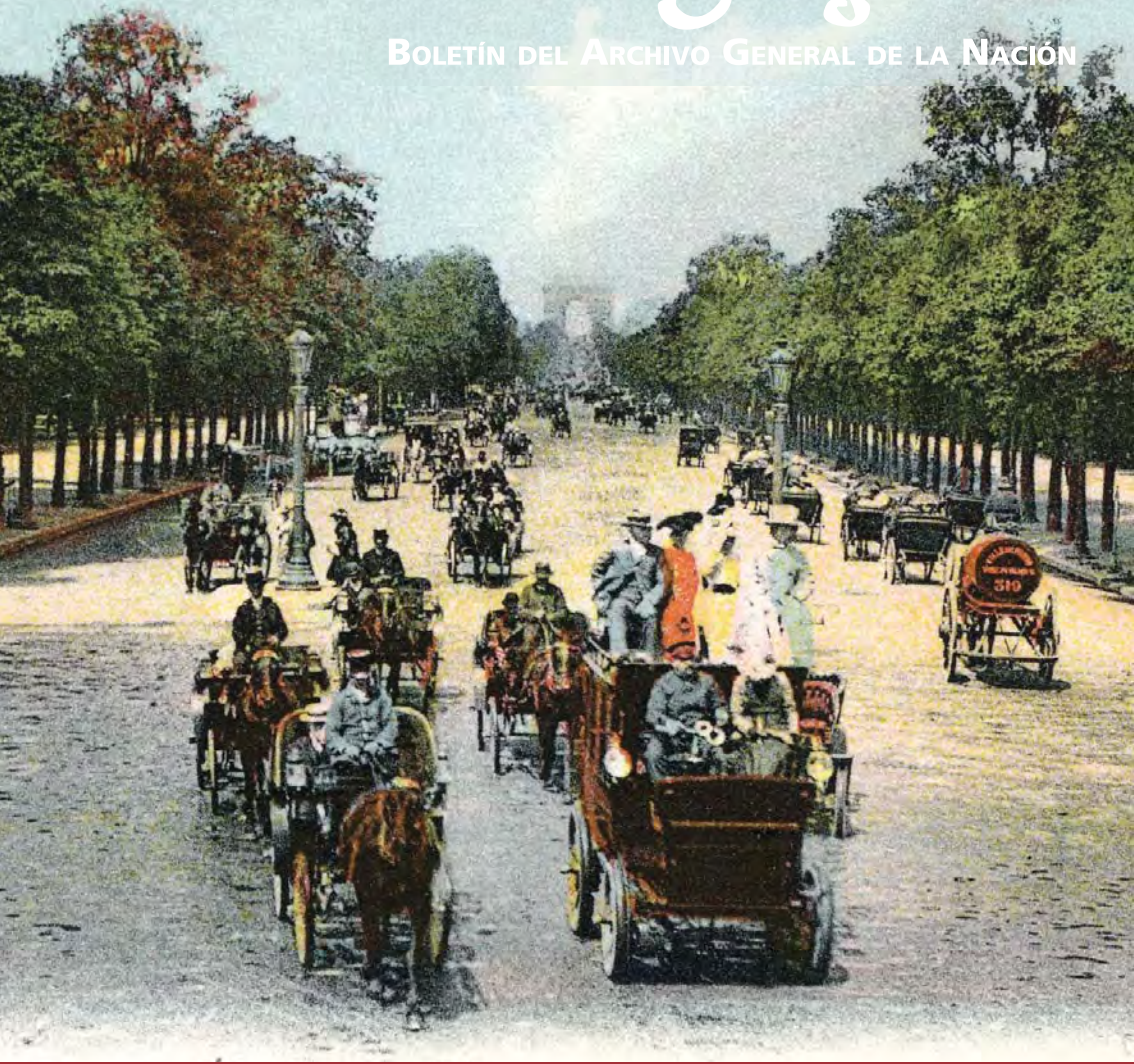
Legajos

Boletín del Archivo General de la Nación



7ª época, año 4, número 16, abril-junio, 2013

Paris. Les Champs Elysées

AGN, *Colección Luis y Leopoldo Zamora Plowes*, Tarjetas postales, 42-30.

Legajos

Boletín del Archivo General de la Nación
7ª época, año 4, núm. 16, abril-junio, 2013

Legajos

Boletín del Archivo General de la Nación

Legajos. Boletín del Archivo General de la Nación, séptima época, año 4, número 16, abril-junio de 2013, es una publicación trimestral del Archivo General de la Nación, donde se publica y distribuye, con domicilio en Eduardo Molina 113, Col. Penitenciaría Ampliación, Delegación Venustiano Carranza, C. P. 15350, México D. F.

Tel. 51 33 99 00, Exts. 19325, 19424 y 19330
Correos electrónicos: boletinagn@agn.gob.mx; mcsilva@agn.gob.mx;
Página web: www.agn.gob.mx

Editor responsable: Marco Antonio Silva Martínez.

