Cloud Computing en la Administración Pública: sobre la utilización de servidores para la externalización del almacenamiento de información.

[Cloud computing in the public administration: about usage of servers for the externalization of the information storage]

RODRIGO CAMPOS CORTÉS *

RESUMEN

El término *Cloud Computing* (computación en la nube) ha ganado creciente presencia y recordación en ámbitos académicos, tecnológicos y empresariales, como una nueva aproximación desde la perspectiva del concepto de "servicio", para la adquisición, acceso, uso, gestión y desarrollo de herramientas de *software* que soportan todo tipo de tareas; a partir de la computación personal y de oficina (por ejemplo documentación en línea) hasta la gestión pública y las tareas críticas de procesamiento y almacenamiento de datos a escala empresarial.

Para propender al acceso de esta clase de tecnología, la cual se destaca por ofrecer todos sus servicios de forma remota a través de esta analogía de "nube virtual", es necesario tener a la vista que existen ciertas variables ineludibles de considerar a la hora de la elección y contratación de un proveedor para sus servicios, así como también diversas interrogantes vinculadas al uso de esta clase de tecnología. Estas son de carácter generales, pero en el caso de las instituciones públicas, estas singularidades se ven esquematizadas en base a legalidades y políticas generales que estas instituciones deben cumplir dado su estatus de públicas, además de sus políticas internas. Es por esto que este trabajo tiene por finalidad aclarar estas interrogantes, además de establecer las pautas que debiesen considerar los organismos públicos a la hora de la redacción y suscripción de los contratos de *"cloud computing"* en vista a la sensibilidad de los datos que manejan.

Palabras claves: *Cloud Computing*,

ABSTRACT

The term Cloud Computing (cloud computing) has gained increasing presence and remembrance in academic, technological and business fields, as a new approach from the perspective of the concept of "service", for the acquisition, access, use, management and development of software tools that support all kinds of tasks; from personal and office computing (example online documentation) to public management and critical data processing and storage tasks at the enterprise level.

To promote access to this kind of technology, which stands out for offering all its services remotely through this "virtual cloud" analogy, it is necessary to bear in mind that there are certain inescapable variables to consider when the choice and contracting of a provider for its services, as well as various questions related to the use of this kind of technology. These are of a general nature, but in the case of public institutions, these singularities are outlined on the basis of legalities and general policies that these institutions must comply with given their public status, in addition to their internal policies. That is why this work aims to clarify these questions, in addition to establishing the guidelines that public bodies should consider when drafting and signing cloud computing contracts in view of the sensitivity of the data they handle.

Keywords: Cloud Computing, cloud contracting, questions in the use of this technology, public institutions

contratación *cloud*, interrogantes en el uso de esta tecnología, instituciones públicas.

I. INTRODUCCIÓN

Cada cierto tiempo se produce un cambio en la forma de cómo usamos las herramientas que nos brinda la informática en los diversos ámbitos de nuestra vida, y los estados no son ajenos a esta realidad, sea por conveniencia o necesidad se ven inmersos en la utilización de estas nuevas tecnologías

El sistema de externalización para el almacenamiento de información *Cloud Computing* o "Computación en la Nube" (en adelante CN) se inserta dentro de este contexto. Este sistema que surgió desde el mundo privado como forma de dar una solución a los grandes volúmenes de información que se manejaban y transaban, se ha extrapolado al sector público siendo de gran utilidad e importancia en la actualidad, derivando a lo que se conoce como el gobierno electrónico (*e-government*).

Dentro de nuestra realidad, el desarrollo del gobierno electrónico, cada día se hace más presente. En razón de este uso y desarrollo, se puede mencionar que en el estado chileno ha habido una evolución exponencial en el uso de las TI (*information technology*), pudiendo hacer una segmentación de los procesos de modernización.

En la etapa inicial de desarrollo (1990-2000) "las instituciones concentraron su esfuerzo en renovar y adquirir equipamiento, tanto para sus plataformas centrales como en lo que se refiere a computación personal"[1]. El objetivo era hacer que los procedimientos desarrollados por la administración del estado fueran más rápidos y ejecutados a menor costo, pues "procesar un formulario manual cuesta 10 veces más que uno electrónico"[2].

Una segunda etapa de evolución (2000-2005) estuvo enfocada en el "rediseño de procesos utilizando fuertemente las TIC's, estableciendo modelos multicapa con un enfoque web-enable como plataforma para interactuar con los ciudadanos"[3]. Las páginas web de las diversas entidades públicas pasaron a ser una especie de ventanillas modernas de atención, habiendo un esfuerzo importante de dotar a los servicios públicos con personal idóneo para estas áreas.

En la actualidad nos encontramos insertos en un nuevo proceso evolutivo en cuanto al uso de las TI, que tiene como característica principal la externalización de los grandes volúmenes de información que las entidades públicas manejan, como mecanismo de resguardo de esta información y para hacer más ágiles las labores que realizan estas mismas entidades.

Esto último se constituye como un gran avance, ya que hasta hace unos años las administraciones públicas manifestaban justificadas reservas respecto de la viabilidad de confiar sus aplicaciones y datos a proveedores de servicios "en la nube", dado que ello "implicaba una

---

[1] BARROS, Alejandro, *Servicios Compartidos (Share Services): la reforma faltante*. Disponible en https://www.alejandrobarros.com/servicios-compartidos-share-services-la-reforma-faltante/ [Consultado el 20 de noviembre de 2018].
[2] BARROS, Alejandro, cit. (n.1).
[3] BARROS, Alejandro, cit. (n.1).

dependencia respecto de terceros, así como cierta intangibilidad en las garantías de seguridad, confidencialidad y privacidad de los datos".[4]

Sin embargo, "la creciente capacidad y confiabilidad de los proveedores, junto a la disposición de éstos para alinear sus prestaciones a las condiciones del servicio requeridas, anima sucesivamente a los organismos gubernamentales a prescindir de las inversiones, gastos, limitaciones y problemas asociados a la adquisición y escalamiento de capacidades y recursos propios de TIC"[5]. Esto permite establecer el foco tanto de recursos humanos como de los recursos materiales que posee el servicio en su área crítica y enfocarse en la calidad de sus propios servicios en pro de los mismos ciudadanos.

