Buenas prácticas
en materia de **contratación**
de Servicios de Computación en la Nube
(***Cloud Computing***) al interior
de la Administración del **Estado**:

Un documento para el apoyo de toma de decisiones.

Versión 1.0
Santiago, 28 de febrero de 2014

uMGD
Modernización
y Gobierno Digital

Acerca de la Unidad de Modernización y Gobierno Digital.

La Unidad de Modernización y Gobierno Digital del Ministerio Secretaría General de la Presidencia tiene por objetivo mejorar la satisfacción y calidad de servicio que entregan las instituciones públicas a los ciudadanos. En este contexto y entendiendo la importancia creciente que tienen las tecnologías de información en la vida de los ciudadanos, tanto como herramientas de trabajo como plataformas de comunicación y participación, se han integrado a las tareas de modernización, las de Gobierno Electrónico, enfocadas al desarrollo de políticas de e-gob al interior del Estado.

Información de contacto.

Unidad de Modernización y Gobierno Digital,
Ministerio Secretaría General de la Presidencia
Dir.: Teatinos Nº 333, piso 4to, Santiago
Tel.: +56 (2) 2688-7701
URL: www.modernizacion.gob.cl
Correo electrónico: http://www.modernizacion.gob.cl/contactenos.html
Twitter: @Modernizacioncl

Sobre el presente documento:

Este documento no es vinculante para los órganos de la Administración del Estado. No pretende, tampoco, establecer una política de contratación en este tipo de materias. Tales órganos son libres de tomar las decisiones que estimen convenientes en torno a esta materia, en la medida que se adopten dentro de sus competencias y de conformidad al marco legal que las rige.

Este documento sólo pretende entregar antecedentes que permitan la toma de decisiones informadas por parte de tales órganos, adoptando las buenas prácticas que se aquí se sugieren.

Cómo citar este documento:

MISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA, 'Buenas prácticas en materia de contratación de Servicios de Cloud Computing al interior de la Administración del Estado: Un documento para el apoyo de toma de decisiones', Versión 1.0., Santiago, 4 de febrero de 2014.

Derechos de Autor:

ÍNDICE:

RESUMEN EJECUTIVO

Existen grandes beneficios potenciales en torno a la contratación de servicios de computación en la nube (Cloud Computing). En efecto, su empleo puede implicar importantes ahorros de costos económicos y de tiempo en la gestión de plataformas electrónicas. Además, dependiendo del prestador del servicio, la computación en nube puede, potencialmente, entregar beneficios tales como la escalabilidad, elasticidad, alto rendimiento, resistencia y seguridad.

Dada la heterogeneidad de estos servicios, los aspectos legales que implican su contratación varían radicalmente dependiendo de una serie de factores, tales como el tipo de nube que se trata (pública, privada, comunitaria o híbrida), el tipo de información que se sube a la nube, qué prestador de servicio estamos contratando, qué órgano de la administración es el que contrata y una larga lista de factores adicionales. Luego, resulta imposible dar una respuesta de carácter general en torno al tema.

Considerando que serán los propios órganos de la Administración del Estado quienes adoptarán decisión de contratar o no un servicio de esta naturaleza, este documento no es vinculante para ellos. Sólo pretende ser una herramienta que les permita adoptar una decisión que sea lo más informada posible.

Este documento se enfoca principalmente los aspectos legales de la contratación de servicios *cloud*. Este documento presta utilidad, además, al momento de redactar las respectivas Bases de Licitación (cuando ello proceda). Asimismo, si el servicio *cloud* se encuentra en un convenio marco, este documento se puede emplear: (a) para decidir contratar o no a determinado oferente que está inscrito en el convenio marco; (b) para redactar los Acuerdos Complementarios que se puedan considerar en dicho convenio y (c) para pedir a los proveedores inscritos en este convenio o a terceros que se encuentran fuera del convenio marco, la contratación bajo condiciones más ventajosas.

La primera parte de este documento describe los tipos de servicios *cloud* que pueden ser contratados, cuáles son sus ventajas y desventajas y qué forma pueden adoptar.

La segunda parte, establece una serie de aspectos generales al momento de cualquier contratación como:

1. Se debe notar, por obvio que parezca, que el estatuto legal aplicable en esta clase de contratación se rige por la Ley N° 19.886.

2. Atendido los artículos 14 y 15 de la Ley N° 19.886 y los artículos 74 y 76 del reglamento y al hecho a que en esta clase de contratos se hace tomando especial consideración del prestador del servicio, se debe contratar directamente al prestador del servicio.

3. Es muy importante que los abogados junto con los departamentos informáticos y oficiales de seguridad de la información revisen, de forma conjunta y de forma exhaustiva, los términos contractuales del servicio *cloud* que es ofrecido y las características técnicas del mismo.

4. Se debe definir con claridad qué tipo de información va a ser subida a la nube y si debe ser o no encriptada.

Luego, en lo que concierne a los aspectos específicos de contratación, se recomienda:

- Revisar cuáles son los niveles de servicio ofrecidos (SLA).

- Poner especial énfasis en evitar cláusulas que faculten al prestador del servicio a poner término unilateral del contrato o suspender el servicio.

- Considerar la confidencialidad de la información subida a la nube, la protección de los datos personales (en caso de que los haya) y la adopción de medidas de seguridad necesarias para asegurar que la información que se suba a la nube no sea revelada a terceras partes o se pierda irreversiblemente. En este sentido, se sugiere contratar servicios de respaldo (backup) para evitar pérdidas de información y encriptar la información que es subida a la nube.

- Poner atención en mantener los derechos de propiedad intelectual de los documentos y demás informaciones que se suben a la nube.

- Evitar la inclusión de cláusulas que permitan la modificación unilateral de los servicios cloud.

- Establecer la posibilidad de que el órgano contratante pueda auditar al prestador del servicio o que dicho prestador de servicios cuente con determinadas certificaciones.

- Revisar que, en caso de cesar los servicios, el órgano contratante pueda recuperar y descargar los datos que tienen en la nube y pueda, sin mayores costos, el migrar su información a un nuevo proveedor a fin de evitar situaciones de “vendor lock-in”.

- Tomar las medidas necesarias para que, en caso de término del contrato, los datos que están en la nube sean debidamente eliminados de los servidores del prestador del servicio.

- Poner atención al alcance de la responsabilidad del proveedor del servicio. Conviene recordar que las cláusulas limitativas de responsabilidad por parte de los proveedores importa una renuncia anticipada de derechos, cuestión que se encuentra prohibida a los órganos de la Administración del Estado de

conformidad a la jurisprudencia administrativa de la Contraloría General de la República.

- Establecer sanciones importantes en caso de deficiencias en los servicios del proveedor *cloud*.

- Considerar aspectos como la subcotratación de servicios, cambios en el control o propiedad del prestador del servicio y la cesión de contratos.

- Tutelar que tanto el derecho aplicable a la contratación sea el Derecho Chileno y, en caso de disputa, esta se resuelva por los tribunales de la República de Chile.

Finalmente, a modo de anexo, se deja una serie de cláusulas modelo que podrían servir de base para la redacción de bases de licitación, contratos o términos de referencia.

INTRODUCCIÓN

En términos generales, la tecnología de "Computación en la Nube" o *"Cloud Computing"* consiste en un modelo tecnológico que hace posible *"el acceso a red adecuado y bajo demanda a un conjunto de recursos de computación configurables y compartidos (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) cuyo aprovisionamiento y liberación puede realizarse con rapidez y con un mínimo esfuerzo de gestión e interacción por parte del proveedor del cloud."*[1]

Existen grandes beneficios potenciales en torno al uso de esta tecnología puesto que su utilización puede implicar importantes ahorros de costos económicos y de tiempo en la gestión de plataformas electrónicas. Además, dependiendo del prestador del servicio, la computación en nube puede, potencialmente, entregar beneficios tales como la escalabilidad, elasticidad, alto rendimiento, resistencia y seguridad[2].

Por las razones antes anotadas, **la Unidad de Modernización y Gobierno Digital recomienda, como regla general, la adopción de este tipo de soluciones tecnológicas al interior de los órganos de la Administración del Estado**. Ello atendido a que dicha tecnología impacta positivamente en la forma en que tales órganos ejercen sus funciones, con plena consonancia con los principios de eficacia y eficiencia que considera el artículo 3° de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado[3].

---

[1] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN DEL GOBIERNO DE ESPAÑA | INTECO-CERT, 'Riesgos y Amenazas en Cloud Computing', Marzo de 2011, p. 6. Disponible en línea en: <http://bit.ly/TTkcg1> [Visitado: 22 de noviembre de 2012].

[2] AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN (en adelante, "ENISA"), 'Seguridad y resistencia en las nubes de la Administración Pública. Informe para la toma de decisiones', Enero de 2011, p. 7. Disponible en línea en: <http://bit.ly/Sitjte> [Visitado: 22 de noviembre de 2012].

[3] Decreto con Fuerza de Ley Nº 1 del Ministerio Secretaría General de la Presidencia, fija el texto refundido, coordinado y sistematizado de la Ley Nº 18.575, Orgánica Constitucional de Bases

Con todo, al momento de adoptar una tecnología de esta naturaleza, los órganos de la Administración del Estado deben tener en consideración el mandato constitucional que les impone el deber de actuar dentro de sus competencias, respetar el marco legal vigente, proteger y promover los derechos fundamentales de las personas y resguardar la seguridad nacional[4]. Por lo mismo, **dichos órganos deben poner especial atención a una serie de consideraciones legales que permitan adoptar una decisión que se ajuste a los requerimientos establecidos por nuestro Ordenamiento Jurídico**.

El presente documento pretende abordar dichas consideraciones legales de manera de guiar el trabajo de las autoridades, funcionarios y abogados que están involucrados en el proceso de contratación de esta clase de servicio.

Si bien el texto habla de forma permanente sobre contratos, es importante destacar que las recomendaciones de este documento se aplican no solo a la redacción de contratos sino que a todo el proceso de contratación pública. Por lo mismo, estas sugerencias y observaciones debieran considerarse, por ejemplo:

1.- Al momento de redactar las respectivas Bases de Licitación.

2.- En caso de haber un convenio marco, se pueden emplear los criterios y recomendaciones de este documento para:

(a) Decidir contratar o no a determinado oferente;

(b) Para redactar los Acuerdos Complementarios que se puedan considerar en dicho convenio.

Generales de la Administración del Estado, D.O. 17 de noviembre de 2001 (en adelante, "LOCBGAE").

[4] Véase los artículos 1°, 5°, 6° y 7° de la Constitución Política de la República de Chile.

En este sentido es preciso señalar que en el "Convenio Marco de Data Center y Servicios Asociados", contempla la posibilidad de suscribir "Acuerdos Complementarios", en donde, además de consignarse el monto de la garantía de fiel cumplimiento del contrato, se pueden especificar "…las condiciones particulares de la adquisición, tales como condiciones y oportunidades de entrega, entre otros"[5].

La única limitante de tales acuerdos es que éstos no pueden apartarse de los aspectos regulados por el convenio marco.

(c) Pedirle a los proveedores inscritos en este convenio o a terceros que se encuentran fuera del convenio marco, la contratación bajo condiciones más ventajosas, de conformidad a lo dispuesto en el artículo 30, letra d) de la Ley N° 19.886 de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios[6] y artículos 8 y 15 del reglamento de dicha ley.[7]

Por otro lado, cabe destacar que **este documento no es vinculante** y sólo pretende dar recomendaciones de buenas prácticas que permiten la incorporación de esta tecnología de forma informada y de conformidad a nuestro Ordenamiento Jurídico.

Por otra parte, es importante notar que este documento **sólo se enfoca en los aspectos legales básicos** relativos a la contratación de esta clase de servicios. Para quienes quieran tener noticia de los aspectos técnicos a considerar al mo-

[5] Convenio Marco de Data Center y Servicios Asociados, Licitación ID: 2239-17-LP11. Disponible en línea en: <http://bit.ly/1ICERsS> [visitado: 6 de febrero de 2014]
[6] Ley N° 19.886 de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios. D.O. 30 de julio de 2003.
[7] Decreto N° 250, del Ministerio de Hacienda, Aprueba reglamento de Ley N° 19.886 de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios. D.O. 24 de septiembre de 2004.

mento de contratar esta clase de servicios (por ejemplo, evaluación de ventajas, riesgos técnicos, análisis FODA de los diversos servicios *cloud*, modelos de decisión sobre la adopción de servicios *cloud computing*[8], etc.) se sugiere revisar los siguientes documentos:

CUADRO N° 1: LECTURAS RECOMENDADAS RELATIVA A LOS ASPECTOS TÉCNICOS DE CONTRATACIÓN DE SERVICIOS *CLOUD*.

- **AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN (ENISA),** 'Seguridad y resistencia en las nubes de la Administración Pública. Informe para la toma de decisiones', Enero de 2011. Disponible en línea en: <http://bit.ly/Sitjte> [Visitado: 8 de mayo de 2013].

