*Informe nº 3/2011*

# *Utilización del* cloud computing *por los despachos de abogados*

## I. INTRODUCCIÓN: EL CONCEPTO DEL CLOUD COMPUTING Y LOS SERVICIOS PARA LOS DESPACHOS DE ABOGADOS

Cloud Computing es un modelo de prestación de servicios tecnológicos que permite el acceso bajo demanda y a través de la red a un conjunto de recursos compartidos y configurables (como redes, servidores, capacidad de almacenamiento, aplicaciones y servicios) que pueden ser rápidamente asignados y liberados con una mínima gestión por parte del proveedor de servicios.

El modelo tiene las siguientes cinco características esenciales:

1. **Autoservicio bajo demanda**. El usuario puede acceder a capacidades de computación "en la nube" de forma automática conforme las necesita sin necesidad de una interacción humana con su proveedor o sus proveedores de servicios Cloud.

2. **Múltiples formas de acceder a la red**. Los recursos son accesibles a través de la red y por medio de mecanismos estándar que son utilizados por una amplia variedad de dispositivos de usuario, desde teléfonos móviles a ordenadores portátiles o PDAs.

3. **Compartición de recursos**. Los recursos (almacenamiento, memoria, ancho de banda, capacidad de procesamiento, máquinas virtuales, etc.) de los proveedores son compartidos por múltiples usuarios, a los que se van asignando capacidades de forma dinámica según sus peticiones. Los usuarios pueden ignorar el origen y la ubicación de los recursos a los que acceden, aunque sí es posible que sean conscientes de su situación a determinado nivel, como el de CPD o el de país.

4. **Elasticidad**. Los recursos se asignan y liberan rápidamente, muchas veces de forma automática, lo que da al usuario la impresión de que los recursos a su alcance son ilimitados y están siempre disponibles.

5. **Servicio medido**. El proveedor es capaz de medir, a determinado nivel, el servicio efectivamente entregado a cada usuario, de forma que tanto proveedor como usuario tienen acceso transparente al consumo real de los recursos, lo que posibilita el pago por el uso efectivo de los servicios.

En definitiva, desde la perspectiva de los despachos de abogados como usuarios, el modelo Cloud Computing permite acceder a una serie de servicios, que pueden ir desde el correo electrónico hasta el almacenamiento de documentos, pasando por aplicaciones de gestión del despacho, de contabilidad, de bases de datos de jurisprudencia o legislación, o de compartición de documentación e información con clientes o con otros despachos; y todo ello sin necesidad de disponer de servidores o de software en el propio despacho, con sus necesidades asociadas de mantenimiento y administración, y con las correspondientes inversiones en equipamiento y *software* y gastos en operación y mantenimiento de los mismos. Lo único que se necesita es un dispositivo, que puede ser desde un ordenador portátil hasta un *smartphone* o un iPad, y una conexión a Internet. Los datos y las aplicaciones se encuentran en algún lugar de Internet, la cual se representa frecuentemente como una nube, de ahí el término Cloud Computing.

Las ventajas técnicas y económicas del modelo son inmediatas para los usuarios. No es necesario que los despachos —especialmente los más pequeños— cuenten con personal informático propio dedicado al mantenimiento de los servidores y las aplicaciones, a la realización de copias de seguridad de la información y a velar por su integridad y seguridad. Los servicios tecnológicos pasan a ser un gasto operativo, obviándose la necesidad de inversiones en infraestructuras de breves ciclos de vida y rápida obsolescencia. El acceso a los servicios está garantizado desde cualquier lugar del mundo en el que se disponga de una conexión a Internet, y el proveedor de servicios asegura la disponibilidad del servicio y la actualización permanente de aplicaciones y sistemas.

