos vitales.

Referencias

- Adeva, A. (2011, 18 de mayo). EMC centra sus nuevos lanzamientos en los *big data* y el *cloud computing*. *Computing* (España), (663).
- Alcaldía Mayor de Bogotá. Plan de emergencias de Bogotá (2010). Recuperado el 24 de junio del 2011 de http://www.fopae.gov.co/portal/page/portal/FOPAE_V2/PDPAE, p. 64.

- Alonso, J. A., García Alsina, M. y Lloveras i Moreno, M. R. (2008). La norma ISO 15489: un marco sistemático de buenas prácticas de gestión documental en las organizaciones. *Item*, (47).
- Barrientos, S. (2010, 27 de mayo). *Servicio sismológico. Informe técnico*. Santiago de Chile: Universidad de Chile. Recuperado el 23 de junio del 2011 de [http://www2.ing.puc.cl/~wwwice/sismologia/INFORME_TECNICO%20\(may%2027\).pdf](http://www2.ing.puc.cl/~wwwice/sismologia/INFORME_TECNICO%20(may%2027).pdf)
- Bonilla, L. (2011, 24 de mayo). La gestión del riesgo constituye la principal preocupación del *cloud computing*. *Computing* (España). Recuperado el 23 de junio del 2011de <http://www.computing.es>. No 666.
- Delgado, A. (2011). El concepto *cloud* está sobreexplotado. *Computing* (España), 28-31. Recuperado el 23 de junio del 2011 de <http://www.computing.es/e-administracion/noticias/1035791000901/albert-delgado-penteo-concepto.1.html>
- Esteban Navarro, M. A., y Navarro Bonilla, D. (2003). Gestión del conocimiento y servicios de inteligencia: la dimensión estratégica de la información. *El Profesional de la Información* (Madrid), 12 (4), 276.
- Gartner (2011). Las últimas tendencias en el CPD aceleran la transformación de las tecnologías de backup. *Computerworld - La actualidad TIC* (España), 1263.
- Gobierno de España, Ministerio de Política Territorial y Administración Pública (s. f.). Portal de Administración Electrónica (PAE). Magerit versión 2. Recuperado el 23 de junio del 2011 de http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184
- Japón, un lustro para salir a flote (2011, 21 de marzo). *BBC Mundo* (Redacción - Noticias de la BBC). Recuperado el 23 de junio del 2011 de http://www.bbc.co.uk/mundo/noticias/2011/03/110321_recuperacion_japon_cr.shtml
- Joyanes Aguilar, L. (2010). Computación en nube (*cloud computing*) y centros de datos: la nueva revolución industrial. ¿Cómo cambiará el trabajo en organizaciones y empresas? *Sociedad y Utopía. Revista de Ciencias Sociales* (Universidad Pontificia de Salamanca) (36), 111-128.
- La inseguridad de la nube (s. f.). *Computerwolrd* (España). Recuperado el 23 de junio del 2011 de <http://www.idg.es/computerworld/La-inseguridad-de-la-nube/seccion-mercado/articulo-203754>
- La virtualización y la deduplicación están impulsando el *backup* de nueva generación (2011). *Computerworld, La actualidad TIC* (España), (1263).
- Llorente, I. (2011). El *cloud* como soporte a la innovación y generación de negocio. *Computing* (España), (666), 24-26.

- Mandianes, A (2010, 13 de enero). Arsys apuesta por el *cloud storage*. *Computing* (España), (666). Recuperado el 23 de junio del 2011 de <http://www.computing.es>
- Muñoz de Solano y Palacios, B. (2006). La gestión de riesgos orientada a la conservación de información en soporte digital. *Documentación de las Ciencias de la Información-Cindoc (CSIC)* (Madrid), 29, 125-140.
- Organización de las Naciones Unidas, Office for the Coordination of Humanitarian Affairs (Ochoa), Colombia ssh.org: Sala de Situación Humanitaria. (2011). *Colombia - Inundaciones 2010-2011. Informe de situación de marzo de 2011*. Recuperado el 23 de junio del 2011 de http://www.colombiassh.org/site/IMG/pdf/Sit_Rep_27_Inundaciones_Colombia.pdf
- República de Colombia, Archivo General de la Nación-AGN (2011). *Sistema Nacional de Archivos*. Bogotá: AGN. Recuperado el 24 de junio del 2011 de <http://www.archivogeneral.gov.co/index.php?idcategoria=1180>
- República de Colombia, Archivo General de la Nación-AGN (s. f.). *Programa de Gestión Documental*. Bogotá: AGN. Recuperado el 23 de junio del 2011 de <http://www.archivogeneral.gov.co/index.php?idcategoria=1233>
- República de Colombia, Archivo General de la Nación-AGN (2011, abril 29). *Circular Externa No. 001. Asunto: Protección de archivos por ola invernal*. Bogotá: AGN.
- República de Colombia, Instituto Colombiano de Geología y Minería - Ingeominas (s. f.). *Material educativo*. Recuperado el 23 de junio del 2011 de http://seisan.ingeominas.gov.co/RSNC/index.php?option=com_content&view=article&id=48&Itemid=60
- República de Colombia, Ministerio de Tecnologías de la Información y las Comunicaciones, Gobierno en Línea (s. f.). Recuperado el 24 de julio del 2011 de <http://www.gobiernoenlinea.gov.co/web/guest;jsessionid=B75219421C16FE49660175D4A6FBFDED>
- República de Colombia, Ministerio del Interior y de Justicia. *Sistema Nacional para la Atención y Prevención de Desastres* (Snapd) (s. f.). Recuperado el 23 de junio del 2011 de <http://www.sigpad.gov.co/sigpad/index.aspx>
- Sector público y la nube (2011, 1º de junio). *Computerworld* (España). Recuperado el 23 de junio del 2011 de <http://www.idg.es/computerworld/Sector-publico-y-la-nube/seccion-/articulo-203599>
- United States of America, Department of Commerce, National Oceanic and Atmospheric Administration, National Weather Service, Service Assessment (2005, 23-31 de agosto). *Hurricane Katrina*. Recuperado el 25 de junio del 2011 de <http://www.weather.gov/os/assessments/pdfs/Katrina.pdf>

- United States of America, National Archives (1999). *Records management: vital records and records disaster mitigation and recovery: an instructional guide*. Recuperado el 23 de junio del 2011 de <http://www.archives.gov/records-mgmt/vital-records/>
- Universidad de Puerto Rico, Recinto Universitario de Mayagüez, Departamento de Geología, Red Sísmica de Puerto Rico (2010, 12 de enero). *Informe especial: terremoto de Haití*. Recuperado el 23 de junio del 2011 de http://redsismica.uprm.edu/Spanish/informacion/informes_especiales/Informe_Especial_Haiti_2010.pdf
- Universitam (2011, 26 de enero). *Informe sismológico mundial*, Simeulue, Indonesia University. Recuperado el 23 de junio del 2011 de <http://universitam.com/academicos/?p=8315>
- Veloza, A. (2011). *Smart cities: el cloud aumenta el valor del servicio municipal*. *Computing* (España), (666), 10-14.
- Zapata, C. A. (2010). La preservación de documentos vitales: aproximación a la situación actual en el Distrito Capital. *Investigación Bibliotecológicas* (México), 24 (51), 147-171.