- **GOBIERNO FEDERAL DE LOS ESTADOS UNIDOS DE AMÉRICA, CIO COUNCIL & CHIEF ACQUISITIONS OFFICERS COUNCIL**, 'Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service', 24 de febrero de 2012. Disponible en línea en: <http://1.usa.gov/QztYcN> [Visitado: 8 de mayo de 2013].

El análisis legal efectuado en este documento se basa en la legislación vigente y toma nota de una serie de observaciones legales identificadas por agencias gubernamentales de otros países que han tenido oportunidad de revisar estos temas con mayor profundidad. Así, se ha tomado en cuenta las observaciones del Gobierno Federal de los Estados Unidos de América[9], las guías publicadas por la

[8] Tales como la revisión de las motivaciones de adopción, consideraciones previas a la adopción de dicha tecnología y consideraciones a tener en cuenta durante la prestación del servicio de 'cloud computing'.

[9] OFFICE OF MANAGEMENT AND BUDGET, U.S. CHIEF INFORMATION OFFICER (2011) 'Federal Cloud Computing Strategy', 8 de febrero de 2011. Disponible en línea en: <http://1.usa.gov/WG44Wp> [Visitado: 8 de mayo de 2013]; CIO COUNCIL & CHIEF ACQUISITIONS OFFICERS COUNCIL, 'Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service', 24 de febrero de 2012. Disponible en línea en: <http://1.usa.gov/QztYcN> [Visitado: 8 de mayo de 2013]; NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COM-

Agencia Europea de Seguridad de las Redes y de la Información (en adelante, "ENISA")[10], el Instituto Nacional de Tecnologías de la Comunicación del Gobierno de España[11] (en adelante, "INTECO-CERT") y el Ministerio de Defensa, Seguridad e Inteligencia del Gobierno de Australia[12].

Asimismo, se toma en cuenta los estudios legales y empíricos en torno a la evolución de los contratos de prestación de servicios *cloud* que se han elaborado a nivel comparado[13].

MERCE, 'The NIST Definition of Cloud Computing', NIST Special Publication 800-145, Septiembre de 2011. Disponible en línea en: <http://1.usa.gov/10GjEQZ> [Visitado: 8 de mayo de 2013]; NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE, 'US Government Cloud Computing Technology Roadmap, Release 1.0 (Draft), Volume I High-Priority Requirements to Further USG Agency Cloud Computing Adoption', NIST Special Publication 500-293, Noviembre de 2011. Disponible en línea en: <http://1.usa.gov/UiFmZG> [Visitado: 8 de mayo de 2013]; NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE, 'US Government Cloud Computing Technology Roadmap, Release 1.0 (Draft), Volume II Useful Information for Cloud Adopters', NIST Special Publication 500-293, Noviembre de 2011. Disponible en línea en: <http://1.usa.gov/XJUGT2> [Visitado: 8 de mayo de 2013]; NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE, 'NIST US Government Cloud Computing Technology Roadmap Volume III - Technical Considerations for USG Cloud Computer Deployment Decisions (First Working Draft)', Noviembre de 2011. Disponible en línea en: <http://1.usa.gov/U1WFfa> [Visitado: 8 de mayo de 2013].

[10] ENISA, 'Seguridad y resistencia en las nubes de la Administración Pública…', *Op. Cit.*; ENISA, 'Cloud Computing. Benefits, risks and recommendations for information security', 1 de noviembre de 2009. Disponible en línea en: <http://bit.ly/QBBNNQ> [Visitado: 8 de mayo de 2013].

[11] INTECO-CERT, 'Riesgos y Amenazas en Cloud Computing', *Op. Cit*.

[12] CYBER SECURITY OPERATIONS CENTRE, DEPARTMENT OF DEFENSE, SECURITY AND INTELLIGENCE OF THE GOVERNMENT OF AUSTRALIA, 'Cloud Computing Security Considerations', 12 de abril de 2011. Disponible en línea en: <http://bit.ly/1eu0VIA> [Visitado: 8 de mayo de 2013].

[13] BRADSHAW, Simon, MILLARD, Christopher & WALDEN, Ian, 'Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services', *Legal Studies Research Paper No. 63/2010*, Queen Mary University of London, School of Law, año 2010. Disponible en línea en: <http://bit.ly/1e6JUYH> [Visitado: 8 de mayo de 2013]; HON, Kuan, MILLARD, Christopher & WALDEN, Ian, 'Negotiating Cloud Contracts - Looking at Clouds from Both Sides Now', *Legal Studies Research Paper No 117/2012*, Queen Mary University of London, School of Law, año 2012. Disponible en línea en: <http://bit.ly/LC3khi> [Visitado: 8 de mayo de 2013]; HON, Kuan, MILLARD, Christopher & WALDEN, Ian, 'UK G-Cloud v1 and the impact on cloud contracts', *Legal Studies Re-*

El presente documento se divide en tres partes. La primera de ella describe qué es la tecnología del *Cloud Computing*. La segunda parte discute acerca de cuáles son los aspectos contractuales básicos que los órganos deben tener en cuenta antes de contratar estos servicios. Finalmente, la tercera parte se refiere a aspectos contractuales específicos a los que los órganos contratantes debieran poner especial atención cuando se pretenda negociar esta clase de servicios. Adicionalmente se entrega una breve conclusión sobre la materia y se acompaña un anexo con una serie de cláusulas estándar que podrían ser empleados por los órganos de la Administración del Estado.

I. ¿QUÉ ES EL COMPUTACIÓN EN LA NUBE O "*CLOUD COMPUTING*"?[14]

La Computación en la Nube o *"Cloud computing"* se ha definido como un modelo para hacer posible el acceso a red adecuado y bajo demanda a un conjunto de recursos de computación configurables y compartidos (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) cuyo aprovisionamiento y liberación puede realizarse con rapidez y con un mínimo esfuerzo de gestión e interacción por parte del proveedor del servicio *cloud*.

El origen del término está en el gráfico de uso común para representar Internet como si fuera una nube (*cloud*). Los recursos de computación (*hardware* y *software*) de estos modelos están disponibles a través de Internet.

---

search Paper No 115/2012, Queen Mary University of London, School of Law. Disponible en línea en: <http://bit.ly/1dtiUTa> [Visitado: 8 de mayo de 2013] y MOWBRAY, Miranda, 'The Fog over the Grimpen Mire: Cloud Computing and the Law', *SCRIPTed*, Vol. 6, Issue 1, Abril de 2009, pp. 132-146. Disponible en línea en: <http://bit.ly/1bu8YJk> [Visitado: 8 de mayo de 2013].

[14] **IMPORTANTE:** Este capítulo fue tomado prácticamente en su integridad del documento 'Riesgos y Amenazas en Cloud Computing' del Instituto Nacional de Tecnologías de la Comunicación del Gobierno de España. Sobre este punto, cabe notar que el documento redactado por dicha entidad se encuentra bajo una licencia Reconocimiento-No comercial 3.0 España <http://creativecommons.org/licenses/by-nc-sa/3.0/es/>. Véase INTECO-CERT, 'Riesgos y Amenazas en Cloud Computing', *Op. Cit.*, pp. 6-11.

A continuación, se describen los distintos tipos de infraestructuras y servicios *cloud*.

1. Tipos de infraestructura *Cloud*

Atendiendo a la titularidad de la infraestructura en la nube se pueden distinguir tres tipos de infraestructuras *cloud*: privada, pública y comunitaria. A continuación se presentan las ventajas e inconvenientes de cada uno.

1.1. Nube Pública

Es aquel tipo de *cloud* en el cual la infraestructura y los recursos lógicos que forman parte del entorno se encuentran disponibles para el público en general a través de Internet.

Suele ser propiedad de un proveedor que gestiona la infraestructura y el servicio o servicios que se ofrecen.

Ventajas	Inconvenientes
Escalabilidad	Se comparte la infraestructura con más organizaciones.

Ventajas	Inconvenientes
Eficiencia de los recursos mediante los modelos de pago por uso.	Poca transparencia para el cliente, ya que no se conoce el resto de servicios que comparten recursos, almacenamiento, etc.
Gran ahorro de tiempo y costos.	Dependencia de la seguridad de un tercero.

1.2. Nube Privada

Este tipo de infraestructuras *cloud* se crean con los recursos propios del organismo que lo implanta, generalmente con la ayuda de empresas especializadas en este tipo de tecnologías.

Ventajas	Inconvenientes
Cumplimiento de las políticas internas.	Elevado costo material.
Facilidad para trabajo colaborativo entre sedes distribuidas.	Dependencia de la infraestructura contratada.
Control total de los recursos.	Retorno de inversión lento dado su carácter de servicio interno.

1.3. Nube Comunitaria

Un *cloud* comunitario se da cuando dos o más organizaciones forman una alianza para implementar una infraestructura *cloud* orientada a objetivos similares y con un marco de seguridad y privacidad común.

Ventajas	Inconvenientes
Cumplimiento de las políticas internas.	Seguridad dependiente del anfitrión de la infraestructura.

Ventajas	Inconvenientes
Reducción de costos al compartir la infraestructura y recursos.	Dependencia de la infraestructura contratada.
Rápido retorno de inversión.	

1.4. Nubes Híbridas

Este es un término amplio que 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.

En este caso las ventajas e inconvenientes son los mismos que los relativos a los tipos de *cloud* que incluya la infraestructura.

2. Tipos de Servicios *Cloud*

Los servicios en *cloud* pueden identificarse según se ofrezca *software*, plataformas o infraestructuras como servicio.

2.1. Software como servicio (SaaS)

Este modelo, *Software* como servicio o **SaaS** (del inglés, *'Software as a Service'*) 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 costos tanto de *software* como *hardware*, así como los gastos de mantenimiento y operación.

Las consideraciones de seguridad son controladas por el proveedor del servicio. El suscriptor del servicio únicamente tiene acceso a la edición de las preferencias y a unos privilegios administrativos limitados.

2.2. Plataforma como servicio (PaaS)

Este es el modelo de Plataforma como servicio o **PaaS** (del inglés, *'Platform as a Service'*) en el cual el servicio se entrega como bajo demanda, desplegándose el entorno (*hardware* y *software*) necesario para ello. De esta forma, se reducen los costos y la complejidad de la compra, el mantenimiento, el almacenamiento y el control del *hardware* y el *software* que componen la plataforma.

El suscriptor del servicio tiene control parcial sobre las aplicaciones y la configuración del entorno ya que la instalación de los entornos dependerá de la infraestructura que el proveedor del servicio haya desplegado. La seguridad se comparte entre el proveedor del servicio y el suscriptor.

2.3. Infraestructura como Servicio (IaaS)

Es un modelo en el cual 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. Se denomina Infraestructura como Servicio o **IaaS** (del inglés, *'Infrastructure as a Service'*).

El fin principal de este modelo es evitar la compra de recursos por parte de los suscriptores, ya que el proveedor ofrece estos recursos como objetos virtuales accesibles a través de un interfaz de servicio.

El suscriptor mantiene generalmente la capacidad de decisión del sistema operativo y del entorno que instala. Por lo tanto, la gestión de la seguridad corre principalmente a cargo del suscriptor.

II. ASPECTOS BÁSICOS A CONSIDERAR AL MOMENTO DE CONTRATAR SERVICIOS *CLOUD*.

1. Aplicación de la Ley N° 19.886

Por obvio que parezca, parece razonable advertir de antemano que, para efectos de llevar adelante la contratación de esta clase de servicios, es preciso que el órgano contratante se ajuste a las normas establecidas en la Ley N° 19.886 de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios y su reglamento

Frente a cualquier duda sobre la materia, conviene destacar que la Dirección de Compras y Contratación Pública tiene, dentro de sus funciones, tiene el deber asesorar a los organismos públicos en la planificación y gestión de sus procesos de compras y contrataciones y promover la máxima competencia posible en los actos de contratación de la Administración. En este sentido, siempre es factible que, frente a cualquier duda sobre el alcance de esta normativa, se efectúen consultas a dicho órgano.

Por otra parte, en tales casos siempre es relevante consultar la jurisprudencia administrativa de la Contraloría General de la República. En este sentido, conviene destacar que el sitio web de dicho organismo contiene una completa base de da-

tos de los dictámenes que ha publicado sobre la materia. Este repositorio puede consultarse en el sitio web www.contraloria.cl.

2. Sobre la importancia de contratar directamente al prestador del servicio *cloud*

A diferencia de la compra de equipos computacionales, hardware o licencias de software, el *cloud computing* implica un servicio que, en gran medida, es contratado tomando especial consideración a la persona del contratista. Atributos del proveedor tales como su reputación, capital financiero y humano, capacidad técnica, idoneidad de la tecnología que es de propiedad del contratista, experiencia, etc., son aspectos centrales que llevan a los órganos a contratar a determinado proveedor.

La naturaleza de esta clase de contratos obliga a ser muy cuidadoso en la elección del oferente. Por lo mismo, se recomienda que, antes de decidir una determinada contratación, **se tengan a la vista los antecedentes de la empresa, verificar que sea el oferente quien presta el servicio cloud[15], investigar la experiencia que han tenido otros órganos de la Administración del Estado con dicho proveedor y solicitar al oferente las demás informaciones escritas que sean necesarias para que el órgano contratante sepa las capacidades del proveedor del servicio**.