Sin embargo, como ya sucedió en el pasado con otras innovaciones tecnológicas, surgen dudas relativas a la seguridad e integridad de la información, especialmente la que pueda tener naturaleza más sensible por su carácter confidencial, así como ciertas lógicas reservas a perder el control físico de datos confidenciales o reservados de clientes del despacho, que dejan de estar en los servidores propiedad del mismo o en discos o dispositivos que se guardan en un lugar físicamente seguro. Efectivamente, los datos en el modelo de "Cloud Computing" pasan a situarse en algún lugar indeterminado, en un servidor cuya ubicación física se desconoce.

Para ilustrar esta desconfianza, hasta cierto punto lógica, valga como ejemplo el hecho de que el Comité de Ética y Responsabilidad Profesional de la Asociación Americana de la Abogacía (*American Bar Association, Standing Committee on Ethics and Professional Responsibility*) no consideró el correo electrónico como medio válido y seguro para comunicarse con los clientes hasta el año 1999, en el que mediante la "*Formal Opinion No. 99-413, Protecting the Confidentiality of Unencrypted E-Mail*", consideró que el correo electrónico ofrecía la misma expectativa razonable de privacidad que el correo postal, el fax o el teléfono.

El propósito de este informe es señalar cuáles son los aspectos esenciales que los despachos de abogados deben de tomar en consideración a la hora de contratar servicios Cloud Computing para su actividad diaria y sus relaciones con sus clientes, para aprovechar así las ventajas de este nuevo paradigma tecnológico sin asumir riesgos jurídicos relacionados con la seguridad y confidencialidad de la información de los que se puedan derivar perjuicios tanto para el despacho como para sus clientes.

Para ello, en los apartados siguientes se desarrollan los que se han considerado tres aspectos esenciales que deben tenerse en cuenta a la hora de decidir contratar servicios de Cloud Computing por un despacho de abogados:

- La seguridad y confidencialidad de los datos.
- Territorialidad y jurisdicción aplicable.
- Aspectos esenciales del contrato de servicios que debe firmarse, tanto desde el punto de vista técnico como jurídico.

El enfoque del tratamiento que se ha dado a estos tres aspectos es eminentemente práctico; es decir, se ha tratado de establecer pautas y recomendaciones para facilitar a los despachos la interlocución con los proveedores de servicios Cloud Computing, ya que en la actualidad, como es lógico, no hay desarrollada normativa ni mucho menos jurisprudencia relacionada con los servicios de Cloud Computing, dado lo novedoso del concepto.

## II. ASPECTOS TÉCNICOS Y JURÍDICOS ESENCIALES DE LOS SERVICIOS CLOUD COMPUTING

La seguridad y confidencialidad de la información es un aspecto esencial a la hora de contratar servicios Cloud por parte de un despacho de abogados. Se trata por tanto de determinar cuáles son las garantías, tanto jurídicas como técnicas, que el despacho ha de recibir por parte de su proveedor de servicios, garantías tendentes a asegurar —desde un punto de vista técnico— que la información no se va a perder o a corromper "en la nube" y también a asegurar que ningún usuario no autorizado va a disponer de acceso a esta información. Además, lógicamente, si esto por cualquier circunstancia no fuese así, deberá establecerse la oportuna garantía jurídica de que el despacho quedará indemne frente a los perjuicios que se le pueden ocasionar a él o a sus clientes. La propia Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), establece en su art. 12.2 que "*La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que*

*el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas*". Por tanto, el contrato de prestación de servicios entre el despacho y su proveedor de servicios Cloud ha de incorporar, por mandato legal, las previsiones necesarias para garantizar el adecuado cumplimiento de la normativa relativa a la protección de datos.