Licitud de título y licitud de contenido otorgado por la Comisión Calificadora de Publicaciones y Revistas Ilustradas de la Secretaría de Gobernación número: 15036.

ISSN-0185-1926

Legajos. Boletín del Archivo General de la Nación se terminó de imprimir en julio de 2013 en Tipográfica, S. A. de C. V. Imagen núm. 26, Col. Lomas de San Ángel Inn, C. P. 01790, México, D. F.

Consejo Editorial

Investigador (a) de temas históricos y de archivística:

Legajos

Boletín del Archivo General de la Nación

Es una publicación trimestral especializada en historia y archivística editada por el Archivo General de la Nación desde 1930.

El propósito de esta revista es la publicación de textos originales basados en investigaciones fundamentalmente académicas que contribuyan al estudio, difusión y reinterpretación de temas relacionados con la historia y la archivística, así como a la divulgación del acervo documental que resguarda el Archivo General de la Nación de México.

Todos los artículos deben someterse a dictamen bajo el sistema doble ciego: el evaluador desconoce el nombre y procedencia del autor, y éste recibe los comentarios de aprobación o rechazo sin saber quién dictaminó su artículo.

Si deseas someter un artículo a dictamen para su posible publicación en

Legajos. *Boletín del Archivo General de la Nación,*

Envíanos tu texto a los correos electrónicos:

boletinagn@agn.gob.mx
mcsilva@agn.gob.mx

También consulta

las normas editoriales en las últimas páginas de esta edición y en:

www.agn.gob.mx/menuprincipal/difusion/publicaciones/inv_boletin.html

Tabla de contenido

Reseñas

Documentos del Archivo General de la Nación

municipales, Archivos universitarios para cuestiones como cuadros de clasificación o tablas de valoración de series comunes. Actualmente, los esfuerzos plurales para las mismas cosas no tienen sentido.

Bibliografía

Heredia Herrera, Antonia, "Archivística y Legislación: términos y conceptos", *Tábula*, Salamanca, núm. 15, 2012, pp. 363-381.

Heredia Herrera, Antonia: "¿Permanencia, renovación, desvirtuación de conceptos archivísticos?", *Legajos. Boletín del Archivo General de la Nación*, núm. 11, enero-marzo 2012, pp. 107-124.

Mendoza Navarro, Aida, "Marco jurídico y reglamentario de Archivos en Iberoamérica", curso de experto en conservación y gestión del patrimonio documental, UNIA, 2012, p. 4.

TEAM México, Glosario InterPARES de preservación digital en español. Versión 3.0., 2012.

La nube

Alejandro Delgado Gómez*

Resumen

El presente artículo explora el modelo de negocio conocido como *Cloud Computing* y sus relaciones con la gestión de documentos y de información. En primer lugar definimos qué es el *Cloud Computing* y sus propiedades y modelos de uso. En segundo lugar, describimos tanto los beneficios como los retos derivados del *Cloud Computing*. Por último, argumentamos que, de hecho, los riesgos existen ya desde antes de la existencia del fenómeno.

Palabras clave: *Cloud Computing*, confiabilidad, sistemas distribuidos de información.

Abstract

This article explores the business model known as Cloud Computing and its relationships with recordkeeping and information management. First, we define what is Cloud Computing, and its properties and use models. Secondly, we describe both benefits and challenges derived from the Cloud Computing. Finally, we argue that, in fact, risks already existed, before the emergence of this phenomenon.

Keywords: Cloud Computing, Distributed Information Systems, Trustworthiness.

*Ayuntamiento de Cartagena-Archivo Municipal

Introducción

El presente artículo pretende explorar el modelo de negocio conocido como *Cloud Computing* y sus relaciones con la gestión de documentos y de información. Los motivos de esta exploración son varios y de diversa naturaleza, pero no es el menor de ellos el hecho de que, con independencia del esfuerzo promocional de la industria y de la enorme cantidad de literatura que toda tendencia novedosa genera, el trabajo cotidiano en la nube será una realidad más bien a corto que a largo plazo, en primer lugar, simplemente porque es más barato, más cómodo y más operativo que otros modelos en uso; y, en segundo, porque básicamente no hay que inventar ninguna tecnología, sino tan sólo re-ordenar algunas de las existentes. De hecho, es más que probable que en este momento ya estemos utilizando en nuestras organizaciones algunas de tales tecnologías para el soporte o para la realización de ciertos procesos o de determinadas tareas.