En este sentido, es muy importante notar que en la industria tecnológica es muy usual que quienes ofrecen productos tales como *hardware* y *software* son terceros distintos a quien lo ha fabricado. En tales casos, estos terceros oferentes suelen ser sociedades filiales establecidas en Chile del proveedor tecnológico o se trata de terceros que operan como vendedores oficiales (‘*resellers*’), agentes, intermediarios o asociados (‘*partners*’) del proveedor tecnológico.

[15] Conviene notar que, tal como lo veremos, el proveedor del servicio puede subcontratar parcialmente los servicios. Véase punto punto III.12 del presente documento.

Si bien esta práctica es razonable en el caso de productos como *hardware* y s*oftware* y determinados servicios (por ejemplo, mantenimiento o soporte), **en el caso de los servicios *cloud* estamos a una situación sumamente diversa: el carácter de contrato *intuitu personae*[16] y de tracto sucesivo[17] de los contratos de prestación de servicios cloud hace fundamental que éste sea suscrito directamente con el prestador del servicio *cloud* y no con el tercero oferente o, alternativamente, que el tercero oferente represente legalmente al prestador del servicio *cloud* para efectos de suscribir el contrato a nombre de este último.**

Lo anterior se debe al hecho que es el prestador del servicio *cloud* –y no el tercero oferente− quien realmente ejecuta la obligación de llevar adelante el servicio, almacena información, protege la confidencialidad de los datos del órgano contratante, etcétera.

Lo señalado precedentemente tiene, además, plena consonancia con lo dispuesto con los artículos 14 y 15 de la Ley N° 19.886 y los artículos 74 y 76 del reglamento de dicha ley, disposiciones que, en general, señalan que no se permite que el contratista ceda total o parcialmente del contrato y que sólo permiten una subcontratación parcial de los servicios[18].

3. Sobre la importancia de revisar los términos y condiciones propuesta por el prestador del servicio *cloud*

[16] Un contrato intuitu personae es, en términos simples, un contrato en donde las características personales del contratante son esenciales a la hora de decidir contratar.
[17] Un "contrato de tracto sucesivo" es "aquel en que las obligaciones de las partes o de una de ellas, a lo menos, consisten en prestaciones continuas o repetidas durante cierto espacio de tiempo." ALESSANDRI, Arturo, "De los Contratos", Ed. Jurídica de Chile, Santiago, año 2010, p. 43.
[18] En cuanto al tema de la subcontratación, véase el punto III.12 del presente documento.

Es muy importante que los abogados de los órganos públicos revisen, en todo caso y de forma exhaustiva, los términos contractuales del servicio *cloud* que es ofrecido.

Comúnmente, estos términos están publicados en los sitios web de dichos prestadores de servicios y se incluyen en enlaces con expresiones tales como “términos y condiciones”, “términos de uso”, “Niveles de Servicio”, “Políticas de uso aceptable”, “políticas de privacidad” y otras denominaciones como “aviso legal”, “propiedad intelectual”, “seguridad”, etcétera. Tales documentos suelen describir los derechos y obligaciones de las partes, la forma en que será tratada la información que tratará el servicio *cloud*, los resguardos de seguridad que toma la compañía prestadora del servicio, etcétera.

Es deber de los órganos de la Administración el exigir el acceso a tales condiciones al proveedor para que los abogados del servicio los lean y se adopte una decisión informada y conforme a derecho. El proveedor tiene la obligación de informar de forma detallada dichos aspectos contractuales. Se sugiere exigir que esas condiciones se encuentren en idioma Español.

En este sentido, más allá de la documentación suministrada por los oferentes, los órganos públicos deben hacer, de forma independiente, una revisión exhaustiva de dichos sitios web y contrastar la información contenida en ellos con la documentación que los propios oferentes les entreguen. Si existen inconsistencias entre la documentación suministrada por el oferente con la información recopilada independientemente, se sugiere consultar al mismo prestador del servicio acerca de dicha inconsistencia.

Por otra parte, cabe notar que esta documentación generalmente es sumamente extensa, compleja y suele incorporar por referencia a otros documentos mediante la inclusión de hiperenlaces. En tales casos, se sugiere revisar todos los enlaces y documentos a que se haga referencia.

Además, en caso de llegar acordarse de que los documentos contenidos en tales sitios web serán parte de los términos del contrato a suscribir, se sugiere evitar mantener la referencia a tales enlaces e incorporar dichos documentos en los anexos del instrumento a firmar. Por lo demás, así lo ha exigido Contraloría General de la República en el caso de los decretos y resoluciones aprobatorios de contratos enviados a ese organismo para el trámite de toma de razón: en tales casos, se requiere que todos los documentos que formen parte del contrato (incluyendo anexos, Niveles de Servicio, Términos y Condiciones, Políticas de Privacidad, etc.) se encuentren físicamente incorporados al texto del acto administrativo que los aprueba.

Además, tanto las bases de licitación como el contrato debieran ser explícitos en cuanto a qué términos de los antes aludidos se aplican y cuáles no a fin de que quede absoluta claridad en torno al alcance de la contratación. En tal caso, siempre debiera consignarse una cláusula del contrato que establezca que, en caso de contradicción entre éste y tales términos y condiciones, debe primar siempre lo establecido en el contrato/licitación y lo previsto en la legislación chilena.

Finalmente, atendida la extensión y complejidad técnica de tales documentos, **es importante que esta revisión se efectúe, de forma conjunta, por los departamentos jurídicos, las unidades informáticas y los encargados de seguridad de la información.** Ello con miras a que el servicio tenga una visión global acerca del servicio que se pretende contratar, incluyendo sus ventajas, riesgos y características.

Cualquier duda que tengan los órganos contratantes pueden contactarse con los asesores legales de la Unidad de Modernización y Gobierno Digital del Ministerio Secretaría General de la Presidencia[19].

[19] www.modernizacion.gob.cl.

4. ¿Qué tipo de información es la que se quiere pasar a servicios *cloud*?

Tal como comentamos en la introducción de este documento, se recomienda el uso de Cloud Computing puesto que tales servicios pueden traer aparejado un sinnúmero de ventajas en materia de eficiencia, seguridad y calidad de servicio para los órganos de la Administración del Estado. No obstante, al igual que cualquier otra tecnología, los servicios *cloud* no están exentos de riesgos[20].

Particularmente en el contexto de las *nubes públicas*, uno de los temas relevantes a considerar es el hecho de que el órgano público no maneja ni controla directamente los dispositivos en donde la información es almacenada[21]: en tal caso, la información se encuentra en las dependencias del proveedor del servicio *cloud*[22].

Consecuentemente, en dichas circunstancias, se pueden presentar una serie de contingencias que dicen relación con el tema de la seguridad de la información que trataremos en el punto III y que se deben considerar al momento de usar servicios *cloud* (por ejemplo, la pérdida de la información, el acceso o uso de los datos del órgano por terceros no autorizados o por el propio prestador del servicio para fines distintos a los que son objeto del contrato, etcétera)[23].

En este sentido, **es fundamental que los órganos de la Administración del Estado, antes de adoptar cualquier decisión sobre la materia, se pregunten qué tipo de información es la que se pretende alojar en los sistemas del prestador del servicio *cloud***.

---

[20] Véase INTECO-CERT, 'Riesgos y Amenazas en Cloud Computing', Marzo de 2011. Disponible en línea en: <http://bit.ly/TTkcg1> [Visitado: 22 de noviembre de 2012].
[21] ENISA, 'Seguridad y resistencia en las nubes de la Administración Pública…', *Op. Cit.*, p. 41.
[22] En el caso de las nubes privadas, estas consideraciones no aplican puesto que el servicio mismo está bajo exclusivo del propio órgano estatal.
[23] Véase el punto III del presente documento.

Así, antes de pensar en contratar un servicio *cloud*, tales órganos debieran hacerse las siguientes preguntas respecto de dicha información y servicio:

(a) ¿Es esta información sensible para la Seguridad Nacional?

(b) ¿Es dicha información pública o es reservada de conformidad a lo dispuesto en la Ley N° 20.285?

(c) ¿Cuán importante es para la organización mantener en reserva la información que mantengo en el servicio *cloud*? ¿Cuáles son las consecuencias en caso de que esta información se filtrara?

(d) ¿Tengo bases de datos de personas naturales? ¿Son estos datos sensibles? ¿Cuál es el tamaño de dichas bases de datos? ¿Cuáles son las consecuencias para las personas de que tales datos se filtraran? (ver punto III.2)

(e) ¿En mis bases de datos se contiene información comercial sensible o perteneciente a empresas que no han autorizado la divulgación de dicha información?

(f) ¿Con la potencial divulgación de la información subida a nube se afectarían los derechos de propiedad intelectual o industrial o, en general, cualquier derecho de terceras personas en los casos en que éstas no hubiesen autorizado dicha divulgación?

(g) ¿Contrataré un servicio de nube pública, privada, comunitaria o híbrida? ¿Dónde se encuentran las instalaciones del prestador del servicio (ver punto III.3.)?

Dependiendo de las respuestas a dichas preguntas, los órganos deben adoptar la decisión de adoptar o no un servicio *cloud* y, si deciden adoptarlo, cuánta impor-

tancia le deben dar tales órganos a aspectos contractuales como la protección de datos personales, la confidencialidad y la seguridad de la información.

Así, no parece razonable contratar servicios *cloud* (al menos en su modalidad pública) cuando la información que se pretende manejar en ese sistema es propia de órganos de inteligencia, o donde la confidencialidad de las comunicaciones es un tema fundamental para la Seguridad Nacional o donde se estima que la reserva de la información es un aspecto importante para el órgano.

Por otra parte, al otro extremo se pueden encontrar aquellos casos en donde la información que se pretende pasar a la nube no contiene datos personales y/o se trata de información eminentemente pública. Tal es el caso del *hosteo* de sitios webs gubernamentales dirigidos al público general (en donde se contiene información que es eminentemente pública) o el almacenamiento de datos disociados y/o que no son confidenciales. En tales circunstancias, las consideraciones sobre confidencialidad de la información debiesen ser de menor relevancia, sin perjuicio de que se debe poner atención en que el servicio sea lo suficientemente seguro como para garantizar que la información del órgano público no se pierda.

Cada órgano puede sobre la base de los criterios antes señalados determinar que algún tipo de información pueda ser subida a la nube y otra se mantenga en servidores del órgano.

III. ASPECTOS CONTRACTUALES ESPECÍFICOS EN LOS SERVICIOS *CLOUD*

1. Continuidad del Servicio

Los órganos de la Administración del Estado tienen el deber legal de atender las necesidades públicas en forma continua y permanente[24]. Desde la perspectiva

[24] Artículo 3, LOCBGAE.

reglamentaria, el decreto supremo N° 83/2004 sobre seguridad de los documentos electrónicos exige la adopción de medidas para mantener la continuidad de operaciones críticas para las instituciones[25]. Por su parte, el decreto supremo N° 14/2014 exige se adopten medidas para que las sus plataformas electrónicas a fin de que estas se mantengan operativas[26].

En consecuencia, tales órganos deben poner especial atención a la continuidad permanente del servicio *cloud* puesto que, en caso contrario, se podría ver impedido de satisfacer dichas necesidades de conformidad a lo que requiere la ley.

Como consecuencia de lo anterior, se debe revisar con cuidado los niveles de servicios (SLA) en que el prestador *cloud* está en condiciones de garantizar. En este sentido, se debe privilegiar a aquellos proveedores de servicios que tengan la capacidad organizativa y técnica que pueda asegurar la continuidad del servicio.

Adicionalmente, en tales casos, se debiera considerar la aplicación de multas en caso de incumplir con tales niveles.

Por otra parte, **una cuestión que está del todo vedada** por la Contraloría General de la República en esta materia, es la inclusión de cláusulas contractuales que permitan al proveedor de servicios poner término unilateral al contrato o suspender su continuidad[27]. Luego, bajo ninguna circunstancia debiera incluirse alguna cláusula de esta naturaleza.

Finalmente, existe siempre el caso de que el prestador del servicio se vea impedido de cumplir con sus obligaciones debido a una causa de fuerza mayor o caso

[25] Véase, por ejemplo, artículo 35, Decreto N° 83, del Ministerio Secretaría General de la Presidencia, Aprueba norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos, D.O. 12.01.2005.
[26] Véase número 3, letra h) del artículo primero transitorio del Decreto N° 14, del Ministerio de Economía, Fomento y Turismo, Modifica Decreto nº 181, de 2002, que aprueba Reglamento de la ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, y deroga los decretos que indica, D.O. 27.02.2014
[27] Véase Dictamen N° 44.186, de 4 de agosto de 2010.

fortuito. En tales casos, se debiera obligar al prestador del servicio a informar de esa circunstancia tan pronto sea posible para que el órgano contratante adopte las medidas de contingencia que sean necesarias. Adicionalmente, se debiera facultar al órgano de la Administración para terminar el contrato en caso de que esta circunstancia fuere prolongada. Finalmente, a fin de restringir el alcance de la fuerza mayor o caso fortuito, debiera explicitarse que no constituye un caso fortuito el embargo de los bienes de dicho prestador, huelga de sus trabajadores, etcétera. En el anexo del presente documento se deja a disposición un modelo de cláusula sobre la materia.