Así, es necesario señalar que es claro que la CN ayuda de sobre manera a las diversas entidades públicas, en cuanto simplifica su funcionamiento derivando dicha mejora en el ciudadano, que ve mejorada su posición en cuanto usuario del servicio. Pero es ineludible mencionar que de la CN surgen diversas interrogantes, debido principalmente a la despreocupación por parte de la autoridad de brindar una efectiva reglamentación para el uso y aplicación de las TI, así como también del desconocimiento que se posee de las herramientas que nos brinda la informática dentro de la propia Administración, de esta forma cabe preguntarse, por ejemplo: ¿Qué entendemos por tecnologías *cloud computing*? ¿Qué diferencia al contrato de CN, respecto al contrato de *hosting*? De optar por la CN, ¿qué aspectos legales deben ser cubiertos para la utilización de esta tecnología? ¿Cuáles son las cláusulas que debiese contener el contrato de CN?

La problemática expuesta será abordada analíticamente en la presente memoria, iniciando la primera parte de esta con una introducción al *cloud*, en cuanto a su origen y conceptualización, además de exponer sus diversos caracteres. También se especificará su infraestructura técnica, todas cuestiones que se constituyen como básicas a la hora de comprender lo que se conoce como el "contrato *cloud*", el cual será principalmente el foco de nuestra atención. En esta misma línea se procederá a realizar una comparación entre el contrato de CN y el contrato de *Hosting*, los cuales muchas veces suelen confundirse, finalizando esta primera etapa con el análisis de los aspectos jurídicos generales del contrato de *cloud computing*.

Luego, en una segunda etapa, se procederá a un estudio de nuestra legislación tendiente a determinar qué aspectos legales deben ser cubiertos para la utilización de esta tecnología, analizando nuestra normativa vigente vinculada con el *cloud computing*.

Posteriormente, en una tercera y última etapa, se realizará un análisis de la forma en como la Administración puede hacerse de estos servicios de CN, ahondando específicamente en los aspectos contractuales que los órganos del Estado deben tener en cuenta al momento de contratar y negociar esta clase de servicios.

Se finalizará con algunas conclusiones propias al respecto, las que darán cuenta de una remisión a lo mencionado a lo largo de la memoria.

---

[4] Boletín e-Gobierno Red GEALC, *e-Gobierno en la nube,* edición 118, (2016), p.2. Disponible en http://portal.oas.org/LinkClick.aspx?fileticket=Z6hkABKDNfs%3D&tabid=1729 [consultado el 20 de noviembre de 2018].

[5] Boletín e-Gobierno Red GEALC*, e-Gobierno en la nube.* cit. (n.4), p. 2.

II. INTRODUCCIÓN AL CLOUD COMPUTING

En este primer título, efectuaremos un examen individualizado del origen, concepto, caracteres y las diferentes modalidades que existen en materia de los servicios relativos a la computación en la nube, así como también, estableceremos la diferenciación existente entre el contrato de *Hosting* y el de *cloud computing*, lo cual nos permitirá adentrarnos al contrato de CN desde la perspectiva de sus aspectos jurídicos generales.

1. Qué se entiende por *Cloud*. Origen y concepto

La nube o computación en la nube (diferentes términos para definir el *cloud computing*), es uno de los términos tecnológicos (*buzzwords*) que más ha estado en boga este último tiempo tanto en empresas, organizaciones y entidades de carácter público en general. Esto se debe a que es visto como una solución a los problemas derivados de lo que se conoce como la "infraestructura tecnológica".

En cuanto al origen de "la nube", debemos remontarnos a la década de los sesenta, en particular al año 1962, en donde Licklider de la empresa Bolt, Beranek and Newman (BBN), formuló un concepto de una red de computadoras susceptible de poder llegar a comunicar usuarios desde diversos ordenadores personales[6]. Douglas Parkhill, más de tres décadas después, en 1996, se refirió a muchos de los caracteres inherentes a la computación en la nube. No obstante, a juicio de otros investigadores[7], los verdaderos orígenes de la computación en la nube se sitúan en la década de los cincuenta del siglo XX con Herb Grosch.

Realmente fue a finales de los años noventa, precisamente en 1999, cuando "Salesforce.com" introdujo el concepto de entrega de aplicaciones empresariales a través de un sencillísimo sitio web. Luego, solo tres años después, la popular empresa Amazon puso en práctica Amazon Web Service. Cuatro años más tarde, o sea, en 2006, llegó *Google Docs*[8] que, como es conocido, popularizó el *cloud computing*. Naturalmente, además de los ejemplos enunciados, existen otros muchos, como *Dropbox, Google Drive, iCloud de Apple* y *OneDrive* de *Microsoft*.

Pero, ¿qué se entiende conceptualmente como *cloud computing*? En la actualidad, no existe una definición estándar aceptada universalmente; sin embargo, existen organismos internacionales, que tienen como objetivo la homogenización de las TI y en particular del *cloud computing*. Uno de los organismos más reputados en esta materia es el *National Institute of Standars and Technology* (NIST) y su laboratorio de TI, el cual define computación en la nube como:

---

[6] STELLA RODRÍGUEZ, Gladys, *Computación en la nube: algunas consideraciones técnico-jurídicas,* en *Revista Lex de la facultad de Derecho y Ciencias Políticas de la Universidad de Alas Peruanas,* 17 (2019) 23, p. 150.

[7] LÓPEZ JIMÉNEZ, David, *La computación en la nube o cloud computing examinada desde el ordenamiento jurídico español,* en *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso,* 24 (2013) 20, p. 693.

[8] El servicio de "Google Documentos y Hojas de cálculo", también denominado "Google Docs & Spreadsheets", constituye un programa gratuito basado en "web" para crear documentos en línea con la posibilidad de colaborar en grupo. Ahora bien, debemos poner de relieve que Google Docs recientemente ha sido reemplazado por Google Drive. Cada usuario tiene, de manera gratuita, cinco "gigabytes" de memoria con la finalidad de almacenar sus archivos.

"Un modelo que otorga acceso de red ubicuo, conveniente y *on-demand* a un pool de recursos computacionales configurables compartidos. (Ejemplo: redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente asignados y liberados, fácilmente administrables y de baja interacción con el proveedor del servicio".[9]

Asimismo, el *RAD Lab* de la Universidad de Berkeley señala que el servicio de la computación en la nube alude, por un lado, a las aplicaciones entregadas como servicio a través de Internet, y, por otro, al "*hardware*" y "*software*" de los centros de datos que proporcionan estos servicios.

A nivel normativo, el artículo 52 del Reglamento de la Ley federal mexicana de protección de datos personales, dispone que "*por cómputo en la nube se entenderá el modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software que se distribuyen de forma flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente*".