Es cierto que el fenómeno del *Cloud Computing* genera inquietud entre los gestores de documentos y de información, no siendo descabellado argumentar que quizá derive del temor a perder una potencial posición de privilegio como "guardianes de los documentos", tristemente uno de los pocos privilegios del profesional. Sin embargo, contra esta inquietud cabe argumentar que los sistemas de gestión de documentos se encuentran, en general, inscritos en los sistemas más amplios de gestión de las organizaciones, que los controlan, digamos, mediante sus áreas o servicios de tecnologías de la información. En un escenario en el que el mundo aún no ha salido de una de las peores crisis globales jamás conocidas y en el que la salida parece pasar por nuevas economías enfocadas hacia marcos tecnológicos sostenibles, pedir a una organización, por ejemplo, que no ahorre costes colocando sus datos en la nube se diría ingenuo, cuando no, si se piensa detenidamente, incluso poco ético. Además, la decidida apuesta de la industria a favor de este modelo de negocio y la presión publicitaria, que descubre cada día un nuevo beneficio y un caso de uso mejor que el del día anterior, está convenciendo a muchos. Este convencimiento no tiene por qué estar equivocado.

Puesto que cada momento genera un estado del arte de la tecnología, y ésta se ha utilizado de la mejor manera posible en cada momento para

crear, gestionar, conservar y utilizar documentos e información, el presente artículo no pretende ni demonizar ni bendecir el modelo de negocio del *Cloud Computing*, sino estudiarlo tan objetivamente como sea posible en las condiciones de su ocurrencia, para poder crear, gestionar, conservar y utilizar documentos e información "en nuestro tiempo" y también en las mejores condiciones posibles. De hecho, la nube ya está conformando desde hace tiempo las conductas de gestión de documentos personales, y ha comenzado a conformar también las organizativas, tanto privadas como gubernamentales. Esto no es, en principio, ni bueno ni malo; es simplemente el signo de nuestro tiempo, y la inquietud, que no va a cambiar este signo, debería venir reemplazada por un análisis riguroso y detallado de los indudables beneficios, pero también de los retos, de las tecnologías en uso, con el objeto, por una parte, de ajustar adecuadamente nuestros procesos a las mismas; y, por otra, de descubrir el modo en que los documentos y la información, en un nuevo entorno, pueden seguir siendo evidencia de acciones. Desde luego, el hecho de que los documentos, la información, los datos, no estén detrás de las paredes de nuestro archivo no implica necesariamente que no puedan crearse, gestionarse, conservarse y utilizarse documentos, información y datos, sino más bien que estas actividades han de ejecutarse de otra manera. De igual modo, no implica la desaparición del concepto de evidencia, sino más bien la necesidad de que éste sea repensado, necesidad, por lo demás, que no se plantea por primera vez ni en el tiempo ni en el espacio en la historia de la humanidad.

Así, pues, definiremos qué se entiende por *Cloud Computing* y sus propiedades y modelos de uso. Esta definición, por supuesto, ya ha sido emprendida, pero no parece de más retomarla en el contexto del presente artículo, siquiera a efectos de comodidad de lectura. Además, expondremos tanto los beneficios como los retos que otros han descubierto en el fenómeno del *Cloud Computing*, e intentaremos argumentar que, de hecho, los riesgos existen ya desde antes de la existencia del fenómeno. Este marco inicial debería servir para profundizar en un cuerpo central de exploración, a saber: cómo se crean documentos, información y datos en este marco; cómo deberían gestionarse, conservarse y utilizarse; y cómo deberían establecerse las oportunas garantías para que tales resultados sigan siendo evidencia de acciones, es decir, sigan manteniendo las propiedades

de autenticidad, fiabilidad, integridad y disponibilidad que los convierten, más allá de mera información, en documentos de archivo.

Definiciones

El *Cloud Computing* no es internet, ni las conocidas como granjas de servidores, ni la web 2.0, sino más bien una combinación de tecnologías, entre las que no tienen por qué no encontrarse las mencionadas, para la prestación de servicios remotos. Una definición más refinada y mejor consolidada la proporciona el *Information Technology Laboratory del National Institute of Standards and Technology* (NIST):

> El Cloud Computing es un modelo para hacer posible un conveniente acceso en red bajo demanda a una fuente compartida de recursos informáticos configurables (p. ej., redes, servidores, almacenamiento, aplicaciones y servicios), de los que se puede hacer provisión rápidamente y lanzarse con un mínimo esfuerzo de gestión o de interacción con el proveedor del servicio. Este modelo de nube promueve la disponibilidad y está compuesto de cinco características esenciales, tres modelos de servicio y cuatro modelos de utilización (Mell y Grance, 2009).

Como reconocen los autores de la definición, no existe aún un modelo consolidado de *Cloud Computing*, y el ecosistema de participantes en el mismo es lo suficientemente grande como para impedir una definición más restringida, de tal modo que, añadimos nosotros, la definición del NIST, a simple vista, lo abarca absolutamente todo: en principio, todos los esfuerzos que una organización lleva a cabo actualmente con respecto a sus sistemas de información –adquirir *hardware*, configurarlo, mantenerlo, comprar licencias de *software*, instalarlas, actualizarlas, adquirir servidores de ficheros, conceder privilegios y restricciones de acceso, etc.– podrían trasladarse, a un coste mucho menor, a un proveedor de servicios en la nube, liberándose de esta manera de muchas rutinas molestas, y desplazando las inversiones monetarias y humanas desde estas rutinas hacia, por ejemplo, la investigación y desarrollo. El atractivo es innegable, pero las cosas no son exactamente así. De serlo, todo el mundo querría estar, y estaría, en la nube. El propio NIST establece algunas restricciones sobre el modelo propuesto en

la definición citada: esas cinco características esenciales, esos tres modelos de servicio y esos cuatro modelos de utilización.