Adicionalmente, es importante contratar servicios de respaldo para la continuidad del Servicio. Por mucho que los SLA suelen comprometerse a altos niveles de disponibilidad (por sobre el 99%, en muchas ocasiones), siempre existe la posibilidad que se presenten desperfectos que impliquen la caída total del sistema. Es por lo mismo que se recomienda contratar a otros proveedores para que sirvan de respaldo en caso de caída de los sistemas del primer proveedor. Conviene en este sentido tener presente que el servicio de respaldo o *backup* no es lo mismo que el servicio cloud contratado; el primero sólo operara en caso de caída del segundo.

Finalmente, en caso de término de la relación contractual, es importante considerar cláusulas que garanticen la continuidad operacional de los sistemas de la institución contratante. En este sentido, se debe asegurar que el contratista entregue al Ministerio la información utilizada en la prestación de los servicios hasta ese momento, de modo de habilitar las soluciones que sean adecuadas. Asimismo, el contratista en el proceso de terminación del contrato debiera estar obligado a prestar, a su costa, toda la colaboración que el Servicio requiera para que este último pueda traspasar a otro proveedor, para mantener la continuidad de la operación[28].

[28] En el anexo de este documento se deja un modelo de cláusula.

2. Protección de Datos Personales[29]

Puede que dentro de las informaciones que se pretendan subir a la nube se encuentren bases de datos de personas naturales.

Se considera que los órganos de la Administración pueden contratar esta clase de servicios, en la medida que se tomen ciertas prevenciones.

En este sentido, conviene recordar que, de conformidad a Ley N° 19.628 sobre protección a la vida privada, los órganos pueden tratar datos personales respecto de las materias de su competencia y sin consentimiento del titular[30], en la medida que cumplan con los principios y normas que establece dicha ley. En este contexto, "[los] *órganos o servicios públicos, en conformidad a lo dispuesto en el artículo 8° de la Ley N° 19.628,* [pueden] *encargar el tratamiento de los datos a un tercero, que tendrá la calidad de mandatario*"[31].

Ahora, una vez hecho el análisis sugerido en el punto II.4., y en caso que se decida contratar un prestador de servicio *cloud,* alojando en sus sistemas datos protegidos por la Ley N° 19.628, se deben tomar una serie de resguardos contractuales[32].

[29] Sobre el tema del tratamiento de datos personales por parte de los órganos del Estado, se sugiere consultar CONSEJO PARA LA TRANSPARENCIA, 'Recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la Administración del Estado'. Santiago, 5 de septiembre de 2011. Disponible en línea en: <http://bit.ly/Vbb9hs> [Visitado: 22 de noviembre de 2012].

[30] Artículo 20 de la Ley N° 19.628. En este mismo sentido, véase CONTRALORÍA GENERAL DE LA REPÚBLICA, Dictamen N° 43.866 de 3 de octubre de 2003.

[31] CONSEJO PARA LA TRANSPARENCIA, 'Recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la Administración del Estado'. *Op.Cit.*, p. 15.

[32] En este sentido, cabe recordar que la jurisprudencia de Contraloría requiere a los órganos de la Administración tome todos los resguardos necesarios (incluido los contractuales) para que tal información no sea utilizada en finalidades distintas a las deseadas por el servicio. Véase CONTRA-

En efecto, en el caso de contratar servicios cloud se hace necesario que el contrato con dicho proveedor cumpla con las siguientes condiciones:

(a) Que sea otorgado por escrito;

(b) Que dicho instrumento deje especial constancia de las condiciones de la utilización de los datos por parte del proveedor del servicio *cloud*;

(c) Que el contrato contenga cláusulas que:

(i) Obliguen al prestador para a adoptar *"*[…] *los resguardos necesarios para que tal información no sea utilizada en finalidades distintas a las deseadas por el servicio"*[33];

(ii) Protejan la debida confidencialidad de los datos, a fin de que *"…no se vulneren, además, las disposiciones que regulan la información de carácter secreto o reservado"*[34]. Particular atención se debe poner al artículo 7 de la Ley N° 19.628, el que obliga a las personas que están en el tratamiento de los datos (en este caso, el prestador del servicio *cloud*), a guardar reserva o secreto de los datos que están siendo objeto de tratamiento[35]; y

(iii) Ordenen al prestador del servicio adoptar, en su calidad de mandatario, *"*[…] *todas las medidas, tanto organizativas como técnicas, para res-*

LORÍA GENERAL DE LA REPÚBLICA, Dictamen N° 43.866 de 3 de octubre de 2003 y Dictamen N° 57.623 de 22 de noviembre de 2004.

[33] CONTRALORÍA GENERAL DE LA REPÚBLICA, Dictamen N° 43.866 de 3 de octubre de 2003 y Dictamen N° 57.623 de 22 de noviembre de 2004.

[34] CONTRALORÍA GENERAL DE LA REPÚBLICA, Dictamen N° 43.866 de 3 de octubre de 2003.

[35] *"Artículo 7°.- Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo."*

guardar la integridad, confidencialidad y disponibilidad de los datos contenidos en sus registros con la finalidad de evitar la alteración, pérdida, transmisión y acceso no autorizado de los mismos"[36]. Lo anterior, atendido al deber legal del responsable de las bases de cuidar de tales datos con la debida diligencia, haciéndose responsable de los daños (artículo 11 de la Ley N° 19.628[37])

(iv) Que hagan civilmente responsable al prestador del servicio *cloud* acerca de la filtración o uso inadecuado de los datos personales que le son confiados[38].

(v) Que obliguen al prestador del servicio y sus empleados cumplir con las disposiciones establecidas por la Ley N° 19.628[39].

El mandato a que se hace referencia debe ser parte integrante del instrumento donde consta el contrato de prestación de servicios *cloud*.

Más allá de que pueda contratarse esta clase de servicios, cabe precisar que **lo anterior no faculta a los servicios públicos a ceder o transferir tales datos personales al prestador del servicio**[40]. Por lo mismo, se debe tomar especial cuidado de que quede absolutamente claro que la propiedad sobre tales bases de

[36] CONSEJO PARA LA TRANSPARENCIA, 'Recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la Administración del Estado'. *Op.Cit.*, p. 15.
[37] *"Artículo 11.- El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños."*
[38] CONSEJO PARA LA TRANSPARENCIA, 'Recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la Administración del Estado'. *Ibídem.*
[39] CONSEJO PARA LA TRANSPARENCIA, 'Recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la Administración del Estado'. *Ibídem.*
[40] CONTRALORÍA GENERAL DE LA REPÚBLICA, Dictamen N° 43.866 de 3 de octubre de 2003 y Dictamen N° 57.629 de 16 de diciembre de 2003.

datos se mantienen en el servicio público y, bajo ninguna circunstancia, son cedidas al prestador del servicio *cloud*.[41]

3. Confidencialidad de la información

Uno de los temas relevantes a considerar en materia de contratación de esta clase de servicios es la confidencialidad de las informaciones y datos que son subidos a la nube. Esto tiene particular importancia no solo en el caso de los datos personales y datos sensibles, sino que también cuando el órgano respectivo maneja información secreta o reservada de conformidad a Artículo 21 de la Ley N° 20.285[42].

En todas estas ocasiones, el tema de la confidencialidad de la información es un aspecto legal relevante que deben considerar los órganos de la Administración del Estado.

Si luego del análisis descrito en el punto II.4, el órgano de la Administración del Estado adopta la decisión de subir esa información a la nube, se deben adoptar una serie de medidas de seguridad. Es así que, en tales casos, deben siempre existir cláusulas de confidencialidad acerca de los datos almacenados en el servicio *cloud*, (1) prohibiendo que dicha información sea informada a terceros y (2) exija que esta información sea tratada por el prestador únicamente para la ejecución del contrato[43].

En este mismo sentido, es conveniente que en las respectivas bases de licitación, se exija a los oferentes que, en el evento de ser adjudicados, suscriban una declaración jurada que contenga un compromiso de confidencialidad en términos similares a los anotados en la cláusula estándar que se anexa al final del presente documento.

[41] En el anexo de este documento se pone a disposición un modelo de cláusula relativa a la confidencialidad y protección de datos personales. Nos remitimos a ella.
[42] Ley N° 20.285, sobre acceso a la Información Pública. D.O. 20 de agosto de 2008.
[43] En el Anexo del presente documento se deja a disposición un modelo de cláusula que podría ser empleada por los órganos de la Administración del Estado en este sentido.

Asimismo, **es sumamente importante que, en tales casos, la información a alojarse en los sistemas del prestador del servicio cloud sea siempre encriptada** (por ejemplo, bajo estándares tales como AES (NIST) de 128, 192 o 256 bits).

§ El caso de los proveedores extranjeros

Es muy común que los servidores del prestador del servicio *cloud* sean proveedores extranjeros y/o que éstos almacenen la información en servidores ubicados en el extranjero. Lo anterior conlleva, consecuentemente, a que el prestador del servicio se encuentre sometido a normas extranjeras que facultan a agencias estatales de tales países a solicitarles la información que éstos tengan en sus infraestructuras. Ejemplos bastante conocidos en esta materia son la *Foreign Intelligence Surveillance Act*[44] y la *USA PATRIOT ACT* (Estados Unidos)[45] o la *Regulation of Investigatory Powers Act 2000* (Reino Unido)[46], los que facultan a diversos órganos de seguridad e inteligencia de tales países para requerir información a los prestadores de servicios tecnológicos que sean de su nacionalidad o cuyas dependencias se ubiquen en dichos países.

En este sentido, tiene plena aplicación para el caso chileno las recomendaciones de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA):

> *"Cuando el alojamiento de infraestructuras de la nube se extienda más allá de la jurisdicción local, el organismo público debe tener en cuenta las implicaciones y garantías correspondientes ofrecidas por su proveedor o proveedores. Si los datos gubernamentales están siendo utilizados fuera por grupos privados en jurisdicciones extranjeras, esto crea el riesgo de que los tribunales extranjeros citen a comparecer a la*

[44] *Foreign Intelligence Surveillance Act of 1978*, 50 U.S.C. ch. 36
[45] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (USA PATRIOT ACT) Act 2001, Title V, s. 505.
[46] *Regulation of Investigatory Powers Act 2000*, Part II, s. 28.

entidad privada y, por lo tanto, tengan acceso a los datos del gobierno. […]"[47]

A mayor abundamiento, se han reportado casos en donde agencias de inteligencia de otros países solicitan datos e informaciones contenidas en los servidores de los prestadores de servicios tecnológicos sin la intervención de un órgano jurisdiccional o bajo tribunales que emiten sus autorizaciones de forma reservada[48]. En este sentido, particular notoriedad ha tenido la existencia del programa 'PRISM' llevado adelante por la *National Security Agency* (NSA) para la prevención de ataques terroristas y por la que los principales proveedores de servicios en Internet se han visto en la obligación de entregar información[49].

Este tipo de circunstancias ha llevado algunos estados de Canadá a requerir, por regla general, que los prestadores tengan sus servidores ubicados en su país o se privilegien el uso de nubes privadas[50]. La misma situación explica que en Europa algunos clientes de esta clase de servicios tiendan a exigir que los servidores se encuentren en dicho continente o se inclinen por el uso de las nubes privadas[51].

---

[47] ENISA, 'Seguridad y resistencia en las nubes de la Administración Pública…', *Op. Cit.*, p. 41.
[48] Véase 'Data privacy: Out of shape. The rules on what data governments can demand from communications companies need tightening', *The Economist*, 21 de julio de 2012. Disponible en línea en: <http://econ.st/1byZBv0> [visitado: 29 de diciembre de 2012]; SAVAGE, Charlie, 'Democratic Senators Issue Strong Warning About Use of the Patriot Act', *The New York Times*, 16 de marzo de 2012. Disponible en línea en: <http://nyti.ms/LC3Pbf> [visitado: 29 de diciembre de 2012].
[49] 'Surveillance: Look who's listening' *The Economist*, 15 de junio de 2013. Disponible en línea en: <http://econ.st/1jiJExZ> [visitado: 1 de julio de 2013]; SAVAGE, Charlie, WYATT, Edward and BAKER, Peter, 'U.S. Confirms That It Gathers Online Data Overseas' *The New York Times*, 6 de junio de 2013. Disponible en línea en: <http://nyti.ms/1azEg6v> [visitado: 1 de julio de 2013]; MILLER, Claire, 'Tech Companies Concede to Surveillance Program' *The New York Times*, 7 de junio de 2013. Disponible en línea en: <http://nyti.ms/1e6L3PT> [visitado: 1 de julio de 2013]
[50] Véase MOWBRAY, Miranda, 'The Fog over the Grimpen Mire: Cloud Computing and the Law', *SCRIPTed*, Vol. 6, Issue 1, Abril de 2009, pp. 132-146. Disponible en línea en: <http://bit.ly/1bu8YJk> [Visitado: 4 de diciembre de 2012].
[51] Véase EUROPEAN PARLIAMENT, Directorate General for Internal Policies, 'Cloud Computing', IP/A/IMCO/ST/2011, 18 de mayo de 2012 Disponible en línea en: <http://bit.ly/1IDpDUu> [visitado: 29 de diciembre de 2012].