De esta forma, es posible apreciar que la computación en la nube se erige en una suerte de paradigma de programación, que aún está en proceso de evolución, pero que posee como eje central el hecho de ofrecer variados servicios informáticos a través de la red de redes, lo cual supone un notable cambio en el procesamiento de la información y gestión de las áreas TIC por parte de las empresas privadas y organismos de carácter público, debido a que con la gestión tradicional de las Tecnologías de la Información, las empresas y Administraciones Públicas efectúan cuantiosas inversiones en diversos y múltiples recursos. En este último sentido, podemos referirnos, a título de ejemplo, al "*hardware*" y "*software*", redes, personal, implementación de medidas de seguridad, así como centros de procesamiento de datos. Todas las inversiones mencionadas se reducen sensiblemente con el recurso al servicio de la computación en la nube[10].

2. Caracteres

Existe un conjunto de elementos inherentes al *cloud computing* que nos permiten distinguir este último de otros servicios susceptibles, en gran parte, de adscribirse en lo que podría denominarse sistemas de explotación de las TIC de corte tradicional. Para elaborar esta caracterización, nos remitiremos a lo establecido por López Jiménez[11], quien, desde la informática, nos entrega un análisis desde un punto de vista técnico, el cual consideramos necesario hacer para poder brindar un mejor desarrollo de este documento. De esta forma, conforme a este autor, cabe enunciar como características centrales las siguientes:

i) Pago en función del uso del servicio. El modelo de facturación dependerá del consumo. En otras palabras, la cuantía concreta que deberá abonar el cliente varía según el uso que se realiza del servicio *cloud* efectivamente contratado. Asimismo, nótese que el proveedor

[9] Traducción libre, *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment"*. MELL, Peter, GRANCE, Thimoty, *The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology*, U.S. Department of Commerce. Disponible en https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf, [Consultado el 27 de noviembre de 2018] p.2

[10] LÓPEZ JIMÉNEZ, David, cit. (n. 7), p.694.

[11] LÓPEZ JIMÉNEZ, David, cit. (n. 7), pp.695-696.

puede medir en determinado nivel el servicio efectivamente entregado a cada usuario, de forma que tanto proveedor como el usuario tienen acceso transparente al consumo real de los recursos, lo que, en este sentido, permite el abono por el uso efectivo de los servicios.

ii) Abstracción. Tal cualidad se refiere a la posibilidad de poder aislar los recursos informáticos contratados al proveedor de servicios de los equipos informáticos del cliente. Tenemos que considerar que todo cuanto comentamos es posible gracias a la virtualización.

iii) Aumento o disminución de las funcionalidades ofrecidas al cliente. Son, si se nos permite la expresión, una especie de autoservicio bajo demanda. Todo ello dependiendo de sus necesidades concretas y sin necesidad de nuevos contratos ni penalizaciones.

iv) Posibilidad de recurrir al denominado "servicio multiusuario". Se trata de que varios usuarios puedan utilizar, de manera compartida, medios y recursos informáticos, permitiendo de esta forma la optimización del uso. Es lo que, asimismo, se ha dado en llamar modelo de multiposesión o "*multi-tenancy*".

v) Petición automatizada bajo demanda. El usuario puede contratar, de manera progresiva, los servicios que vaya requiriendo de la computación en la nube a medida que los vaya estimando necesarios. En otros términos, en función a las necesidades empresariales de cada momento, pueden contratarse unos u otros servicios.

vi) Susceptibilidad de acceder a los servicios sin limitaciones. En efecto, los servicios de computación en la nube permiten, entre otros factores, que sean accesibles a cualquier hora, en cualquier lugar y desde múltiples y variados dispositivos informáticos –teléfonos móviles, ordenadores portátiles y PDAs–. Por otro lado, los clientes no precisan, en absoluto, disponer de su propia infraestructura, sino únicamente acceso vía web.

3. Infraestructura *Cloud*

Continuando con el análisis de esta clase de tecnologías desde un punto de vista técnico, cabe mencionar que las tecnologías *cloud computing* ofrecen tres modelos de servicios:

i) Software como Servicio (Saas): Al usuario se le da la posibilidad de que las aplicaciones que su proveedor suministra, corran en una infraestructura *cloud*[12]. Se accede a este servicio a través de un proveedor el cual se ocupa del hospedaje, mantención y seguridad de la aplicación. El consumidor no maneja o controla la infraestructura de la nube subyacente, incluyendo la red, servidores, sistemas operativos o almacenaje[13]. Este modelo ofrece a los clientes múltiples beneficios, tales como: reducción de costos en hardware y software (pago por uso), conectividad en cualquier momento y lugar (mediante conexión internet). Todo el soporte, actualizaciones y mejoras están controladas por el proveedor.

ii) Plataforma como Servicio (PaaS): Al usuario se le permite desplegar aplicaciones propias (adquiridas o desarrolladas por el propio usuario) en la infraestructura *cloud* de su proveedor que es quien ofrece la plataforma de desarrollo y las herramientas de

[12] JOYANES, Luis, *Computación en la nube, estrategias de cloud computing en las empresas*, (México DF, Editorial Alfaomega, 2012), p. 40.

[13] Traducción libre de "*The consumer does not manage or control the underlying cloud infrastructure including network, servers"* MELL, Peter, GRANCE, Thimoty, cit. (n.9), p.2.

programación[14]. El cliente tiene un control parcial sobre las configuraciones del entorno y las mismas aplicaciones, ya que la infraestructura y recursos aún dependen del proveedor que las despliega. Desde el punto de vista de la seguridad, esta es compartida entre el proveedor y el cliente, ya que las aplicaciones desarrolladas o "hosteadas" en la plataforma corren por parte del cliente[15].

iii) Infraestructura como Servicio (IaaS): En este tipo de infraestructura, el proveedor ofrece al usuario recursos, es decir, infraestructura computacional (capacidad de almacenamiento, procesamiento o comunicaciones). Este servicio entrega al cliente la libertad de poder realizar cualquier acción que se pudiese llevar a cabo en una infraestructura propia, tener servicios corriendo, desarrollo de aplicaciones, hosting, almacenamiento de datos, todo esto sin la necesidad de preocuparse por la gestión de los servidores físicos.

La finalidad de este servicio es "evitar la compra de infraestructura por parte de los clientes, buscando reducir costos de equipos, mantención y personal de TI, dado que todo esto es proporcionado por la empresa proveedora"[16].