En lo que concierne a las características del modelo en la nube, para que una prestación de servicios remotos pueda considerarse conforme con el mismo debe:

- tratarse de un autoservicio bajo demanda;
- proporcionar acceso mediante red de banda ancha;
- constituir una fuente de recursos;
- poseer una rápida elasticidad; y
- tratarse de un servicio medible.

En lo que concierne a los modelos de servicio, para que la prestación de éstos pueda considerarse en la nube debe ser:

- prestación de servicios de *software*: consiste en un despliegue de software en el cual las aplicaciones y los recursos computacionales se han diseñado para ser ofrecidos como servicios de funcionamiento bajo demanda, con estructura de servicios llave en mano. De esta forma se reducen los costes tanto de *software* como de hardware, así como los gastos de mantenimiento y operación.
- prestación de servicios de plataforma: el servicio se entrega como bajo demanda, desplegándose el entorno (*hardware* y *software*) necesario para ello. De esta forma, se reducen los costes y la complejidad de la compra, el mantenimiento, el almacenamiento y el control del hardware y el software que componen la plataforma; o
- prestación de servicios de infraestructura: la infraestructura básica de cómputo (servidores, *software* y equipamiento de red) es gestionada por el proveedor como un servicio bajo demanda, en el cual se pueden crear entornos para desarrollar ejecutar o probar aplicaciones (Inteco, 2011).

Aunque el documento no lo menciona, se entiende que una combinación de modelos de servicio es concebible.

Por último, en lo que concierne a los modelos de utilización, éstos han de ser:

1) una nube privada: la infraestructura se crea con los recursos propios de la empresa que lo implanta, generalmente con la ayuda de empresas especializadas en este tipo de tecnologías;
2) una nube comunitaria: dos o más organizaciones forman una alianza para implantar una infraestructura *Cloud* orientada a objetivos similares y con un marco de seguridad y privacidad común;
3) una nube pública: la infraestructura y los recursos lógicos que forman parte del entorno se encuentran disponibles para el público en general a través de internet; o
4) una nube híbrida: implica la utilización conjunta de varias infraestructuras *Cloud* de cualquiera de los tres tipos anteriores, que se mantienen como entidades separadas, pero que a su vez se encuentran unidas por la tecnología estandarizada o propietaria, proporcionando una portabilidad de datos y aplicaciones (Mell y Grance, 2009).

Aunque desde luego las restricciones mencionadas en el párrafo precedente contribuyen a evitar la idea de que la nube lo es todo, resultan a nuestro juicio insuficientes para perfilar adecuadamente qué cosa sea la nube, si es que este perfil resulta posible, dado el actual estado del arte. El *Cloud Computing Use Case Discussion Group*, que asume la definición y las restricciones del NIST, elabora una taxonomía que quizá contribuya a re-elaborar tal definición, a partir de la dilucidación de los roles que juegan los distintos agentes participantes en la nube. De conformidad con el *Discussion Group*, existen básicamente tres tipos de agentes: consumidores de servicios, proveedores de servicios y desarrolladores de servicios, cada uno de los cuales juega un papel diferente en la nube, cuenta con determinados recursos, y mantiene diferentes relaciones con los otros agentes. Así,

1) el consumidor es el usuario final, individuo o corporación, que disfruta de los servicios prestados por el proveedor, previa negociación, más o menos estricta, de las condiciones de prestación de esos servicios;

2) el proveedor de servicios presta tales servicios, que pueden ser extremadamente diversos, de *software*, de plataforma o de infraestructura. Por lo que nos interesa, es el agente que dispone de mayor número de cartas en la mano;
3) por su parte, el desarrollador crea, publica y supervisa un recurso en la nube.

De manera muy significativa, el *Discussion Group* introduce distintos modos en que los agentes de esta taxonomía se relacionan con las normas; así, existen normas que:

- atraviesan toda la nube,
- son de aplicación a los proveedores dentro de una nube,
- relacionan a una empresa con la nube, o
- son de aplicación dentro de una empresa (*Cloud Computing Use Case Discussion Group*, 2009).

Decimos de manera significativa porque es en este punto, en la aplicación de normas, y particularmente en los bloques tres y cuatro, donde los profesionales de la gestión de documentos y de información pueden encontrar su espacio en la nube.