En materia de seguridad y confidencialidad, y desde un punto de vista técnico, los aspectos esenciales a tener en cuenta durante la selección del proveedor de servicios Cloud son los siguientes:

- El proveedor de servicios Cloud ha de garantizar la conservación de los datos, mediante la realización de copias de seguridad periódicas y dotando a su infraestructura de los mayores niveles de seguridad física y lógica.
- El proveedor ha de establecer mecanismos seguros de autenticación para el acceso a la información por parte de los abogados del despacho así como por parte de los clientes, en los términos que el despacho determine. Estos mecanismos han de permitir la compartición e intercambio de información sin que por supuesto sea posible que personas no autorizadas accedan a información reservada o confidencial de otros clientes o de otros abogados.
- El cifrado de los datos almacenados es una necesaria medida de seguridad. El proveedor ha de dar a conocer al despacho el nivel de seguridad ofrecido por las técnicas de cifrado de la información que aplique en sus sistemas.
- Asimismo, es fundamental acordar el procedimiento de recuperación y migración de los datos a la terminación de la relación entre el despacho y el proveedor; así como el mecanismo de borrado de los datos por parte del proveedor una vez que estos han sido transferidos al despacho o al nuevo proveedor designado por éste.

Para tomar una decisión informada sobre la oferta de cada proveedor en materia de seguridad y confidencialidad de la información, es del mayor interés que el despacho o bien quien le asesore en la selección de los servicios Cloud tenga acceso a la política de seguridad del proveedor así como a las normas internacionales y certificaciones en materia de seguridad informática con las que cuenta la infraestructura del proveedor. Entre las certificaciones de seguridad más conocidas aplicables a este tipo de infraestructura, pueden citarse las siguientes:

- ISO 27001, de la International Standards Organization, específicamente orientada a los Sistemas de Gestión de la Seguridad de la Información.

- SAS 70 (Statement on Auditing Standards, nº 70), del American Institute of Certified Public Accountants (AICPA).
- Systrust y Webtrust, igualmente del American Institute of Certified Public Accountants (AICPA).
- Certificación según el Federal Information Security Management Act (FISMA): NIST SP 800-37 "Guide for the Security Certification and Accreditation of Federal Information Systems".

Lógicamente todos estos aspectos técnicos deben de trasladarse a un contrato de servicios entre el despacho de abogados y su proveedor que recoja las garantías jurídicas necesarias en caso de incumplimiento por parte del proveedor, con la finalidad última de que el despacho no sufra perjuicio alguno.

Como hemos señalado al principio, la propia naturaleza del modelo Cloud Computing hace posible que, en principio, los datos almacenados "en la nube" se encuentren físicamente en un servidor ubicado en cualquier punto del planeta.

Esta circunstancia es muy relevante, al menos en materia de protección de datos de carácter personal, aunque también lo es desde el punto de vista de la resolución de posibles conflictos.

Centrándonos en el cumplimiento de la normativa de protección de datos de carácter personal, a la que estará obligado el despacho, se trata de protegerle frente a eventuales reclamaciones, sobre todo en aquellos casos en los que el lugar de almacenamiento de la información está sujeto a otra jurisdicción.

En primer lugar, es necesario tener en cuenta que el papel del despacho que decide poner en manos de su proveedor de servicios Cloud sus ficheros de carácter personal es el de "responsable del fichero" (art. 3 LOPD), mientras que el proveedor de servicios Cloud pasa a ser el "encargado del tratamiento del fichero" (art. 3 LOPD), estando por tanto obligado, según el art. 12 LOPD, a seguir las instrucciones del responsable del fichero en el tratamiento de los datos. Por consiguiente, si el contrato de prestación de servicios establece que el proveedor de servicios no dará a esos datos ningún otro uso que el indicado por el despacho, la extralimitación por parte del proveedor de Cloud en su calidad de encargado del tratamiento tendrá las consecuencias previstas en el art. 12.4 LOPD, en virtud de las cuales el encargado del tratamiento pasa a asumir la condición de responsable del fichero.