No obstante lo anterior, se desaconseja descartar de plano el uso de nubes públicas por el mero hecho de que el prestador del servicio y/o sus infraestructuras se encuentren en el extranjero.

Más bien, se sugiere que el órgano contratante adopte la decisión sobre la base de los siguientes pasos:

- Determinar el tipo de información que se quiere subir a los servidores de los servicios *cloud* de conformidad a lo indicado en el punto II.4. de este documento.

  No se ve mayor inconveniente de contratar a proveedores extranjeros en aquellos casos en que la información que se pretende almacenar es eminentemente pública.

- Revisar la legislación en materia de protección de datos y privacidad que rige al prestador del servicio *cloud* y determinar si dichos marcos regulatorios establecen estándares de protección que son o no lo suficientemente robustos como para proteger adecuadamente los intereses del órgano contratante.

  Si se está frente a un régimen que garantiza la reserva de los datos de forma adecuada, no se ve inconveniente de contratar servicios de computación en la nube extranjeros.

- De preferencia, se sugiere en estos casos encriptar siempre la información que será alojada en las infraestructuras del prestador del servicio cloud.

4. Seguridad de la información

El tema de la seguridad de la información puede ser asumido desde, a lo menos, cuatro perspectivas:

(a) Que el prestador del servicio *cloud* tenga e implemente las medidas técnicas y organizativas adecuadas para que la información que es almacenada en la nube no se pierda, dañe o corrompa

Tal como lo sugiere la ENISA, *"*[la] *integridad y la disponibilidad de los datos son elementos esenciales en la prestación de los servicios de computación en la nube"*[52].

Cuando se estudie la contratación del servicio *cloud*, se sugiere poner especial atención al hecho de que el prestador del servicio cuente con alguna certificación que asegure que éste cumple con normas sobre seguridad de la información tales como, por ejemplo, la normativa ISO 27000. Se sugiere privilegiar a los prestadores de servicios que cuenten con esta clase de certificaciones puesto que, de conformidad a lo establecido en los PMG de Seguridad de la Información y en las normas técnicas de seguridad de la información[53], se obligan a los órganos de la Administración del Estado cumplir con normativa de seguridad como la antes citada. Luego, no se podría contratar prestadores de servicios *cloud* que se guíen por estándares de seguridad de la información que sean menos rigurosos[54].

Por otra parte, **se recomienda siempre respaldar la información contenida en la nube**. Así, en caso de que el prestador del servicio tenga una contingencia de pérdida de información, el contratante no sufriría perjuicio puesto que la duplicación permitiría recuperar dicha información.

(b) Que los datos que se almacenan en las instalaciones del prestador del servicio no sean accedidos/utilizados por terceras personas

[52] ENISA, 'Seguridad y resistencia en las nubes de la Administración Pública…', *Op. Cit.*, p. 43.
[53] Decreto Supremo N° 83, de 2005, del Ministerio Secretaría General de la Presidencia que aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos. D.O. 12 de enero de 2005.
[54] En un mismo sentido, ENISA, 'Cloud Computing. Benefits, risks and recommendations for information security', *Op. Cit.*, p. 124.

Entre las razones más comunes que esto se puede producir es a través de una brecha/violación de seguridad o cuando el prestador del servicio haya revelado, sin autorización del cliente, la información a una tercera persona.

Sobre el punto, se debe poner atención a los aspectos de confidencialidad y protección de datos personales, de conformidad a lo indicado en los puntos III.2. y III.3. ya tratados.

(c) Que los datos que almacena el prestador del servicio no sean accedidos/utilizados por éste para fines distintos a los que establece el contrato

Otro tema relevante es el establecimiento de cláusulas que se aseguren expresamente que el prestador del servicio *cloud* trate la información y datos únicamente con la finalidad establecidas en el contrato. En este sentido, es importante consignar la finalidad del contrato en el mismo instrumento y regular el tema del empleo de los datos: cómo se harán, bajo qué presupuestos, etcétera.

En este sentido, una medida adicional sobre la materia es consignar en los respectivos contratos que, una vez terminado éste, el proveedor deberá entregar la información al órgano contratante y deberá destruir cualquier copia que pudiere tener en sus sistemas.

(d) Que los datos cuando están siendo comunicados entre el prestador del servicio y el cliente de forma segura

Una cuestión relevante a revisar es si acaso las comunicaciones y el acceso remoto que se da entre el prestador del servicio y el órgano contratante tiene la seguridad suficiente como para evitar que sean interceptadas por terceros. En este sentido, se requiere revisar atentamente las políticas de seguridad que tengan los proveedores y poner especial énfasis a la seguridad de di-

chas comunicaciones (por ejemplo, si estas comunicaciones están encriptadas).

Como cuestión adicional, se sugiere que los temas contractuales asociados a la seguridad sean tratados de forma multidisciplinaria, incluyendo abogados, informáticos y otros funcionarios. En este sentido, tiene especial importancia las opiniones que debiera emitir el oficial de seguridad de la información al interior de la institución.

Como cuestión final, se recomienda establecer cláusulas que se hagan cargo de los problemas indicados anteriormente. El anexo de este documento contiene algunas cláusulas que podrían servir de modelo a este respecto.

5. Propiedad Intelectual

Otro tema relevante en torno a la contratación de los servicios *cloud* es la existencia de una cláusula sobre propiedad intelectual.

En este sentido, el órgano contratante debe poner especial énfasis de que es el titular de los derechos de propiedad intelectual sobre la documentación y bases de datos que sube al servicio *cloud* y que éstas sólo podrá ser utilizadas por el proveedor del servicio *cloud* para efectos de la ejecución del contrato. Cualquier otro uso debiera contar la autorización escrita del órgano contratante[55].

Adicionalmente, y siguiendo los criterios formulados por la ENISA[56], se estima aconsejable negociar cláusulas en donde el prestador del servicio *cloud* es penalizado por la violación a los derechos de propiedad intelectual del órgano contratan-

[55] En este mismo sentido, véase CIO COUNCIL & CHIEF ACQUISITIONS OFFICERS COUNCIL, 'Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service', *Op. Cit.*, p. 25.
[56] ENISA, 'Cloud Computing. Benefits, risks and recommendations for information security', *Op. Cit.*, p. 109.

te. Asimismo, debiera dejarse constancia de que una violación sustancial a esta obligación debiera permitir al órgano contratante poner término inmediato al contrato y aplicar multas de importancia.

6. Modificación unilateral

En muchos casos es posible encontrar que los términos y condiciones del prestador de servicios *cloud* le otorga la facultad de modificar unilateralmente los términos de contratación[57].

Lo anterior, **no** puede ser aceptado por el órgano contratante. Ello porque, de acuerdo a la jurisprudencia administrativa de Contraloría General de la República, los órganos de la Administración del Estado no pueden suscribir contratos en donde se da la facultad al prestador del servicio para modificar el contrato dando aviso a su contraparte[58].

Por lo mismo se recomienda establecer en el contrato que cualquier modificación deberá hacerse de forma expresa, por escrito y de común acuerdo por las partes, debiendo aprobarse por el acto administrativo correspondiente.

7. Auditoría

Tanto a nivel europeo como estadounidense, las agencias gubernamentales suelen poner énfasis en la necesidad de que los órganos contratantes estén en condiciones de auditar las políticas, procesos, sistemas y servicios del prestador del servicio *cloud*[59].

[57] En el mismo sentido, véase BRADSHAW, MILLARD y WALDEN, Ian, 'Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services', *Op. Cit.*, p. 41.
[58] Véase CONTRALORÍA GENERAL DE LA REPÚBLICA, Dictamen N° 26.479 de 20 de agosto de 1996.
[59] Véase ENISA, 'Cloud Computing. Benefits, risks and recommendations for information security', *Op. Cit.*, p. 14 y CIO COUNCIL & CHIEF ACQUISITIONS OFFICERS COUNCIL, 'Creating Effective Cloud

En este sentido, en caso de que sea materialmente posible, se estima recomendable establecer cláusulas de esta naturaleza en el contrato de prestación de servicios a fin de que el contratante esté en condiciones de efectuar dichas auditorías. Es deber de los órganos del Estado de cuidar la información que ellos tienen. Un nivel de diligencia debido en este tipo de materias exige, como paso razonable, el efectuar dicha clase de auditorías de forma permanente.

Ahora, en caso de que auditar no sea posible por razones logísticas u otras causas (por ejemplo, que el órgano contratante no tenga el capital humano necesario como para poder efectuar esta clase de auditorías), se recomienda ver la posibilidad de contratar terceros de confianza que puedan hacer dicha auditoría o verificar si acaso estos prestadores cuentan con certificaciones de parte de terceros que gocen de dicha independencia (por ejemplo, el cumplimiento de la normativa técnica de la familia ISO 27.000).

Cualquier decisión en este sentido debiera ser adoptada junto con el oficial de seguridad de la información que se desempeñe dentro del órgano contratante.

8. 'Vendor lock-in'

La noción *"vendor lock-in"* alude al hecho de que una vez que el cliente comienza a utilizar una determinada tecnología, éste se encuentra, en los hechos, en una situación de dependencia de su proveedor ya que el usuario se encuentra impedido de cambiarse a un nuevo prestador de servicios dado que los costos de cambio (*"switching costs"*) son tan altos que el cliente no tiene otra opción más que quedarse con los servicios de su actual proveedor. Esto en muchas ocasiones ocurre cuando se utilizan formatos y protocolos informáticos que sólo pueden ser utilizados con el prestador del servicio *cloud*.

Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service', *Op. Cit.*, p. 16 y p. 23.

Lo anterior suele ser un fenómeno bastante común en el mundo de las tecnologías[60]. Los servicios de *cloud computing* no son la excepción máxime si se considera que los protocolos, estándares y herramientas tienden a ser dispares en los servicios *cloud*, lo que es consecuencia de la reciente masificación de estos servicios[61].

En consecuencia, al momento de analizar los contratos y términos y condiciones **es muy importante** revisar la posibilidad de que el órgano pueda recuperar y descargar los datos que tienen en la nube y pueda, sin mayores costos, el migrar su información a un nuevo proveedor. En este sentido, el/los abogado/s encargado/s del análisis debe/n pedir siempre la asistencia técnica de sus departamentos informáticos a fin de analizar la respuesta que le entregue el oferente.

En caso de que exista una situación de '*vendor lock-in'* el servicio debe analizar los riesgos asociados a mantenerse en una situación de cautividad con dicho prestador y contrastarlo con las ventajas asociadas al servicio. **Se sugiere, no obstante, preferir siempre los servicios *cloud* que permitan a los servicios mantener la libertad de cambiarse de proveedor de conformidad a las necesidades que vaya teniendo el servicio a futuro.**

En este sentido, hacemos nuestros las recomendaciones de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA):

---

[60] Véase ARTHUR, W. Brian, 'Competing Technologies, Increasing Returns, and Lock-In by Historical Events', *The Economic Journal*, Vol. 99, No. 394. (Mar., 1989), pp. 116-131. Disponible en línea en: <http://bit.ly/UEa4Nc> [Visitado: 9 de marzo de 2012].

[61] Véase MCKENDRICK, Joe, 'Cloud Computing's Vendor Lock-In Problem: Why the Industry is Taking a Step Backward', *Forbes*, 20 de diciembre de 2011. Disponible en línea en: <http://onforb.es/YLPlda> [Visitado: 9 de marzo de 2012].

Por favor notar además que, a nivel de autoridades del mundo desarrollado, existe conciencia de que este es un desafío a enfrentar en materia de cloud computing. Véase EUROPA PRESS RELEASE, 'Neelie Kroes Vice-President of the European Commission responsible for the Digital Agenda Setting up the European Cloud Partnership World Economic Forum Davos, Switzerland', 26th January 2012, SPEECH/12/38. Disponible en línea en: <http://bit.ly/YwvdNe> [Visitado: 9 de marzo de 2012].