Desde luego, diríase que la taxonomía de agentes del *Discussion Group* contribuye en algo a restringir la definición inicial. Y no obstante, a la vista de los recursos de que dispone, y que presta, el proveedor de servicios de esta taxonomía –aplicaciones, en torno de *software*, infraestructura, recursos virtualizados de almacenamiento o red, imágenes virtuales que incluyen metadatos, recursos de seguridad, capacidades de gestión y, sosteniéndolo todo, el *firmware* y el *hardware* del propio proveedor–, a pesar de los refinamientos introducidos, la nube sigue siéndolo todo. Sólo hay que echar un vistazo a los distintos estudios de caso propuestos por el *Discussion Group* para consolidar esta sensación:

- relaciones entre un usuario final y la nube;
- de una empresa con un usuario final a través de la nube;
- de una empresa con la nube;

- de una empresa con otra empresa a través de la nube;
- una nube privada;
- una nube híbrida;
- un cambio de proveedor de servicios.

La nube es invasiva y a menudo invisible. Como dijimos, esto no es en principio ni bueno ni malo, en la medida en que las tecnologías no son, nunca lo han sido, ni buenas ni malas. Son buenos o malos los usos que se hacen de ellas. Por ello, deviene urgente conocer cuáles son los beneficios y cuáles los riesgos de vivir, de trabajar, de documentar en la nube.

Beneficios y riesgos

Desde hace varios años, las conductas personales de gestión de documentos han venido siendo permeadas por la nube, algo que no es de extrañar, dados los numerosos atractivos de la misma: el usuario no paga o paga por uso, se ahorra espacio de almacenamiento, no existe la necesidad de instalar aplicaciones complejas que consumen recursos, no deben realizarse copias de seguridad, existe una mayor capacidad para interactuar con la máquina, con otras máquinas, y con otros usuarios. Google, con herramientas App o las grandes capacidades de almacenamiento de GMail, constituye un inmejorable ejemplo.

Como es natural, si estas ventajas, entre otras, han atraído masivamente a los individuos, no existe ningún motivo para pensar que no habrían de atraer igualmente a las organizaciones, y son muchas las empresas privadas que, en mayor o menor medida, están haciendo también uso de la nube (Spinola, 2009). Y no sólo esto: la administración Obama tiene como una de sus prioridades económicas y técnicas la construcción de un marco tecnológico gubernamental apoyado en el *Cloud Computing* (*Crosscutting Programs*, 2009); y el gobierno japonés prepara un marco similar, tentativamente llamado *Kasumigaseki*, que abarcará a los ministerios del gobierno central y, en la medida en que la legislación lo permita, prestará también servicios a nivel local y de prefectura (Chan, 2009).

Por supuesto, como indicamos, no existe un solo modelo de nube, y diferentes tipos de usuarios adoptarán un modelo u otro, dependiendo

de factores tales como la necesidad de que sus datos permanezcan bajo estrictas condiciones de seguridad, de las posibilidades económicas, o de la obligación de adecuarse a un entorno regulador determinado. Por ejemplo, es probable que un abonado personal a GMail requiera condiciones de seguridad básicas o que pueda perder determinada información sin que esto suponga una crisis para su sistema; pero, dadas las restricciones de la legislación nacional, la nube gubernamental japonesa adoptará el modelo de nube privada interna. De igual modo, no es casual que la definición norteamericana de nube y la exploración del modelo a adoptar hayan sido encargadas al NIST.

Precisamente esta flexibilidad, que permite el uso de distintos modelos, o de combinaciones entre modelos, incluida la posibilidad de colocar determinados recursos en la nube mientras otros permanecen bajo control del usuario final, constituye uno de sus principales, aunque quizá no el más publicitado, atractivos. En realidad si, tal y como indicara Gilder en su célebre artículo, "La red es el ordenador" (Gilder, 2006), de lo que estamos hablando es de personalizar la red a un precio en ocasiones inferior al de un ordenador personal. Unido, como se dijo, al hecho de que la salida de la crisis global pasa por una redefinición de las propiedades y los usos de las tecnologías de la información y de las comunicaciones, y a la aserción de que el *Cloud Computing* no es primariamente una revolución tecnológica, con los esfuerzos que ello implica, sino sobre todo una re-ordenación de tecnologías existentes, mucho más cómoda, la tentación no sólo es grande, sino también plenamente justificada.

Sin embargo, no todo son ventajas. Existen sin lugar a duda riesgos, alguno de los cuales ya ha tenido lugar, y de los que no son los menores las brechas de seguridad, la falta de previsión con respecto a la interoperabilidad, o la no perdurabilidad de la información. Aunque los gigantes de la nube, como Google, Amazon, o el líder del desarrollo web Sun Microsystems, afirman haber desarrollado o estar desarrollando nuevas herramientas para garantizar que tales riesgos no se producirán, los especialistas son prudentes. Indudablemente, el riesgo dependerá en gran medida de la actividad que se ubique en la nube. Por ejemplo, en muchas regulaciones, incluida la española, la privacidad de los datos no es un absoluto, sino una determinación, caso por caso, de capas o niveles, de tal modo que una brecha en la seguridad de

una agenda de protocolo cuyo contenido se puede obtener mediante una guía de teléfonos parece intuitivamente menos crítica que una brecha de seguridad en expedientes policiales; intuición que no evita la eventualidad de que una de las personas que aparecen en la agenda no quiera que sus datos circulen en la red. El equilibrio entre beneficios y retos, por tanto, depende una vez más de un estudio de casos que, por otra parte, la propia flexibilidad de la red permite.