No todos los datos de carácter personal gozan del mismo nivel de protección. El art. 7 LOPD establece la existencia de datos especialmente protegidos, entre los que se encuentran por ejemplo los relativos a salud, orientación sexual, ideología o religión, para los cuales la medidas de protección que debe adoptar el

encargado del tratamiento del fichero son especialmente rigurosas. Así, los art. 79 y siguientes del RD 1720/2007, por el que se aprueba el Reglamento de la LOPD, establecen tres niveles de seguridad (básico, medio y alto) que se asocian a tres categorías de datos en función del nivel de protección de los mismos. Es obligación del encargado del tratamiento articular las medidas necesarias para dotar a los datos del nivel de seguridad correspondiente; y corresponde al responsable del fichero, en este caso el despacho de abogados, exigir a su proveedor de servicios Cloud que articule dichas medidas. Los art. 89 y siguientes del RD 1720/2007 desarrollan cuáles son las medidas exigibles al encargado del tratamiento para cada nivel de seguridad de los datos.

Sin embargo, la muy probable circunstancia de que los datos no se almacenen en territorio español nos obliga a contemplar qué ocurre si los datos están almacenados en otro país en el que la LOPD carece de fuerza legal. La Directiva 95/46/CE contempla en su artículo 25 la transferencia de datos personales a países terceros[1], señalando que la transferencia ha de limitarse a naciones en las que los datos cuenten con lo que se define como "un nivel de protección adecuado"[2]. En cuanto a la legislación nacional, el denominado movimiento internacional de datos está regulado en la LOPD en sus artículos 33 y 34.

Por consiguiente, hay que distinguir dos posibilidades: el caso para el que en el país en el que se ubiquen los datos exista una legislación equiparable que garantice un adecuado nivel de protección, y el caso en que no.

En el seno de la Unión Europea, son de aplicación las Directiva comunitaria sobre protección de datos (Directivas 95/46/CE y 2002/58/CE), traspuestas por los distintos estados miembros a sus respectivas legislaciones nacionales. Esta armonización normativa permite a cualquier despacho acudir a los servicios de almacenamiento de información de un proveedor de Cloud Computing que tenga sus centros de proceso de datos ubicados en la Unión Europea, sin temor a que las obligaciones en materia de protección de datos se vean incumplidas. Estas consideraciones son extensivas a los estados cuyas normativas en la materia son consideradas equiparables a la europea, así como a aquellos proveedores radicados en los EE.UU. que son considerados "*safe harbour*" (puerto seguro), por adherirse voluntariamente a este protocolo "*safe harbour*" en virtud del cual se obligan a cumplir requisitos equivalentes a los europeos en materia de protección de datos. En la página web de la Agencia de Protección de Datos pueden

---

1 http://europa.eu/legislation_summaries/information_society/l14012_es.htm.

2 La Agencia Española de Protección de Datos (AEPD) informa de los países con un nivel de protección adecuado en su página web: http://www.agpd.es/portalwebAGPD/canalciudadano/preguntasciudadano/transferencias_internacionales/index-ides-idphp.php.

consultarse los países cuya regulación en la materia se considera equiparable a la europea.

Si, por el contrario, el proveedor almacena sus datos en un país cuya normativa de protección de datos no es equiparable a la europea, hay que tener en cuenta que, por un lado, es necesaria la autorización previa de la Agencia de Proyección de Datos para que el responsable de un fichero de datos de carácter personal encargue su tratamiento a una persona o empresa que reside fuera del espacio de legislación armonizada o equiparada. El procedimiento para la solicitud de la autorización se recoge en los artículos 137 a 140 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD). Por otro lado, el contrato de provisión de servicios ha de incorporar cuantas condiciones sean necesarias para suplir la carencia de legislación y trasladar al encargado del tratamiento del fichero las mismas obligaciones que contempla la normativa europea. Para la elaboración de este tipo de acuerdos pueden tomarse como referencia las *standard contractual clauses for the transfer of personal data to third countries*[3], elaboradas por la Comisión Europea y que garantizan una adecuada protección en la transferencia de información de carácter personal a terceros países.