"Una solución de la nube debe ser interoperable, permitiendo a los gobiernos y las administraciones públicas migrar a los servicios en la nube de un proveedor de servicios en la nube a otro sin restricciones técnicas o contractuales o costes de cambio sustanciales […]

Es muy importante que los gobiernos y las administraciones públicas eviten cualquier forma de "cautividad del mercado" [(vendor lock-in)]*, ya que cualquier falta de disponibilidad (temporal) y/o ineficiencia de los servicios puede dar lugar a importantes responsabilidades para los gobiernos y las administraciones públicas..."*[62]

9. Terminación del contrato y eliminación de los datos en los sistemas del prestador del Servicio

Es importante que los órganos de la Administración del Estado mantengan la libertad de poner término a esta clase de contratos. En ese sentido, se sugiere la contratación de los servicios por términos que no sean excesivamente prolongados en el tiempo para que así se pueda revisar de forma constante la calidad con que el prestador está cumpliendo sus obligaciones contractuales.

Esta libertad, desde luego, permite al órgano contratante el poder cambiarse a otros proveedores en caso de que sea necesario. Esto constituye, además, un incentivo para que el prestador del servicio tome medidas adicionales para mantener a su cliente.

Por otra parte, se estima importante reiterar que es importante que quede claramente establecido que, una vez terminada la relación contractual, el prestador del servicio *cloud* tenga la obligación de eliminar, de forma irreversible, los datos que fueron subidos a la nube y mantener su obligación de confidencialidad de forma indefinida. La cláusula sobre "Confidencialidad y Protección de Datos" consignada

[62] ENISA, 'Seguridad y resistencia en las nubes de la Administración Pública…', *Op. Cit.*, p. 45.

en el Anexo de este documento contiene una estipulación en este sentido. Nos remitimos a ella para que pueda ser empleada como modelo.

10. Responsabilidad del proveedor del Servicio *Cloud*

Un tema bastante importante en materia de contratación de esta clase servicios, lo constituye el tema de la responsabilidad civil en que incurre el prestador del servicio. Tal como lo señala la ENISA:

> *"Al migrar a los servicios en la nube, los gobiernos y las administraciones públicas pasan a depender mucho de la adecuación del desempeño del proveedor de servicios en la nube. Lo más probable es que los fallos o deficiencias del proveedor de servicios en la nube en la prestación de los servicios tengan un impacto muy negativo sobre los servicios que ofrecen los gobiernos y las administraciones públicas a los ciudadanos. Esto se puede traducir no solo en pérdidas económicas para los gobiernos y las administraciones públicas, sino también en daños a su imagen (por tanto, daño político). Las cláusulas de responsabilidad e indemnización en los acuerdos de nivel de servicio (ANS) van a desempeñar un papel fundamental en este tema. Los ANS detallados, en los que se especifican detalladamente los niveles de funcionamiento del proveedor de servicios en la nube, junto con las cláusulas contractuales que asignan claramente, por un lado, los derechos y deberes generales de las partes y, por el otro, las obligaciones y responsabilidades, serán intereses cruciales de gobiernos y administraciones públicas."*[63]

Pues bien, en este orden de cosas, los órganos deben poner especial atención a este aspecto al momento de contratar con los prestadores de servicios *cloud*. En este sentido, cabe notar que una práctica ampliamente extendida en los contratos de prestación de servicios tecnológicos es la limitación (o derechamente la exone-

[63] AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN (ENISA), 'Seguridad y resistencia en las nubes de la Administración Pública. Informe para la toma de decisiones', Enero de 2011, pp. 45-46. Disponible en línea en: <http://bit.ly/Sitjte> [Visitado: 8 de mayo de 2013]

ración) de la responsabilidad civil al momento de incumplir con sus obligaciones, ya sea por la pérdida de la información del usuario que se contenga en sus servicios o por el incumplimiento de alguna disposición contractual.

Esta Unidad sugiere descartar de plano a aquellos prestadores de servicios que impongan clausulas de exoneración de responsabilidad por incumplimiento o en caso que las limitaciones de responsabilidad civil sean tan amplias que implique una renuncia anticipada de derechos por parte de los órganos de la Administración del Estado[64].

En este sentido, cabe destacar que de conformidad a la jurisprudencia administrativa de Contraloría General de la República, los órganos de la Administración del Estado **no** pueden acceder a esta clase de limitaciones de responsabilidad, toda vez que ella configura una renuncia anticipada del organismo público a los derechos que le corresponde ejercer en caso de producirse perjuicios imputables al prestador de servicios[6566].

Por otra parte, sin perjuicio de la responsabilidad civil que le es exigible al prestador del servicio en virtud del contrato, el órgano contratante debe tomar todas las prevenciones necesarias para acotar lo máximo posible los daños que se puedan producir como consecuencia algún incidente que afecte al proveedor. Como mínimo, el órgano contratante debiera:

[64] Para estos efectos, se pone a disposición en el anexo de este documento de una cláusula modelo sobre responsabilidad civil que podrían voluntariamente emplear los órganos de la Administración del Estado en este tipo de contratos.

[65] CONTRALORÍA GENERAL DE LA REPÚBLICA, Dictámenes N°s 46.564, de 22 de julio 2011; y 67.520, de 12 de noviembre de 2010.

[66] Esto, por lo demás, se encuentra en consonancia con las políticas gubernamentales de otros países en este tipo de materias. En efecto, por regla general, las agencias estadounidenses y europeas suelen ser bastante exigentes en torno al tema de la limitación de responsabilidad. Véase CIO COUNCIL & CHIEF ACQUISITIONS OFFICERS COUNCIL, 'Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service', *Op. Cit.*, p. 14 y p. 23 y AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN (ENISA), 'Seguridad y resistencia en las nubes de la Administración Pública. Informe para la toma de decisiones', *Op. Cit*.

(a) **Contratar por separado un servicio de respaldo o *backup* de la información que sea alojada en las infraestructuras de la nube.** De preferencia, este respaldo debiera ser suministrado por un tercero distinto al prestador del servicio *cloud*. Ahora, en caso de contratarse con el mismo proveedor del servicio cloud el respaldo, el almacenamiento de tales datos debiera hacerse en dependencias distintas a las donde se aloja la nube.

(b) **Encriptar la información que es subida a la nube** a fin de que, en caso de que se filtre la información, no sea fácilmente visible a ojos de terceros. Como sea, cabe notar que esta última medida no impide que un grupo limitado organizaciones que cuentan con la tecnología y presupuesto suficiente como para poder desencriptar dicha información puedan, igualmente, acceder a ella.

11. Sanciones por incumplimiento del contrato

Sin perjuicio de la responsabilidad civil del Prestador del Servicio el órgano contratante debiera asegurarse de que existan cláusulas que:

(a) Penalicen con multas a los prestadores del servicio en caso de incumplir sus obligaciones.

En este sentido, hacemos nuestros los comentarios de la ENISA al efecto:

> *"*[Las Administraciones Públicas] *deberían pedir a los proveedores de servicios en la nube que estén atentos para evitar errores, y asegurar este punto a través de cláusulas contractuales* ***que establezcan sanciones importantes*** *en caso de deficiencias en los*

servicios del proveedor de servicios en la nube."[67] (Énfasis añadido)

(b) Permitan al órgano administrativo contratante resolver de inmediato el contrato en caso de que exista algún incumplimiento. Dicha resolución del contrato no debiera dar derecho a indemnización para el prestador del servicio.

(c) Se establezcan garantías para el fiel y oportuno cumplimiento de los contratos que sean de una entidad proporcional a los montos del contrato y de los eventuales daños que se podría provocar en virtud de un incumplimiento contractual.

(d) Además, en todo caso, debiera informarse en el contrato acerca de que el incumplimiento contractual será informado a la Dirección ChileCompra a fin de que ésta estudie su eliminación del Registro de Proveedores[68] y al resto de los órganos que actualmente son clientes del prestador del servicio *cloud* a fin de que estos tomen las medidas que estimen pertinentes.

En este sentido, particular énfasis debe colocarse al incumplimiento de las obligaciones de continuidad del servicio, confidencialidad, protección de datos, seguridad de la información y propiedad intelectual.

12. Subcontratación, cambios de control y cesión del contrato

A diferencia de otros servicios tecnológicos, el consumo de servicios *cloud* pone en una situación de especial dependencia al órgano de la administración del Estado. En ese orden de cosas, no es de sorprender que esta clase de servicios sean

[67] AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN (ENISA), 'Seguridad y resistencia en las nubes de la Administración Pública. Informe para la toma de decisiones', *Op. Cit.*, p. 46.

[68] Ello de conformidad a lo dispuesto en el Decreto N° 250, del Ministerio de Hacienda, Aprueba reglamento de Ley N° 19.886 de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios. D.O. 24 de septiembre de 2004.

tomados en razón de la persona a quien se contrata. No se trata, pues, de un servicio fácilmente intercambiable.

Atendida la especial característica de esta clase de provisión de servicios es que debe ponerse atención al hecho de si el oferente, a su vez, subcontrata los servicios de terceras personas.

Si el órgano contratante decide admitir la subcontratación, éste debe preguntar explícitamente al oferente de si acaso se subcontratan servicios y, en caso de una respuesta afirmativa, qué estándares de seguridad siguen.

Si existe una subcontratación, el órgano debe asegurarse que dicho subcontratista cumpla con las expectativas de seguridad y confianza que se requieren del prestador del servicio. Asimismo, el prestador del servicio debiera hacerse responsable civilmente por cualquier daño producido por el subcontratista el que, además, debiera cumplir con los mismos estándares de seguridad y confidencialidad que se ha acordado con el prestador del servicio.

Adicionalmente, cabe destacar que de conformidad al artículo 15 de la Ley N° 19.886 y el artículo 76 de su reglamento, los órganos contratantes pueden admitir esta subcontratación pero esta siempre debe ser parcial[69]. En tal caso, las respectivas bases y el contrato deben explicitar qué parte o categoría de servicios serán

[69] En el contexto del Convenio Marco de Data Center y Servicios Asociados, cabe notar que se permite la subcontratación parcial de servicios, sin perjuicio que la responsabilidad deberá permanecer en el adjudicatario. En todo caso, los montos subcontratados no pueden exceder del 40% del monto total estimado del contrato. Consecuentemente, si se contrata un servicio cloud bajo esta modalidad, se deberá verificar qué parte del servicio se tiene subcontratado. Asimismo, en tal caso se recomienda tener a la vista el contrato entre el adjudicatario y el subcontratista a fin de tomar una decisión lo más informada posible.

los que se podrán subcontratar[70] y se debe considerar que tales subcontratistas se encuentran afectos a los requisitos de la Ley Nº 19.886[71]. Asimismo, cuando se contrata al proveedor *cloud*, los departamentos jurídicos debieran considerar en las respectivas bases de licitación, contrato y/o acuerdo complementario, la prohibición por parte del adjudicatario de sub-contratar ciertos aspectos esenciales o sensibles del servicio licitado.

Todo lo anterior debiera quedar debidamente regulado en las bases de licitación y en contratos que se suscriben con el prestador del servicio.

Otro tema dice relación con el control / nacionalidad del prestador del servicio. Así, en un caso particular, puede ser una consideración estratégica del contratante que el prestador del servicio se encuentre controlado por persona que revista ciertas características especiales. En tal caso, debiera regularse contractualmente la posibilidad de que el prestador del servicio notifique estos cambios al órgano contratante para que este revise la continuidad del servicio.

En este sentido, hacemos nuestro las recomendaciones de la ENISA:

> *"Dada la relación altamente dependiente, es probable que los gobiernos y las administraciones públicas seleccionen cuidadosamente los proveedores de servicios en la nube. Se deben evitar las situaciones en las que un proveedor de servicios en la nube subcontrate los servicios pertinentes a un tercero o, al menos, se deben incluir en el acuerdo de servicio declaraciones y garantías sobre posibles subcontratistas. Del mismo modo, el proveedor de servicios en la nube debe notificar sin demora los cambios de control al gobierno o administraciones públicas,*

[70] Véase CONTRALORÍA GENERAL DE LA REPÚBLICA, Dictámenes N° 72.839 del 3 de diciembre de 2012, N° 34.982 de 28 de agosto de 2008.
[71] Véase, para el caso de las inhabilidades, CONTRALORÍA GENERAL DE LA REPÚBLICA, Dictamen N° 15.925 de 10 de abril de 2008.

que es posible que desee negociar el derecho de rescindir el contrato en caso que ocurra tal evento."[72]

Finalmente, conviene notar que es importante dejar claramente sentado en las bases o contratos que, por disposición de los artículos 14 de la Ley N° 19.886 y 74 de su reglamento, se prohíbe que el prestador del servicio *cloud* pueda ceder total o parcialmente los derechos y obligaciones del contrato.

13. Derecho aplicable y resolución de disputas

Una cuestión bastante usual que se puede encontrar en los contratos de servicios *cloud* es el establecimiento de una cláusula que establece que los servicios contratados se rigen por la normativa de otro país y que, en caso de conflicto, las disputas que puedan ocurrir entre el prestador del servicio y el cliente debe someterse a la jurisdicción de un tribunal que, generalmente, suele ser la que corresponde al lugar en donde se ubican los cuarteles generales del proveedor *cloud*[73]. Así, por ejemplo, si el proveedor es del Reino Unido, muy probablemente sugerirá la aplicación de las leyes de un determinado Estado y el sometimiento de sus conflictos ante dichos tribunales.