De conformidad con Spinola, los beneficios de trabajar en la nube, sea cual sea el modelo que se emplee, o la combinación de modelos, pueden englobarse en tres categorías (Spinola, 2009):

- suministro más rápido de servicios,
- reducción de costes y
- enfoque sobre la innovación más que sobre el mantenimiento y la implantación.

De manera más específica, indica que no existen inversiones en infraestructura y, por tanto, el riesgo financiero es menor y la competitividad mayor. En este sentido, se ha hecho popular la expresión "pagar sólo por lo que se usa". Además, el acceso a los recursos de *hardware* es casi inmediato, y el multi-arrendamiento de centros de datos, compartiendo recursos, proporciona ventajas a nivel de economía de escala. No debemos olvidar que las redes consumen enormes cantidades de energía eléctrica, cuyos costes derivarían hacia las compañías proveedoras de servicios en la nube, que se instalan en localizaciones físicas donde la electricidad es más barata (Gilder, 2006). Desde el punto de vista técnico, la gestión del cambio de infraestructura es más sencilla, la agilidad en el suministro de soluciones queda mejorada y se eliminan los problemas cotidianos de mantenimiento de *hardware*, *software*, servidores, depósitos, etc., y el personal de tecnologías de la información puede enfocarse sobre la innovación de servicio, más que sobre tal mantenimiento.

No obstante, la misma autora descubre algunos interesantes interrogantes que, tras examinar los beneficios, las organizaciones deberían plantearse, por ejemplo: ¿dónde están mis datos? ¿Con qué seguridad entran en y salen mis datos de la nube? ¿Quién tiene acceso a mis datos? ¿Cómo se protegen

mis datos mientras están en tránsito? ¿Quién se hace responsable si algo va mal? ¿Cuál es el plan de recuperación de desastres, incluidas las respuestas a una pandemia? ¿Cómo se satisfacen legislaciones como las de exportación y privacidad? ¿Desaparecerán mis datos si mi almacenamiento en línea se corta? ¿Qué pasa si desaparece mi proveedor en la nube? ¿Cómo se supervisa el entorno en previsión de fallos de las aplicaciones, del sistema operativo, de las bases de datos? ¿Cómo se notifican estos fallos? ¿Cómo se protegen y aseguran los datos contra robo o daño? ¿Se encriptan? ¿Cómo rotan y se gestionan las claves de encriptación? ¿Es fácil la integración con las tecnologías de la información ya existentes a nivel local? ¿Tiene el sistema la suficiente capacidad de personalización como para adecuarse a mis necesidades? ¿Es difícil volver a migrar a un sistema local? ¿Es posible? ¿Existen requisitos normativos en mi actividad que me impidan utilizar la nube?

Con el objeto de que el gestor de documentos dispusiera de un mecanismo para ponderar los riesgos de trabajar en la nube, la Australasian Recordkeeping Initiative (ADRI) desarrolló una metodología que incluía una cómoda lista de verificación de la conformidad.

Por otra parte, el Instituto Nacional de Tecnologías de la Comunicación (Inteco), a partir de informes anteriores, ha categorizado los siguientes riesgos:

- De acuerdo con la Cloud Security Alliance:
  - Abuso y mal uso del *Cloud Computing*;
  - Interfaces y APIs poco seguros;
  - Amenazas internas;
  - Problemas derivados de las tecnologías compartidas;
  - Pérdidas o fugas de información;
  - Secuestro de sesión o servicio; y
  - Riesgos por desconocimiento.
- De conformidad con Gartner:
  - Accesos de usuarios con privilegios;
  - Cumplimiento normativo;
  - Localización de los datos;
  - Aislamiento de datos;

- Recuperación;
- Soporte investigativo; y
- Viabilidad a largo plazo. (Inteco, 2011)

Desde luego, no son dudas triviales: tienen que ver con la supervivencia de nuestros datos, con la privacidad de los mismos, con la posibilidad de cambiar de opinión. La propia nube ya ha respondido a algunas de ellas; pero lo realmente divertido no es esto. Lo que llama nuestra atención es que muchas de estas dudas deberíamos plantearlas también en nuestros entornos de trabajo fuera de la nube, pero rara vez lo hacemos. Como indicamos anteriormente, la nube no es una revolución, es una re-ordenación. De igual modo, las prevenciones que provoca, prevenciones que pueden resumirse en los términos precariedad e invisibilidad, no son novedosas, existen en nuestro entorno cotidiano. La diferencia, con toda probabilidad, es meramente de tamaño y alcance.

¿Realmente estamos seguros fuera de la nube?