Además, es importante considerar que existen cuatro posibles formas de desplegar y operar una estructura *cloud computing* (modalidades de implementación de computación en la nube). Nosotros, en atención al control y la gestión de los entornos informáticos, nos centraremos en cuatro tipos diversos, a saber: pública, privada, comunitaria e híbrida.

i) Nube Privada*:* La infraestructura de nube es proporcionada para el empleo exclusivo de una organización que comprende a múltiples consumidores (p.ej., unidades de negocio). Puede ser poseído, manejado, y administrado por la organización, un tercero, o alguna combinación de ellos[17].

ii) Nube Pública: La infraestructura de nube es proporcionada para el empleo abierto del público. Puede ser poseído, manejado y administrado por una empresa, institución o una organización del gobierno, o alguna combinación de ellos.

iii) Nube Comunitaria: La infraestructura de nube es proporcionada para el empleo exclusivo de una comunidad específica de consumidores que ha sido organizada para servir a una función o propósito común, puede ser una o varias organizaciones, pero que comprenden objetos comunes como su misión, políticas, seguridad o necesidades de cumplimientos regulatorios.

iv) Nube Hibrida: La infraestructura de nube es una composición de dos o más infraestructuras de nube distintas (privada, comunitaria o pública) pudiendo ser a su vez propias, compartidas o públicas, y permite portar datos o aplicaciones entre ellas. Con la combinación de ambas estructuras se puede mantener alta seguridad de una nube privada y al mismo tiempo aprovechar la escalabilidad y recursos *on-demand* de una nube pública, para momentos de sobrecarga.

---

[14] JOYANES, Luis, cit. (n.12), p. 41.

[15] QUIROZ ARÁNGUIZ, Alonso Diego*, Guía metodológica para el uso de cloud computing en instituciones públicas chilenas*, (Santiago, Chile, Memoria Departamento de Informática, Universidad Santa María, noviembre 2016), p.11.

[16] QUIROZ ARÁNGUIZ, Alonso Diego, cit. (n.15), p 12.

[17] Traducción libre de "*The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of the*m", MELL, Peter, GRANCE, Thimoty, cit (n.9), p.3.

Lo anterior es posible de reconducir al hecho que, en primer lugar, el modelo Iaas, es compatible tanto con la infraestructura de nube privada como híbrida, por su parte, el modelo PaaS, se inserta dentro de la nube comunitaria y también dentro de la nube pública y, por último, el modelo SaaS, se condice tanto con la infraestructura de nube comunitaria, como de nube híbrida.

En lo que respecta a los servicios de CN utilizados por la Administración del Estado, que es principalmente lo que nos concierne, es necesario tener en consideración que el tipo de nube a contratar se relaciona directamente con el tipo de información que la institución pública desea almacenar en esta. En este sentido al tratarse de información de carácter pública, la utilización de una nube pública no debiese ser inconveniente alguno para la institución, debido a que esta información tiene la finalidad de ser expuesta, por ende, posibles filtraciones de información o uso de la información por terceros no es una preocupación.

Por otro parte, si la información a almacenar es de carácter privado o sensible, el almacenamiento en una nube pública puede ser un problema si es que esta no cumple con los requisitos necesarios para poder operar información de esta clase. En este sentido un gran inconveniente que se origina con la utilización de esta clase de modelo *cloud*, es el hecho de que realmente no existe conocimiento exacto acerca de quien posee acceso a la información. Otro posible inconveniente con nubes públicas son las limitaciones técnicas que estas pudiesen llegar a tener con respecto a los requisitos necesarios que debe cumplir una institución pública como tal [18](disponibilidad[19], redundancia[20]). Por último, respecto de esta clase de modelo de implementación, cabe destacar que el uso de nubes públicas, para los órganos de la Administración, en nuestro país no se encuentra prohibido por ningún cuerpo legal, sin perjuicio de que existen múltiples nubes públicas con altos estándares de disponibilidad y seguridad de la información.

Por su parte, la utilización de una nube privada puede ser una buena opción en lo que respecta a la seguridad, debido a que la información no se encuentra en manos de terceros, ni se comparte infraestructura con otros clientes, sino que la información se encuentra en una nube privada donde el acceso a los recursos de esta nube es particularmente utilizado por la institución en cuestión. Además, por ser una nube privada, el cliente posee completo control sobre la misma, permitiendo un óptimo control respecto a la seguridad y los protocolos implementados, aunque es necesario tener a la vista respecto de este modelo de implementación *cloud* que, para poseer un óptimo funcionamiento de una nube privada, se requiere una inversión considerablemente mayor a la contratación de una nube pública. Las

---

[18] QUIROZ ARÁNGUIZ, Alonso Diego, cit. (n.15), p. 30.

[19] Disponibilidad es una característica de arquitectura que mide el grado con el que los recursos de los sistemas están activos-disponibles para su uso por el usuario final. Por lo que la Alta disponibilidad nos asegura que nuestros sistemas, ante posibles fallos, seguirán estando disponibles para su uso.

[20] La redundancia de Hardware significa tener los componentes del sistema duplicados; tenemos que tener en cuenta que al final cualquier proveedor de *cloud* lo que tiene en los CPD's son equipos, y el "hierro" al final siempre se termina estropeando, pero para que estos fallos no salpiquen a los usuarios y empresas que tienen contratados los servicios de *cloud*, se tienen todos los sistemas críticos, como he comentado, duplicados para que en caso de fallo se "muevan" de forma virtual las máquinas a aquellos sitios donde no haya afectado dicho fallo. De esta forma todos los elementos físicos de una plataforma *Cloud* deben estar redundados con alojamiento en diferentes ubicaciones del centro de datos o en diferente situación geográfica. Esto no exime de tener que programar copias de seguridad de cada una de las instancias, algo de lo que suele encargarse el proveedor. Estas copias permiten reponer un servidor *Cloud* incluso en aquellos casos en los que se pierda todo, ya sea por fallo técnico, error humano o intrusión.

nubes híbridas ofrecen lo mejor de ambos mundos, permitiendo mezclar ambos tipos de nubes en búsqueda de una combinación que se acomode a las necesidades del cliente.[21]

4. El Hosting v/s *Cloud* Computing

En tiempos actuales, en donde se busca la eficiencia y rendimiento óptimo en base a presupuestos apretados, empresas de todos los tamaños, así como también organismos públicos y entidades de diversa índole, buscan formas eficientes para atender sus necesidades de almacenamiento de datos.