Por regla general, los órganos de la Administración del Estado **no tienen potestades públicas para someterse a las leyes y jurisdicciones extranjeras**[74]. Luego, no pueden contratar servicios que establezcan cláusulas de esta naturaleza.

[72] ENISA, 'Seguridad y resistencia en las nubes de la Administración Pública…', *Op. Cit.*, p. 45.
[73] En este mismo sentido, véase BRADSHAW, MILLARD y WALDEN, 'Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services', *Op. Cit.*, p. 17.
[74] En este sentido, véase CONTRALORÍA GENERAL DE LA REPÚBLICA, dictamen N° 32.447 de 11 de diciembre 1987 sobre la materia.

Por lo mismo, tanto en las licitaciones como en los contratos se debe establecer expresamente que cualquier disputa entre las partes **se someten a las leyes y tribunales chilenos**[75].

Adicionalmente, al momento de contratar esta clase de servicios se sugiere efectuar una solicitud a los proveedores de declaraciones juradas en las que señalen que todos los servicios que se presten, se someterán a la legislación chilena (fundamentalmente: la Ley N° 19.628, Sobre Protección de la Vida Privada o Protección de Datos de Carácter Personal; Ley N° 17.336, sobre Propiedad Intelectual; Ley N° 20.285, sobre Acceso a la Información Pública y Ley N° 19.223, que Tipifica Figuras Penales Relativas a la Informática, entre otras).

IV. CONCLUSIONES

Como el lector lo podrá advertir, la contratación de esta clase de servicios varía radicalmente dependiendo del caso particular: qué tipo de información se sube a la nube, qué tipo de nube se trata (privada o pública), qué prestador de servicio estamos contratando, qué órgano de la administración es el que contrata y una larga lista de factores adicionales determinan cuáles son los énfasis que se deben colocar al momento de contratar.

Asimismo, como lo puede notar el lector, estas contrataciones revisten una complejidad que requieren de un trabajo multidisciplinario al interior del órgano de la Administración del Estado.

[75] En el anexo se puede encontrar un modelo de cláusula a emplear por los órganos de la Administración del Estado.

En este sentido, se recomienda tener presente la serie de variables legales que se han indicado en el presente documento a fin de adoptar una decisión de contratación en esta clase de servicios.

Como sea, siempre que sea posible contratar un servicio de esta naturaleza, esta Unidad recomienda la adopción de esta clase de tecnologías puesto que se traducen en una mejora significativa de la eficiencia con la que el Estado puede prestar servicios a las personas.

--- o ---

ANEXO: CLÁUSULAS A EMPLEAR EN LOS CONTRATOS CLOUD

Sin perjuicio de que los órganos de la Administración del Estado son completamente libres de determinar las modalidades y cláusulas propias de la contratación de servicios cloud, el presente Anexo entrega una serie de cláusulas que podrían ser empleadas y modificadas por ellos al momento de contratar un servicio de esta naturaleza.

1. Confidencialidad y protección de datos.

Para los efectos de la presente cláusula, "Información Confidencial" constituye toda información, sea completa o parcial, sea verbal o escrita, independiente del medio en que conste o se transmita, que el [Prestador del Servicio Cloud] *recibe desde el* [órgano contratante] *u otros entes públicos en virtud del presente contrato o que el* [Prestador del Servicio Cloud] *tome conocimiento por cualquier medio y ya sea que se refiera al* [órgano contratante]*, otros órganos públicos, sus autoridades, funcionarios, contratistas u otras personas.*

La Información Confidencial del [órgano contratante] *será mantenida en estricta reserva por el* [Prestador del Servicio Cloud]*, quien deberá mantener la debida confidencialidad de los datos, bases de datos, documentos y a todos los archivos informáticos a que tenga acceso con motivo del presente contrato, quedándole expresamente prohibido divulgarlos, publicarlos, fotocopiarlos, copiarlos o distribuirlos a terceros extraños a este contrato o hacer cualquier uso indebido de ellos. Estas informaciones y datos sólo podrán ser revelados por instrucción del* [órgano contratante].

El [Prestador del Servicio Cloud] *guardará especial atención a la confidencialidad de los datos personales a que pueda tener acceso en virtud del presente contrato. En este sentido, el* [Prestador del Servicio Cloud] *no podrá recolectar, almacenar, transferir, transmitir, comunicar, tratar,*

ceder o usar, de cualquier forma, los datos indicados anteriormente, salvo que dichas acciones sean indispensables para el cumplimiento de las obligaciones consignadas en el presente contrato y/o que medie una autorización escrita por parte del representante legal del [órgano contratante]. *En ningún caso se entenderá que el* [Prestador del Servicio Cloud] *tiene algún derecho sobre tales datos personales.*

El [Prestador del Servicio Cloud] *adoptará todas las medidas conducentes a resguardar la confidencialidad de la información por parte de su personal, incluyendo profesionales, consultores, contratistas o demás personas que deban tomar, hayan tomado o tengan conocimiento de la Información Confidencial del* [órgano contratante].

Los consultores y personal dependiente del [Prestador del Servicio Cloud], *que de una u otra manera se hayan vinculado a la ejecución de los servicios contratados, en cualquiera de sus etapas, deberán guardar confidencialidad de la misma forma aplicable al* [Prestador del Servicio Cloud]. *La responsabilidad del* [Prestador del Servicio Cloud] *en este ámbito, será solidaria respecto de la de sus administradores, representantes, personeros, empleados, consultores y todo aquel que se encuentre vinculado a la ejecución de los servicios contratados*

La divulgación, por cualquier medio, de la totalidad o parte de la información referida en los párrafos anteriores, por parte del [Prestador del Servicio Cloud], *durante la vigencia del contrato o una vez finalizado éste, podrá dar pie a que la* [órgano contratante] *entable en su contra las acciones judiciales que correspondan, sin perjuicio de la responsabilidad solidaria por los actos en infracción de esta obligación que hayan ejecutado sus empleados. Asimismo, lo anterior facultará al* [órgano contratante] *a informar a otros órganos públicos que tuvieren contratados servicios con el* [Prestador del Servicio Cloud] *acerca de este incumplimiento.*

Toda la Información Confidencial (incluyendo las copias tangibles y la almacenada por medios electrónicos y/o cualquier otro medio) propor-

cionada por el [órgano contratante] *será devuelta a éste dentro de los 30 días corridos contados desde la recepción de un requerimiento escrito por el* [órgano contratante]*. Para dichos efectos, el* [Prestador del Servicio Cloud] *entregará al* [órgano contratante] *todos los materiales que contengan o representen la Información Confidencial recibida. Hecho lo anterior, el* [Prestador del Servicio Cloud] *no podrá mantener ninguna Información Confidencial del* [órgano *contratante] en su poder, debiendo eliminar de forma irreversible cualquier copia de dicha información que disponga en sus registros lógicos y físicos.*

2. Seguridad de la información.

"El [Prestador del Servicio Cloud] *deberá adoptar todas las medidas técnicas y organizativas de seguridad que sean precisas para efectos de evitar que la información del* [órgano contratante] *sea accedida por terceros no autorizados.*

Lo anterior se extiende, además, a las comunicaciones electrónicas de dicha información entre [Prestador del Servicio Cloud] *y el* [órgano contratante]*. En tal caso, el* [Prestador del Servicio Cloud] *deberá emplear las medidas seguridad que sean necesarias para que estas comunicaciones no sean interceptadas.*

Para lo anterior, seguirá los estándares de seguridad establecidos en las normas técnicas contenidas en la serie 27000 co-publicada conjuntamente por la International Organization for Standardization (ISO) y la International Electrotechnical Commission (IEC).

Asimismo, para efectos de claridad, se deja expresa constancia que [Prestador del Servicio Cloud] *deberá adoptar las medidas de respaldo de la información que impidan que ésta se pierda como consecuencia de alguna contingencia que afecte sus sistemas informáticos."*

3. Responsabilidad Civil.

La responsabilidad civil de las partes derivadas de algún incumplimiento o cumplimiento parcial de las obligaciones establecidas en el presente contrato se regirá por las leyes de la República de Chile.

En ningún caso se entenderá que el [órgano contratante] *acepta o admite alguna limitación convencional de responsabilidad por parte del* [Prestador del Servicio Cloud].

Finalmente, el [Prestador del Servicio Cloud] *será responsable de (1) cumplir con todas las leyes, reglamentaciones, ordenanzas y disposiciones gubernamentales vigentes que le fueren aplicables en la República de Chile y (2) de respetar los derechos de propiedad intelectual de terceras personas en la ejecución de las obligaciones establecidas en el presente instrumento.*

El [Prestador del Servicio Cloud] *defenderá, indemnizará y mantendrán a salvo al* [órgano contratante] *de y en contra de cualquier reclamación, acción, demanda, y procedimiento legal (conjuntamente "Reclamo(s)") y de toda responsabilidad, daño, pérdida, juicio, declaración autorizada, costos y gastos directos e indirectos (en adelante "Daños") que surjan de o en relación con la violación de lo establecido en el presente contrato.*

4. Propiedad Intelectual.

Toda la información, datos, documentos y bases de datos que el [Prestador del Servicio Cloud] *recibe desde el* [órgano contratante] *o que el* [Prestador del Servicio Cloud] *toma conocimiento por cualquier medio en virtud de la presente licitación serán de propiedad del* [órgano contratante] *y sólo podrá ser utilizado por el* [Prestador del Servicio Cloud] *para efectos de la ejecución de las obligaciones emanadas en virtud de la presente licitación y su respectivo contrato. Cualquier otro uso estará prohibido salvo que el* [Prestador del Servicio Cloud] *cuente con la autorización escrita del* [órgano contratante].

Todos los informes, especificaciones, estudios técnicos, y, en general, todos los documentos que el [Prestador del Servicio Cloud] *elabore en virtud del presente contrato, serán de propiedad exclusiva del* [órgano contratante].

El [Prestador del Servicio Cloud] *defenderá, indemnizará y mantendrá a salvo al* [órgano contratante] *y a sus funcionarios de y en contra de cualquier reclamación, acción, demanda, y procedimiento legal y de toda responsabilidad, daño, pérdida, juicio, declaración autorizada, costos y gastos directos e indirectos incluyendo, sin limitación, los honorarios razonables de los abogados, que surjan de o en relación con cualquier violación y/o usurpación efectuada por el* [Prestador del Servicio Cloud] *de cualquier derecho de autor, patente, marca registrada, secreto industrial u otro derecho propietario o de propiedad intelectual de cualquier tercero.*

5. Vendor lock-in

Los estándares empleados por los servicios contratados en virtud de la presente licitación deberán permitir que el [órgano contratante] *pueda recuperar y descargar los datos que se encuentran en las dependencias o sistemas del* [Prestador del Servicio Cloud] *o sus subcontratistas. Ello con miras a que el* [órgano contratante] *pueda, sin mayores costos, migrar su información a un nuevo proveedor una vez terminado el contrato objeto de la presente licitación.*

6. Fuerza mayor o caso fortuito.

Si se presentase una situación de fuerza mayor o caso fortuito en los términos que se encuentra definido por el artículo 45 del Código Civil, el [Prestador del Servicio Cloud] *deberá notificar al* [órgano contratante] *inmediatamente y por escrito de dicha situación y sus causas, quedando excusada de cumplir las obligaciones que emanen del presente Contrato, desde el momento de la ocurrencia de la fuerza mayor o caso fortuito hasta la desaparición de la misma.*

Si la situación de fuerza mayor o caso fortuito, se prolongase mas allá de lo razonable o previsible, según la naturaleza del bien o servicio comprendido en el Contrato, o fuere evidente que éste ya no podrá cumplirse, el [órgano contratante] *estará facultado para resolver el Contrato, conforme las normas de la legislación vigente.*

Sin perjuicio de lo anterior, en ningún caso se considerará caso fortuito o causal de fuerza mayor lo siguiente:

(a) El embargo de los bienes del [Prestador del Servicio Cloud].

(b) Las acciones que pueda ordenar la autoridad que impidan al [Prestador del Servicio Cloud] *desarrollar su labor por no cumplir con las disposiciones legales o reglamentarias que le correspondan.*

(c) La huelga de los trabajadores del [Prestador del Servicio Cloud] *o de alguno de sus contratistas o subcontratistas.*

7. Facultad del órgano de comunicar el incumplimiento del prestador del servicio a otros órganos públicos.

En caso de incumplimiento total o parcial del presente contrato por parte del [Prestador del Servicio Cloud], *el* [órgano contratante] *podrá comunicar de esta circunstancia a los demás órganos de la Administración del Estado que hayan contratado a éste. Asimismo, el* [órgano contratante] *será libre de comunicar a los demás órganos de la Administración del Estado su opinión acerca de la calidad de los servicios prestados en virtud del presente contrato.*

Lo anterior es sin perjuicio de las cláusulas del presente instrumento que se refieran la resolución del contrato, multas, responsabilidad civil y demás que fueren procedentes.

8. Legislación aplicable y resolución de controversias.

El presente Contrato se rige por las leyes y normas jurídicas de la República de Chile.