De igual modo que, como dijimos, el *Cloud Computing* no es una novedad, las dudas que plantea, en nuestra opinión, tampoco lo son. En realidad, desde que dejamos de utilizar el papel y comenzamos a utilizar ordenadores, comenzamos también a perder el control. En el mejor de los casos, lo perdimos cuando dejamos de trabajar en equipos locales y se generalizó el uso de redes de área local, primero; de arquitecturas cliente-servidor, segundo; y, más recientemente, de arquitecturas multicapa o tecnologías como la de la virtualización. Veamos si los interrogantes de Spinola pueden plantearse de igual modo en un escenario que todavía no ha pasado por la nube, digamos las aplicaciones y los datos de un archivo que pertenece a una organización compleja (en este caso, el escenario en el que trabajamos de manera cotidiana).

¿Dónde están mis datos? Bien, mis datos están, según me han dicho, en un Oracle 11 al que no puedo acceder directamente, alojado en un servidor del que sólo sé que se llama Minerva y que se comparte con otras unidades vinculadas al archivo. Ignoro dónde se encuentra ese servidor, aunque el equipo del Servicio de Informática es amigo y "confío" en ellos. Mis

ficheros están en un servidor del que sé que se llama Artillero y que veo todos los días, pero sobre el que no puedo ejecutar ninguna operación. Una vez más, "confío" en los amigos.

¿Con qué seguridad entran y salen mis datos de la nube? Bueno, no están en la nube, están en un entorno cerrado, aunque a veces hay que abrirlo, o acceder mediante mecanismos como los de una red privada virtual, porque preciso realizar operaciones desde lugares remotos, digamos un hotel en México D. F. "Confío" en la seguridad de una red privada virtual.

¿Quién tiene acceso a mis datos? Realmente, no lo sé; presumiblemente hemos establecido permisos y restricciones de acceso muy estrictos, pero al menos el Servicio de Informática y una compañía privada que ha firmado una cláusula de confidencialidad tienen los mismos permisos que yo. De nuevo, es una cuestión de "confianza".

¿Cómo se protegen mis datos mientras están en tránsito? Tampoco lo sé, o, en sentido estricto, lo sé: el equipo de criptografía de mi organización trabaja muy bien y documenta sus procedimientos de encriptación. Además, me facilita esta documentación. La parte mala es que, puesto que no soy especialista en criptografía, no entiendo prácticamente nada de esta documentación. Utilizaré una vez más la expresión "confío" en el equipo de criptografía.

¿Quién se hace responsable si algo va mal? Eso está claro: todos los que estamos implicados en el funcionamiento del sistema y, en último extremo, nuestros superiores pertenecientes a la alta gestión; lo cual, por supuesto, no evita que se pierdan datos si algo va mal. "Confío" en que nada vaya nunca mal.

¿Cuál es el plan de recuperación de desastres, incluidas las respuestas a una pandemia? Las medidas para prevenir desastres y pandemias, y para recuperarse de ambos, son exhaustivas, en ocasiones paranoicas, lo cual es bueno; no sé si funcionan, o "confío" en que funcionan, porque hasta el momento no hemos padecido un desastre ni una pandemia.

¿Cómo se satisfacen legislaciones como las de exportación y privacidad? Se satisfacen hasta el aburrimiento, pero somos tantos los implicados en conseguir que se satisfagan, e intervienen tantos sistemas en conexión y tantos datos transitan de manera tan continuada que, de nuevo, deviene una cuestión de "confianza".

¿Desaparecerán mis datos si mi almacenamiento en línea se corta? No desaparecerán, pero no podré trabajar, o podré hacerlo de manera limitada, hasta que se recupere la línea. Tengo que "confiar" en que la línea no se corte, aunque a veces sucede, de modo que, para ser exacto, tengo que "confiar" en que suceda muy raras veces.

¿Qué pasa si desaparece mi proveedor en la nube? Puesto que no estamos hablando de un escenario en la nube, tengo que plantear la pregunta en otros términos: ¿qué pasa si el equipo de informática se va de vacaciones? ¿Qué pasa si se quema un servidor? Bien, "confío" en que esto no suceda, o al menos que no suceda de manera simultánea, simplemente porque habría que restaurar la última copia de seguridad, y yo no estoy cualificado para hacerlo. Incluso aunque el equipo de informática no esté de vacaciones, a veces me llaman para decir algo del estilo de "tengo que reiniciar el servicio". No sé ni cómo ni por qué, pero "confío" en ellos.

¿Cómo se supervisa el entorno en previsión de fallos de las aplicaciones, del sistema operativo, de las bases de datos? A decir verdad, no creo que se supervise: actuamos más bien "confiando" en la posibilidad de que no se produzcan fallos. Como éstos, a pesar de todo, se producen, actuamos a posteriori, con la "confianza" en la posibilidad de que podremos solventarlos. Hasta ahora, nos ha ido bien.