Es importante destacar que el responsable del fichero, en nuestro caso el despacho de abogados, es responsable de seleccionar como encargado del tratamiento del mismo a alguien que verifique los requisitos legalmente establecidos. Así, el artículo 20.2 RLOPD establece que "*Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento*". Esta responsabilidad se extiende a la subcontratación de servicios. Así, cuando en encargado del tratamiento subcontrate alguna actividad propia del tratamiento de los ficheros, dicha subcontratación habrá de recogerse en el contrato de prestación de servicios entre el responsable y el encargado, siendo necesaria una autorización expresa del primero en los casos de subcontratación sobrevenida no prevista en el contrato (art. 21 RLOPD).

En todos los casos, el encargado del tratamiento, conforme a lo establecido en el 82.2 ROLPD "*Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamien-*

---

[3] Decisiones 2004/915/EC, 2001/497/EC, y 2002/16/EC de la Comisión Europea.

*to*", habrá de disponer de un documento de seguridad elaborado conforme a las previsiones del art. 88 ROLPD. Dicho documento, cuya existencia y contenidos esenciales deberían incorporarse al contrato de prestación de servicios, habrá de contemplar necesariamente los siguientes aspectos de seguridad (apartados 3 a 5 del art. 88 RLOPD):

> *3. El documento deberá contener, como mínimo, los siguientes aspectos:*
> *• Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.*
> *• Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.*
> *• Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.*
> *• Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.*
> *• Procedimiento de notificación, gestión y respuesta ante las incidencias.*
> *• Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.*
> *• Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.*
> *4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:*
> *• La identificación del responsable o responsables de seguridad.*
> *• Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.*
> *5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.*

No obstante, existen otros aspectos relevantes que van más allá de normativa de protección de datos de carácter personal y que conviene traer a colación. Son temas que encontrarán su mejor acomodo y resolución en el propio contrato mercantil de prestación de servicios entre el proveedor y el cliente, el despacho de abogados en nuestro caso. Por la novedad de este tipo de contratos, consideramos conveniente tratarlos a continuación.

Efectivamente, para garantizar la seguridad jurídica del servicio Cloud contratado, el contrato de prestación de servicios de carácter mercantil suscrito entre el despacho y el proveedor ha de recoger, a nuestro juicio, un conjunto mínimo de cláusulas, entre las que cabe destacar las siguientes:

- Propiedad de los datos. Es esencial que el contrato especifique que todos los datos que se van a albergar en la nube son de la propiedad del despacho, y que en consecuencia el proveedor no puede disponer de ellos ni

hacer uso de los mismos para ningún fin que no esté expresamente autorizado por el despacho.

- Cumplimiento de legislación de protección de datos de carácter personal. El proveedor ha de asumir expresamente el papel de encargado del tratamiento de los ficheros de datos de carácter personal que el despacho decida trasladar "a la nube", con todas las obligaciones propias de tal figura tal y como se recogen en la legislación española y europea. Además si el proveedor almacena la información de carácter personal en sistemas ubicados fuera de la Unión Europea, ha de asumir las obligaciones que al encargado del tratamiento de los ficheros de datos de carácter personal impone la legislación europea, con independencia de la jurisdicción aplicable al territorio en el que se localizan los centros de proceso de datos. En particular, si la localización no se encuentra entre las aceptadas por la Agencia Española de Protección de Datos, es preciso recabar autorización de la misma, y es aconsejable incluir en el contrato de servicios las cláusulas tipo propuestas por la Unión Europea.
- Seguridad en el acceso. El proveedor ha de garantizar que la información solo será accesible al despacho de abogados que contrata sus servicios, y a quienes el despacho determine con los perfiles de acceso correspondientes. Igualmente, el proveedor ha de articular los mecanismos necesarios para que los clientes del despacho puedan acceder a datos y documentos para cuyo acceso estén legitimados, pero no a aquellos que correspondan a otros clientes, estableciendo las barreras y cautelas técnicas precisas.
- Integridad y conservación. El proveedor ha de disponer de los mecanismos de recuperación ante desastres, continuidad en el servicio y copia de seguridad necesarios para garantizar la integridad y conservación de la información.
- Disponibilidad. El proveedor ha de garantizar una elevada disponibilidad del servicio, así como comprometerse a organizar las paradas programadas para mantenimiento con la suficiente antelación y dando aviso de las mismas al despacho.
- Portabilidad. El proveedor ha de obligarse, a la terminación del servicio, a entregar toda la información al despacho en el formato que se acuerde, para que éste pueda almacenarla en sus propios sistemas o bien trasladarla a los de un nuevo proveedor, en el plazo más breve posible y con total garantía de la integridad de la información.
- Consecuencias para el caso de incumplimiento del proveedor de servicios Cloud de las obligaciones anteriormente recogidas, las propias de la contratación mercantil, incluidas posibles penalizaciones así como la obliga-