Ante cualquier dificultad que se suscite entre las partes de este contrato respecto de la existencia, validez, exigibilidad, resolución, término, interpretación, aplicación, cumplimiento o suscripción del mismo o por cualquier otra razón relacionada con este contrato, las Partes se someterán a la jurisdicción y competencia de los tribunales ordinarios de justicia de la ciudad y comuna de Santiago.

9. Procedimiento para hacer efectiva la terminación y medidas para mantener la continuidad del servicio.

La terminación del Contrato se efectuará por vía administrativa, sin necesidad de pronunciamiento judicial, cuando el Ministerio considerare que se cumple con las causales que se establecen en el acápite [indicar cláusulas donde se establecen las causales de terminación].

La terminación del Contrato será notificada por carta certificada dirigida al domicilio indicado por el Contratista en el Contrato y se entenderá practicada a contar del tercer día hábil siguiente a su ingreso para despacho en oficina de correos.

La resolución que declara la terminación del Contrato deberá invocar la causal de terminación que se emplea, sus fundamentos, el alcance de la terminación y la fecha a contar de la cual ésta entrará en vigor.

Una vez notificado, el Contratista dispondrá de un plazo de cinco días hábiles a contar de la fecha de la comunicación para formular descargos respecto de la resolución que declara la terminación del Contrato. Para lo anterior, el Contratista podrá acompañar todos los antecedentes que estime pertinentes.

Transcurrido este plazo, y recibido los descargos, el Ministerio resolverá sobre el particular mediante resolución o resoluciones fundadas, previa ponderación de los antecedentes, remitiéndose copia del acto administrativo al Contratista.

Si transcurrido el plazo, y no habiéndose recibido descargos, o habiéndose recibido descargos, y el Ministerio los hubiere rechazado, la resolución que declara la terminación del Contrato quedará a firme.

Una vez ocurrido lo anterior, el Contratista deberá entregar al Ministerio la información utilizada en la prestación de los servicios hasta ese momento, de modo de habilitar cualquier solución que este defina.

Durante el periodo que media entre la notificación de la terminación y la fecha en que se ésta se hará efectiva, el Contratista deberá prestar, a su costa, toda la colaboración que el Ministerio le requiera para que este último pueda traspasar a otro proveedor la operación del servicio de manera tal que se mantenga la continuidad del mismo en todo momento.

Adicionalmente, se podrán aplicar todas las medidas tendientes a mantener la continuidad de servicio que deba efectuar el Ministerio, por cuenta, costo y riesgo del Contratista, previa notificación al mismo. Para estos efectos, a modo ejemplar, se entenderán como medidas correctivas, el tener que recurrir para la ejecución de las obligaciones contractuales del Contratista a la contratación de terceros o a funcionarios del Ministerio

REFERENCIAS

I. Normativa consultada

1. Decreto con Fuerza de Ley Nº 100 del Ministerio Secretaría General de la Presidencia, Fija el texto refundido, coordinado y sistematizado de la Constitución Política de la República de Chile, D.O. 22 de septiembre de 2005.

2. Ley N° 19.223, que Tipifica Figuras Penales Relativas a la Informática. D.O. 7 de junio de 1993.

3. Ley N° 19.628, Sobre Protección de la Vida Privada. D.O. 28 de agosto 1999.

4. Ley N° 17.336, sobre Propiedad Intelectual. D.O. 02 de octubre de 1970.

5. Ley N° 19.886 de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios. D.O. 30 de julio de 2003.

6. Ley N° 20.285, sobre acceso a la Información Pública. D.O. 20 de agosto de 2008.

7. Decreto con Fuerza de Ley Nº 1 del Ministerio Secretaría General de la Presidencia, fija el texto refundido, coordinado y sistematizado de la Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, D.O. 17 de noviembre de 2001.

8. Decreto N° 250, del Ministerio de Hacienda, Aprueba reglamento de Ley N° 19.886 de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios. D.O. 24 de septiembre de 2004.

9. Decreto N° 14, del Ministerio de Economía, Fomento y Turismo, Modifica Decreto nº 181, de 2002, que aprueba Reglamento de la ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, y deroga los decretos que indica, D.O. 27.02.2014.

10. Decreto N° 83, del Ministerio Secretaría General de la Presidencia, Aprueba norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos, D.O. 12.01.2005.

11. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act 2001, Title V, s. 505.

12. Regulation of Investigatory Powers Act 2000, Part II, s. 28.

II. Bibliografía

1. 'Data privacy: Out of shape. The rules on what data governments can demand from communications companies need tightening', *The Economist*, 21 de julio de 2012. Disponible en línea en: <http://www.economist.com/node/21559345> [visitado: 29 de diciembre de 2012]

2. 'Surveillance: Look who's listening' *The Economist*, 15 de junio de 2013. Disponible en línea en: <http://www.economist.com/node/21579473> [visitado: 1 de julio de 2013].

3. **ARTHUR**, W. Brian, 'Competing Technologies, Increasing Returns, and Lock-In by Historical Events´, *The Economic Journal*, Vol. 99, No. 394. (Mar., 1989), pp. 116-131. Disponible en línea en: <http://bit.ly/UEa4Nc> [Visitado: 9 de marzo de 2012].

4. **BRADSHAW**, Simon, **MILLARD**, Christopher & **WALDEN**, Ian, 'Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services', *Legal Studies Research Paper No. 63/2010*, Queen Mary University of London, School of Law, año 2010. Disponible en línea en: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1662374> [Visitado: 4 de diciembre de 2012].

5. **EUROPA PRESS RELEASE**, 'Neelie Kroes Vice-President of the European Commission responsible for the Digital Agenda Setting up the European Cloud Partnership World Economic Forum Davos, Switzerland', 26th January 2012, SPEECH/12/38. Disponible en línea en: <http://bit.ly/YwvdNe> [Visitado: 9 de marzo de 2012].

6. **HON**, Kuan, **MILLARD**, Christopher & **WALDEN**, Ian, 'Negotiating Cloud Contracts - Looking at Clouds from Both Sides Now'*, Legal Studies Research Paper No 117/2012*, Queen Mary University of London, School of Law, año 2012. Disponible en línea en: <http://ssrn.com/abstract=2055199> [Visitado: 4 de diciembre de 2012].

7. **HON**, Kuan, **MILLARD**, Christopher & **WALDEN**, Ian, 'UK G-Cloud v1 and the impact on cloud contracts', *Legal Studies Research Paper No 115/2012*, Queen Mary University of London, School of Law. Disponible en línea en: <http://ssrn.com/abstract=2038557> [Visitado: 4 de diciembre de 2012].

8. **MCKENDRICK**, Joe, 'Cloud Computing's Vendor Lock-In Problem: Why the Industry is Taking a Step Backward', *Forbes*, 20 de diciembre de 2011. Disponible en línea en: <http://onforb.es/YLPlda> [Visitado: 9 de marzo de 2012].

9. **MILLER**, Claire, 'Tech Companies Concede to Surveillance Program' *The New York Times*, 7 de junio de 2013. Disponible en línea en: <http://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html?pagewanted=all> [visitado: 1 de julio de 2013]

10. **MOWBRAY**, Miranda, 'The Fog over the Grimpen Mire: Cloud Computing and the Law', *SCRIPTed*, Vol. 6, Issue 1, Abril de 2009, pp. 132-146. Disponible en línea en: <http://www.law.ed.ac.uk/ahrc/script-ed/vol6-1/mowbray.asp> [Visitado: 4 de diciembre de 2012].

11. **SAVAGE**, Charlie, 'Democratic Senators Issue Strong Warning About Use of the Patriot Act', *The New York Times*, 16 de marzo de 2012. Disponible en línea en: <http://www.nytimes.com/2012/03/16/us/politics/democratic-senators-warn-about-use-of-patriot-act.html?_r=0> [visitado: 29 de diciembre de 2012].

12. **SAVAGE**, Charlie, **WYATT**, Edward and **BAKER**, Peter, 'U.S. Confirms That It Gathers Online Data Overseas' *The New York Times*, 6 de junio de 2013. Disponible en línea en: <http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html?pagewanted=all&_r=0> [visitado: 1 de julio de 2013].

II. Guías e informes gubernamentales

§ Estados Unidos de América

1. **OFFICE OF MANAGEMENT AND BUDGET, U.S. CHIEF INFORMATION OFFICER**, 'Federal Cloud Computing Strategy', 8 de febrero de 2011. Disponible en línea en: <http://1.usa.gov/WG44Wp> [Visitado: 8 de mayo de 2013].

2. **CIO COUNCIL & CHIEF ACQUISITIONS OFFICERS COUNCIL**, 'Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service', 24 de febrero de 2012. Disponible en línea en: <http://1.usa.gov/QztYcN> [Visitado: 8 de mayo de 2013].

3. **NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE**, 'The NIST Definition of Cloud Computing', NIST Special Publication 800-145, Septiembre de 2011. Disponible en línea en: <http://1.usa.gov/10GjEQZ> [Visitado: 8 de mayo de 2013].

4. **NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE**, 'US Government Cloud Computing Technology Roadmap, Release 1.0 (Draft), Volume I High-Priority Requirements to Further USG Agency Cloud Computing Adoption', NIST Special Publication 500-293, Noviembre de 2011. Disponible en línea en: <http://1.usa.gov/UiFmZG> [Visitado: 8 de mayo de 2013].

5. **NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE**, 'US Government Cloud Computing Technology Roadmap, Release 1.0 (Draft), Volume II Useful Information for Cloud Adopters', NIST

Special Publication 500-293, Noviembre de 2011. Disponible en línea en: <http://1.usa.gov/XJUGT2> [Visitado: 8 de mayo de 2013].

6. **NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE**, 'NIST US Government Cloud Computing Technology Roadmap Volume III - Technical Considerations for USG Cloud Computer Deployment Decisions (First Working Draft)', Noviembre de 2011. Disponible en línea en: <http://1.usa.gov/U1WFfa> [Visitado: 8 de mayo de 2013].

§ Unión Europea

7. **AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN (ENISA)**, 'Seguridad y resistencia en las nubes de la Administración Pública. Informe para la toma de decisiones', Enero de 2011. Disponible en línea en: <http://bit.ly/Sitjte> [Visitado: 8 de mayo de 2013].

8. **AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN (ENISA)**, 'Cloud Computing. Benefits, risks and recommendations for information security', 1 de noviembre de 2009. Disponible en línea en: <http://bit.ly/QBBNNQ> [Visitado: 8 de mayo de 2013]

§ Australia

9. **CYBER SECURITY OPERATIONS CENTRE**, Department of Defense, Security and Intelligence of the Government of Australia, 'Cloud Computing Security Considerations', 12 de abril de 2011. Disponible en línea en: <http://www.dsd.gov.au/infosec/cloudsecurity.htm> [Visitado: 8 de mayo de 2013]

§ España

10. **INSTITUTO NACIONAL DE TECNOLOGÍA DE LA COMUNICACIÓN (INTECO-CERT), GOBIERNO DE ESPAÑA**, 'Riesgos y Amenazas en Cloud Computing', Marzo de 2011. Disponible en línea en: <http://bit.ly/TTkcg1> [Visitado: 8 de mayo de 2013].

11. **INSTITUTO NACIONAL DE TECNOLOGÍA DE LA COMUNICACIÓN (INTECO-CERT), GOBIERNO DE ESPAÑA**, 'Estudio sobre el cloud computing en el sector público en España', Julio de 2012. Disponible en línea en: <http://www.inteco.es/Estudios/Estudio_Cloud_AAPP> [Visitado: 1 de julio de 2013].

§ Chile

12. **CONSEJO PARA LA TRANSPARENCIA**, 'Recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los órganos de la Administración del Estado'. Santiago, 5 de septiembre de 2011. Disponible en línea en: <http://bit.ly/Vbb9hs> [Visitado: 8 de mayo de 2013].

III. Dictámenes de Contraloría General de la República

1. Dictamen N° 19.444 de 30 de julio de 1993.

2. Dictamen N° 26.479 de 20 de agosto de 1996.

3. Dictamen N° 14.568 de 21 de abril de 1998.

4. Dictamen N° 9.642 de 10 de marzo de 2003.

5. Dictamen N° 30.305 de 21 de julio de 2003.

6. Dictamen N° 43.866 de 3 de octubre de 2003.

7. Dictamen N° 57.629 de 16 de diciembre de 2003.

8. Dictamen N° 57.623 de 22 de noviembre de 2004.
9. Dictamen N° 36.407 de 5 de agosto de 2005.
10. Dictamen N° 34.982 de 28 de agosto de 2008.
11. Dictamen N° 15.925 de 10 de abril de 2008.
12. Dictamen N° 44.186, de 4 de agosto de 2010.
13. Dictamen N° 67.520 de 12 de noviembre de 2010.
14. Dictamen N° 72.839 de 3 de julio de 2010.
15. Dictamen N° 46.564 de 22 de julio 2011.
16. Dictamen N° 72.839 de 3 de diciembre de 2012.