Con la llegada del *cloud* computing, una nueva posibilidad de hospedaje nació, diferente del modelo tradicional de almacenamiento que el mercado conocía como *Hosting*. Aunque la nube no sea más novedad, algunos profesionales todavía confunden ambos servicios de almacenamiento. Por esto en este apartado, vamos a explicar las principales diferencias existentes entre ellos.

Aunque antes de proceder con la distinción, nos detendremos en el análisis vinculado a si el *Hosting* y el alojamiento de datos se refieren al mismo contenido contractual. En este sentido, a falta de regulación en nuestro país, conviene remitirse a la normativa europea, la que en el art.14 de la Directiva 2000/31 CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, la cual tradujo el concepto de *Hosting* de su versión original en inglés al español utilizando la expresión "alojamiento de datos", siendo esto uno de los elementos esenciales del *Hosting*, debiendo entenderse este como " aquel contrato por el cual el prestador se obliga a: i) posibilitar el almacenamiento de la información (hasta una determinada capacidad fijada en el propio contrato) en un soporte informático; ii) conservar los datos; y iii) hacerlos accesibles a través de la red global que constituye internet[22]". En este sentido, es posible señalar que existe un deber de custodia de los datos por parte del proveedor de manera segura, conservando su confidencialidad, integridad y disponibilidad, con lo cual este deber de custodia se configuraría como una obligación inherente al contrato de *Hosting*, aunque siempre teniendo en cuenta que esto se trata de una cuestión no del todo resulta, debido a que existe otra postura doctrinal la cual se refiere al deber de custodia de la información como una obligación accesoria y no como deber esencial del contrato de *Hosting*, especialmente respecto del hospedaje de páginas web, al entenderse en este caso que el fin último del contrato es la presencia del sitio web en Internet.

En nuestra opinión, si bien el concepto de alojamiento de datos puede abarcar algunos contratos de computación en la nube que impliquen el alojamiento remoto de contenidos digitales del cliente, lo cierto es que el contrato de computación en la nube, suele abarcar elementos distintos o añadidos al alojamiento remoto de información, de los cuales carece el contrato de *Hosting*. Entre estos elementos cabe destacar, en primer lugar, la existencia de un objeto más amplio del contrato, pudiendo consistir en funcionalidades facilitadas por aplicaciones informáticas, en redes virtuales o en plataformas de desarrollo de software, sin tener que corresponder estrictamente con el almacenamiento remoto de datos del cliente. En segundo lugar, en cuanto a las obligaciones esenciales de las partes, estas también son más amplias, relacionadas con los deberes de colaboración e información mutua, la adaptabilidad de

[21] QUIROZ ARÁNGUIZ, Alonso Diego, cit. (n.15), p. 30.
[22] YANGUAS GÓMEZ, Roberto, *Contratos de conexión a Internet, Hosting y búsqueda* (Navarra, Editorial Thomson Reuters, 2012), p. 316.

los recursos a las necesidades del cliente y la necesidad de devolución útil y segura de los datos migrados (las cuales serán analizadas con posterioridad). Por último, otra diferencia radicaría en la prestación bajo demanda y en el pago de recursos consumidos que suelen ser característicos de la computación en la nube, en contraposición a las capacidades y precios que suelen ser predeterminados en los contratos de *Hosting*[23].

En conclusión, aunque en algunas situaciones la distinción no parece sencilla, en el sentido de que ambos pueden compartir ciertas características, no puede asimilarse el contrato de CN al contrato de *Hosting*. El *cloud computing* abarca prestaciones heterogéneas que quedan fuera del ámbito del *Hosting* (por ejemplo, *softwares* como servicios que ofrezcan funcionalidades que vayan más allá del mero alojamiento, o plataformas de desarrollo informático), una mayor interacción del cliente con el servicio prestado (y por tanto, una mayor asunción de responsabilidades en cuanto a contenidos y uso del servicio) y la necesidad de un deber de colaboración entre las parte más estrecho, además de otras diferencias en la remuneración del servicio[24]. Ello no obsta para que puedan efectuarse analogías entre el concepto del contrato de *Hosting* y aquel contrato *cloud* cuyo objeto principal sea el alojamiento remoto de datos, a modo de criterio interpretativo.

5. Aspectos Jurídicos Generales

La referencia anteriormente mencionada relativa al contrato de *cloud computing*, permite adentrarnos más a fondo a un análisis de este, señalando elementos que deben ser tenidos en cuenta por cualquiera que celebre esta clase de contratos, sean entidades de carácter públicas o privadas. A este respecto podemos hacer una categorización que involucre sus aspectos jurídicos generales.

a) Naturaleza Jurídica del contrato de servicios de Computación en la Nube y régimen supletorio

De entrada, y adelantándonos a lo que se mencionará más adelante respecto de las características de esta clase de contratos, consideramos adecuado calificar al "contrato *cloud*" como un contrato atípico posible de reconducir por analogía al tipo general de contrato de prestación de servicios, en el sentido que en esta clase de contratos "se destaca como objeto una obligación de hacer, cuya prestación consiste en ejecutar o realizar una actividad, sea material o inmaterial, que en sí misma considerada o junto con su resultado si lo hubiere, beneficia exclusivamente al cliente y satisface su interés, en tanto representa la utilidad que persigue concretar con el contrato. Esta actividad es lo que constituye el servicio. Todo contrato que tenga este objeto podrá ser calificado como de servicios"[25].

Como se mencionó a nivel general el contrato de servicios es en rigor atípico, en tanto carece de una reglamentación sistemática destinada especialmente a fijar su régimen supletorio[26]. En la regulación particular de los contratos, la noción de servicios fue recogida en el contrato de arrendamiento, distinguiéndose tres tipos contractuales, posiblemente aplicables: la confección de una obra material, arrendamiento de transporte y arrendamiento de servicios.

---

[23] ROSELLÓ, Francisca María, *Cloud Computing. Régimen Jurídico Para Empresarios* (Pamplona, Editorial Thomson Reuters, 2018), p. 99.

[24] ROSELLÓ, Francisca María, cit. (n.23), p. 99.

[25] BRANTT, María Graciela, MEJÍAS ALONZO, Claudia, *El contrato de servicios como categoría general en el derecho chileno. Su contenido y rasgos distintivos,* en *Revista Ius et Praxis* 24 (2018) 3, p. 613.

[26] BRANTT, María Graciela, MEJÍAS ALONZO, Claudia, cit. (n.25), p. 586.