ción de dejar indemne al despacho de las reclamaciones de terceros y particularmente de las de sus propios clientes por cualquier incumplimiento de las cláusulas imputable al proveedor.

Los contratos de prestación de servicios Cloud pueden ser muy extensos, al detallar todas las condiciones en las que se presta el servicio, los SLAs (*Service Level Agreement*, o Acuerdo de Nivel de Servicio) aplicables, las penalizaciones por incumplimiento, etc.

Un ejemplo ilustrativo, por lo exhaustivo, de contrato de servicios Cloud es el suscrito por una Administración Pública que externaliza servicios informáticos a un proveedor. Aunque el poder de compra de una Administración y la envergadura de los contratos suscritos por éstas les otorga una capacidad de negociación que no está al alcance de la mayoría de los despachos de abogados, este tipo de contratos sí puede servir como guía o modelo de todos los aspectos que es necesario tomar en consideración.

En el enlace siguiente puede descargarse el contrato suscrito por el Ayuntamiento de la Ciudad de Los Angeles (California, Estados Unidos), con un proveedor de servicios Cloud Computing, en virtud del cual este último proporciona a la Administración servicios de almacenamiento de datos y correo electrónico, entre otros:

http://clkrep.lacity.org/onlinecontracts/2009/C-116359_c_11-20-09.pdf

El contrato recoge un completo conjunto de cláusulas que cubren los siguientes aspectos:

1. Características técnicas de los servicios prestados.
6. Evolución futura de las características técnicas de los servicios prestados.
7. Formación al personal del cliente por parte del proveedor de servicios Cloud en el uso y administración de dichos servicios.
8. Copias de seguridad y respaldo.
9. Titularidad de los datos y derecho del cliente para recuperarlos y trasladarlos a otro proveedor. Confidencialidad de la información.
10. Documentación que el proveedor tiene que aportar al cliente. Informes periódicos.
11. Mecanismos de seguridad, como por ejemplo antivirus, puestos a disposición del servicio.
12. Duración del acuerdo y tarifas aplicables. Revisión de las tarifas.
13. Derecho del cliente para realizar auditorías de seguridad independientes.

14. Obligación del proveedor para llevar a cabo una revisión y auditoría anual de sus sistemas.
15. Compromiso de disponibilidad y mecanismo de gestión de incidencias de servicio.
16. Penalizaciones aplicables en caso de incumplimiento.

En resumen, la transición de un modelo *in premises* a un modelo Cloud es plenamente factible para un despacho de abogados, y muy aconsejable desde un punto de vista operativo y financiero. Sin embargo, es necesario que el contrato de prestación de servicios suscrito con el proveedor contemple los aspectos esenciales que se han expuesto en este documento, para garantizar que el servicio se recibe con todas las garantías técnicas y legales. En estos casos puede ser aconsejable, para mejorar la posición negociadora frente a los eventuales proveedores de servicios Cloud, agregar la demanda de varios despachos para obtener así la oferta más ventajosa posible, sin perjuicio de que una vez el proveedor inicie la prestación de servicios, cada despacho suscriba su contrato de forma individual.