¿Cómo se notifican estos fallos? Se notifican mediante intranet: si se advierte un fallo se envía la incidencia y se traslada a aquel en quien se "confía" como más cualificado para solventarlo y, si el fallo es de relevancia, esta persona de "confianza" va llamando a su vez a otras personas de su "confianza", hasta que todo se soluciona. En realidad somos un buen equipo: "confiamos" todos en todos.

¿Cómo se protegen y aseguran los datos contra robo o daño? No lo sé, por todo lo que dije antes. Nos movemos en un entorno cerrado, pero en ese entorno cerrado no todos tienen las mismas habilidades y no se descarta la posibilidad de que alguien se equivoque, incluido yo. "Confío" en que esto no suceda.

¿Se encriptan? Sí se encriptan y se documentan los mecanismos de encriptación. Como dijimos más arriba, la parte mala es que, al no entender esta documentación, tengo que "confiar" en que seremos capaces de desencriptarlos.

¿Cómo rotan y se gestionan las claves de encriptación? No lo sé. De nuevo, es una cuestión de "confianza".

¿Es fácil la integración con las tecnologías de la información ya existentes a nivel local? En absoluto: los frecuentes cambios de tecnología, o la integración de tecnologías existentes, son complicadísimos y llevan meses de trabajo de uno o varios equipos compuestos por muchas personas. El cambio tecnológico no es fácil, pero "confiamos" en que entre todos, combinando las mejores destrezas de cada uno, podremos llevarlo a cabo.

¿Tiene el sistema la suficiente capacidad de personalización como para adecuarse a mis necesidades? No: mis necesidades, o las necesidades del archivo y unidades asociadas, son tan diversas, variables e insospechadas que no creo que ningún sistema las acomode con facilidad. Una vez más, "confío" en que el equipo multidisciplinar que gestiona las tecnologías tenga capacidad para elaborar tales personalizaciones.

¿Es difícil volver a migrar a un sistema local? Sería una pesadilla, "confío" en que no tenga que retroceder a un sistema anterior. ¿Es posible? Sí, al menos "confío" en ello, aunque no será ni fácil ni barato.

¿Existen requisitos normativos en mi actividad que me impidan utilizar la nube? Por supuesto, existen, particularmente los referidos a seguridad, protección de datos, privacidad, etc.; pero existen, después de todo, nubes privadas, firmas de convenios o redes seguras en desarrollo. Tendría que "confiar" en este marco y la infraestructura que implica. Paulatinamente se han promulgado requisitos normativos que me permiten usar la nube bajo ciertas condiciones: también tendré que "confiar" en ellos.

La cuestión es que en nuestros entornos cotidianos de trabajo ya no tenemos de hecho el control y, sin embargo, confiamos en el sistema, aunque el sistema a veces falla. Seamos realistas: trabajamos con las tecnologías no sólo porque en términos objetivos nos facilitan las cosas; también porque somos capaces –social, organizativa y culturalmente– de establecer mecanismos subjetivos de confianza en las mismas y en el entorno que las gestiona. La nube no es diferente; simplemente es más grande y más difusa. Esto no es motivo suficiente para abandonar sus ventajas, entre otras cosas porque a medio plazo no existirá otra alternativa.

Bibliografía

Australasian Digital Recordkeeping Initiative: *Advice on Managing the Recordkeeping Risks Associated with Cloud Computing. Version 1.0*. Council of Australasian Archives and Records Authorities, 2010. URL: http://www.adri.govt.nz/ (Consulta: 10-09-2012).

Chan, Tony: "Japan to Build Massive Cloud Infrastructure for e-Government", en: Greentelecomlive. URL: http://www.greentelecomlive.com/2009/05/13/japan-to-build-massive-cloud-infrastructure-for-e-government/ (Consulta: 10-09-2012).

Cloud Computing Use Case Discussion Group: Cloud Computing Use Cases White Paper. Version 2.0. Cloud Computing Use Case Discussion Group, 2009. URL: http://www.scribd.com/doc/18172802/Cloud-Computing-Use-Cases-Whitepaper (Consulta: 10-09-2012).

Crosscutting Programs, 2009.

Foley, John: "Obama's Cloud Computing Strategy Takes Shape", en: InformationWeek, 05-11-2009.

Gilder, George: "The Information Factories". En: Wired. N. 14.10 (october 2006).

Instituto Nacional de Tecnologías de la Comunicación: Riesgos y amenazas en Cloud Computing. Inteco, 2011. URL: http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf (Consulta: 10-09-2012).

Mell, Peter, Grance, Tim: The NIST Definition of Cloud Computing. National Institute of Standards and Technology, 2009. URL: http://csrc.nist.gov/groups/SNS/cloud-computing/ (Consulta: 10-09-2012).

Spinola, Maria: An Essential Guide to Possibilities and Risks of Cloud Computing. Autor, 2009.

Sun Microsystems: *Take your Business to a higher level*. Sun Microsystems, 2009.

Legajos. Boletín del Archivo General de la Nación, 7ª época, núm. 16,
se terminó de imprimir en julio de 2013
en Tipográfica, S. A. de C. V.
Se tiraron 500 ejemplares.