Creemos que la figura contractual que más se asemeja a los servicios de CN, es esta última referida al arrendamiento de servicios, en cuanto que en los "contratos *cloud*" podemos advertir un objeto principal (asimilable a un servicio) el cual consiste en la realización por parte del prestador del servicio *cloud*, de una o más tareas informáticas ofrecidas a través de la computación en la nube. Estas prestaciones pueden abarcar desde el suministro y el uso de medios de conexión simples y servicios básicos de computación (como almacenamiento de datos, mensajes de correo electrónico o aplicaciones de oficina) hasta la utilización y suministro de toda la gama de recursos físicos y virtuales necesarios para que el cliente elabore sus propias plataformas de tecnologías de la información, o para que el cliente despliegue, administre y ejecute aplicaciones o programas informáticos creados o adquiridos por él[27].

Obviamente, no es posible calzar exactamente el *cloud computing* dentro del arrendamiento de servicios, ya que aquél trasciende a este, pues la relación que se configura entre las partes de esta clase de contratos, es mucho más estrecha que un hacer y un pagar. Sin embargo, ello no debe perturbarnos, ya que nuestro objetivo no consiste en encontrar moldes exactos, sino que figuras similares, con la finalidad de hacer aplicable su regulación en caso de ausencia de norma convencional que solucione algún problema[28].

En consecuencia, a partir de lo anteriormente señalado, es posible mencionar que, siendo el contrato de CN atípico o innominado, posee la naturaleza jurídica propia de un contrato de servicios, en razón de su objeto principal, consistente en una prestación por parte del prestador del servicio *cloud*, de una o más tareas informáticas ofrecidas a través de la computación en la nube. La determinación de la naturaleza jurídica importa principalmente para la determinación del régimen supletorio aplicable para el caso en que las partes no hayan previsto la solución a algún problema. En este supuesto el vacío debe ser integrado aplicando las normas de interpretación de los contratos (arts. 1560 y ss. del Código Civil chileno) para poder desentrañar el verdadero sentido y alcance del mismo, como también las normas positivas referidas tanto a las obligaciones, como a los contratos en generales, además de las normas del contrato típico más semejante que en este caso serían las del arrendamiento de servicios[29] y por supuesto, los principios generales del Derecho.

Todo lo anteriormente mencionado resulta relevante, especialmente en los "contratos *cloud*" celebrados por la Administración, en donde, como se analizará con posterioridad, es la propia ley°19.886 la que explicita la posibilidad de aplicar categorías del Derecho Privado a situaciones no reguladas por la referida ley o en las cláusulas del respectivo contrato.

b) Características de los contratos de servicios de computación en la nube

Este tipo de contrato posee elementos propios que lo caracterizan, a saber:

i) Contrato atípico o innominado: Como se mencionó, el contrato de CN es atípico o innominado, en cuanto no ha sido objeto de regulación estructurada por parte del legislador.

---

[27] GRUPO DE TRABAJO IV (COMERCIO ELECTRÓNICO), CNUDMI, *Aspectos contractuales de la computación en la nube,* p.13.
Disponible en: https://undocs.org/es/A/CN.9/WG.IV/WP.142

[28] INOSTROZA Sáez, Mauricio Andrés, *El Contrato de Outsourcing Informático* (Memoria Universidad de Concepción, Concepción, Chile, 2004), p. 109.

[29] INOSTROZA Sáez, Mauricio Andrés, cit. (n.28), p.109.

Como es conocido, las partes dentro de un contrato, en razón del principio de autonomía de voluntad, poseen libertad para dar a sus convenciones el contenido que les plazca, siempre y cuando éste se enmarque dentro de los márgenes establece la ley, en particular en cuanto a los requisitos generales de la contratación, situación que posibilita crear convenciones que no estén expresamente reglamentadas por el legislador, tal como sucede en el contrato *cloud*.

Sin embargo, es importante considerar que, pese a su atipicidad, se trata de un contrato cuya naturaleza jurídica es posible de reconducir al tipo general de contrato de servicios, tal como se mencionó en el acápite anterior.

ii) Contrato consensual: El contrato de CN es consensual debido a que se perfecciona por el solo consentimiento de las partes (art.1443 del Código Civil).

La regla general en nuestro ordenamiento jurídico es el consensualismo, en el sentido que la exigencia de formalidades o solemnidades para manifestar la voluntad es de Derecho estricto, lo que implica que, tanto una como otras, deben estar exigidas por ley[30]. Siendo un contrato atípico, no existe norma positiva que establezca formalidades o solemnidades para poder celebrar un contrato *cloud*, lo que ha dado lugar a convenciones en que hay una ausencia de formalidades, y que pese a ello son perfectos desde el punto de vista del Derecho.

iii) Contrato bilateral: El contrato de computación en la nube es un contrato bilateral y sinalagmático, debido a que crea obligaciones recíprocas a cargo de ambas partes, pese a que, en la mayoría de los contratos celebrados entre particulares, las partes no se encuentren en igualdad de condiciones, a diferencia de lo que sucede con los contratos celebrados por la Administración y los proveedores *cloud*, en donde las partes se encuentran en posiciones equivalentes.

iv) Contrato oneroso: Ello porque esta convención tiene por objeto la utilidad de ambos contratantes, gravándose cada uno a beneficio de otro (art. 1440 del Código Civil). Los contratos de servicios de computación en la nube, generalmente se remuneran de acuerdo con la monitorización que realiza el proveedor del consumo de recursos del cliente, permitiendo ajustar el precio a la capacidad suscrita contractualmente y al efectivo volumen de recursos consumidos. Igualmente, existe la posibilidad de que el proveedor establezca otras modalidades de tarifado, como por ejemplo una tarifa plana que permita el acceso del recurso hasta un cierto límite de su capacidad, o una retribución que atienda al número de usuarios[31].

v) Contrato conmutativo: Debido a que cada una de las partes debe dar o hacer una cosa que se mira como equivalente a lo que la otra parte debe dar o hacer a su vez (art.1441 del Código Civil).

vi) Contrato de tracto sucesivo que se presta por medios electrónicos: Se constituye como otro rasgo característico del contrato *cloud*. Esta característica hace alusión a que el servicio en cuestión se presta de manera continuada en el tiempo, durante el cual se prolonga la relación entre el cliente y el proveedor. La duración de este contrato de tracto sucesivo variará dependiendo del proveedor y de las necesidades propias del cliente, y generalmente son

[30] DOMÍNGUEZ ÁGUILA, Ramón, *Teoría general del negocio jurídico* (Santiago, Editorial Jurídica de Chile, 1977), p. 125.
[31] ROSELLÓ, Francisca María, cit. (n.23), p. 113.

vinculantes desde que se suscriben, haciendo surgir desde ese momento las eventuales contraprestaciones.

vii) Contrato *intuito personae*: Se definen los negocios jurídicos *intuito personae* como aquellos en los que la identidad de la persona con quien se celebran es el principal motivo que lleva a manifestar la voluntad[32].

Lo señalado en la definición es lo que sucede en esta clase de contrato, ya que el proveedor del servicio es seleccionado por el cliente mediante un proceso metódico en donde se consideran diversos factores, principalmente los que dicen relación con las características propias de la institución, que la hacen subjetivamente diferente a las demás. Por otra parte, el hecho de delegar en un tercero el manejo de las tareas informáticas vinculadas al manejo de información implica un verdadero acto de confianza, habida consideración de la crucial importancia que esta actividad reviste para cualquier organización[33].

Por último, debemos señalar que a la hora de referirse a los contratos de CN celebrados por los órganos de la Administración, surge una consecuencia derivada de este carácter *intuito personae*, en cuanto el prestador del servicio tendrá sobre sí la obligación de cumplir por sí mismo todas las obligaciones que le impone el contrato, salvo cuando la ley establezca lo contrario, como sucede en el caso de los servicios *cloud* contratados por la Administración, en donde es posible la subcontratación parcial de los servicios conforme a la Ley N°19.886, de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios, la cual será analizada de forma posterior.

c) Obligaciones del prestador de servicios cloud computing y del suscriptor

En este acápite analizaremos, lo que es a nuestra consideración, las obligaciones generales tanto del proveedor como del suscriptor de estos tipos de servicios, de forma independiente al tipo de modelo *cloud* utilizado. Para la realización de esta labor, utilizamos como punto de referencia lo establecido por Rosselló Rubert[34], quien a nuestro entender sistematiza tales obligaciones de una manera clara, correcta y exacta.

De esta forma, el primer actor a analizar en cuanto a sus obligaciones, es el prestador del servicio, teniendo a la vista la consideración referida al hecho de que una prestación satisfactoria del servicio de computación en la nube supone el cumplimiento por parte del proveedor, no de una única obligación, sino de varias obligaciones inherentes a la naturaleza del servicio. Considerando las peculiaridades propias de la relación jurídica mencionaremos que el contenido de la prestación a la cual se obliga un proveedor de servicios *cloud*, se puede dividir en tres acciones complementarias:

i) En primer lugar, encontramos lo referido a la conectividad externa, entendiendo esta como el acceso ininterrumpido del usuario a los recursos (capacidad de almacenamiento, software, etc.), tal conectividad implica la disponibilidad de los recursos computacionales a través de internet o software, el mantenimiento de las instalaciones y la programación de los sistemas involucrados en la operativa de distribución del servicio que estén bajo control del proveedor, por ejemplo, a través del replicado entre diferentes centros de datos y la eficaz

[32] DOMÍNGUEZ ÁGUILA, Ramón, cit. (n.30), p.77.
[33] INOSTROZA SÁEZ, Mauricio Andrés, cit. (n .28), p. 100.
[34] ROSELLÓ, Francisca María, cit. (n.23), pp.243-245, pp. 317-320.

implementación de planes de recuperación frente a desastres. La conectividad externa se configurará en torno a la "multitenencia" que caracteriza a los entornos *cloud* (sobre todo de implementación pública), permitiendo así que múltiples usuarios utilicen el servicio de manera simultánea y sin interferencia entre sus datos o su manejo de los recursos. La disponibilidad del servicio exigirá que los sistemas del proveedor estén configurados adecuadamente no solo para facilitar el acceso simultáneo de distintos equipos de los usuarios al servicio *cloud* (conectividad externa), sino también para responder a cada una de las peticiones de recursos manera rápida y sin errores.

ii) En segundo lugar, y vinculada con la obligación anterior, encontramos la obligación de entregar recursos suministrados (capacidad de almacenamiento, software, etc.) de calidad. Esta calidad en el contexto del *cloud computing* corresponde a la suficiente elasticidad, a la fiabilidad del hardware y del software que los soporta y a un eficaz diseño de la interfaz que permita al cliente el aprovisionamiento bajo demanda con la mínima intervención del proveedor. Asimismo, puesto que generalmente el servicio implicará la transferencia de datos del cliente al proveedor y su almacenamiento remoto, este deberá custodiar de manera segura los contenidos procesados y migrados, manteniéndolos disponibles, íntegros y confidenciales para las personas autorizadas al acceso de esos contenidos. Una vez terminada la relación contractual de la custodia de los datos del cliente en los sistemas del proveedor, se deriva el deber de este de poner a disposición del cliente la información migrada, en un formato útil y que posibilite su uso sin que el cliente tenga que volver a introducir la información manualmente en los sistemas propios o de otro proveedor.

iii) Como tercer elemento, consideramos que el proveedor de servicios de computación en la nube tiene el deber de facilitar cierta información al cliente, preferiblemente antes de la suscripción del contrato. Dada la importancia que pueda tener para el cliente la adecuación del servicio a la criticidad de la información que se maneja. Asimismo, consideramos que el cliente debe recibir información sobre la utilidad concreta del servicio suscrito, puesto que la efectiva adecuación de las características del servicio a lo publicitado genera expectativas en el cliente que motivarán su elección del proveedor con quien contratar para así satisfacer de manera continuada sus concretas necesidades informáticas. Por último, consideramos que el proveedor deberá informar al cliente de los efectos derivados de la extinción del contrato, como el formato de recuperación de los datos, su portabilidad (es decir, la facilidad de transferirlos a otro proveedor sin necesidad de reintroducirlos manualmente), así como la información sobre la técnica de borrado que se ejecutará sobre los datos remanentes en sistemas del proveedor y que garantizará la máxima reversibilidad del servicio *cloud*.

Aunque las obligaciones mencionadas sean inherentes a la propia prestación del servicio, es importante marcar la diferencia entre los contratos *cloud* celebrados por la Administración y entre privados, ya que respecto a estos últimos, en ocasiones dichas obligaciones no se ven reflejadas contractualmente, es decir, el proveedor no siempre asume compromisos relacionados con un mínimo de calidad o continuidad en la prestación del servicio o con la devolución de datos migrados, a modo de objetivos de nivel de servicio. Ello es así porque, al ser el propio proveedor quien predispone el contrato de adhesión que deberá suscribir el cliente que quiera acceder al servicio, puede no incorporar un acuerdo de nivel de servicio o cláusulas que se refieran a estos extremos. En este supuesto, el contrato quedará sujeto a un abstracto deber de diligencia profesional del proveedor de servicios de

computación en la nube, y debiéndose tomar como referencia a tal efecto, y a falta de regulación específica los usos del sector.

Por su parte, una vez analizadas las obligaciones del proveedor que debiesen establecerse en los contratos de *cloud* celebrados entre proveedor y suscriptor, es menester analizar las obligaciones propias del suscriptor:

i) En primer lugar, y como obligación principal en aquellos contratos que se presten a cambio de precio, será esencial determinar de antemano los precios fijos por el uso del servicio, las tarifas con importe variable (como, por ejemplo, el consumo de recursos) y los precios derivados de eventuales servicios accesorios que se puedan contratar de manera separada.

En los contratos en base a modelos de nube pública, el precio a diferencia de los demás tipos de modelo *cloud*, por regla general no es determinado vía negociación, sino que se determina al aceptar el cliente la suscripción del servicio.

En cuanto a la determinación del precio, es importante señalar que, en la práctica, ante la falta de regulación, se estila que este se determine a través del pago de ciertas funcionalidades, a modo de tarifa plana, mediante el pago de consumos de recursos o el pago por el número de usuarios con derecho a utilizar el servicio. Al tratarse de un contrato de tracto sucesivo, el pago se realiza con periodicidad (mensual, triestamental, anual, etc.).

ii) En segundo lugar, entre las obligaciones del suscriptor del servicio, encontramos la existencia de un deber de colaboración con el proveedor, que por otra parte resulta implícito al propio contrato de servicios. En este sentido, las consecuencias establecidas contractualmente para el incumplimiento de la política de uso también se devengarán en los casos en el que el cliente entorpezca el servicio, teniendo en cuenta, para la determinación del daño, la incidencia que haya tenido el incumplimiento en la puesta en compromiso de la accesibilidad, rendimiento o seguridad del sistema, y si esa utilización ha causado daños y perjuicios al proveedor o a terceros usuarios.

Cuando la adecuación del servicio a las necesidades del cliente dependa de la recomendaciones que pueda hacerle el proveedor (por ejemplo, en relación a la sensibilidad de los datos que maneja, problemas técnicos que padece, etc.), será conveniente que el suscriptor tenga conocimiento de las informaciones que precisa aportar al proveedor, aunque siempre es deseable que este deber tenga reflejo contractual[35]. De esta forma el cliente destinatario del servicio tiene el deber de informar al proveedor *cloud* de peculiaridades que puedan afectar a la prestación, por ejemplo, el manejo de datos especialmente sensibles o de cargas de trabajo muy exigentes. Este deber está estrechamente vinculado con su deber de colaboración y con el principio de buena fe contractual.

iii) Por último, el suscriptor tiene el deber de usar adecuadamente el servicio, conforme a la finalidad prevista. Si el proveedor detecta un comportamiento del cliente que contravenga las disposiciones de la política de uso adecuado, podrá adoptar las consecuencias que contractualmente se prevean ante tal incumplimiento. Estas consecuencias pueden abarcar desde la suspensión o terminación del servicio para el presunto infractor mientras se investigan

[35] APARICIO VAQUERO, Juan Pablo, *La nueva contratación informática. Introducción al outsourcing de los sistemas de información* (Granada, Editorial Comares, 2002), p.125.

los hechos, hasta la asunción de responsabilidades por daños causados al proveedor o a terceros y derivados de la realización de actividades no permitidas[36].

III. Normativa Aplicable a los Servicios de Cloud Computing utilizados por la Administración del Estado

Una vez realizado el estudio del *cloud computing* desde un plano general, cabe adentrarse al análisis de esta tecnología desde el punto de vista de la Administración del Estado. En este sentido, un elemento esencial para propender con esta tarea es determinar qué normativa debiese ser tomada en cuenta tanto por los prestadores de los servicios *cloud*, pero principalmente por los órganos de la Administración a la hora de contratar esta clase de servicios.

Lo anterior resulta relevante, en el sentido de que en nuestro país no existen normas de seguridad para la provisión de productos y servicios tecnológicos al Estado de Chile que posean las cualidades de ser transversales, obligatorias y de aplicación directa. Sin embargo, son las mismas entidades públicas las que paulatinamente han ido incorporando requisitos de seguridad para los proveedores por la vía contractual, fundamentalmente en los procesos de licitación pública[37].

Estos requisitos de seguridad poseen como principales fuentes: i) normas obligatorias aplicables únicamente a la administración pública y/o ii) buenas prácticas o recomendaciones extendidas por la Dirección de Compras y Contratación Pública y cuyo objetivo es la misma administración (*soft law*).

Bajo este orden de ideas, es indispensable conocer cuáles son las normas obligatorias a la hora de proveerse de estos servicios, de forma que la Administración pueda aclarar sus dudas y para que los proveedores de servicios tecnológicos puedan prepararse con la debida antelación frente a una contraparte pública que le requiera de su cumplimiento. Este punto busca aclarar estas incertezas, entregando un catálogo de las leyes, ordenadas en forma decreciente en cuanto a su preponderancia (a nuestro parecer), que involucran el uso de tecnologías *cloud* y sus correspondientes implicancias.

1. Ley N°18575, Orgánica Constitucional de Bases Generales de la Administración del Estado

De esta forma, en cuanto a la regulación en torno a las tecnologías de CN en la Administración del Estado, es necesario colegir que el primer aspecto legal a cubrir es lo referido al régimen de responsabilidad extracontractual aplicable a los órganos del Estado, conforme a la "Ley Orgánica Constitucional de Bases Generales de la Administración del Estado".

---

[36] En nuestro país, esta obligación de uso adecuado del servicio se entiende consagrada en uno de los principios previstos por la Ley N°19.628, sobre Protección de la Vida Privada, este es el principio de finalidad, conforme al cual se debe respetar la finalidad informada al momento de recoger los datos, de manera que exista una relación directa entre aquella y el dato recabado (artículo 1° inciso segundo, artículo 5°).

[37] En Chile no hay una norma equivalente a los requisitos de ciberseguridad del DFARS de los Estados Unidos, que requiere a los contratistas de una institución pública cumplir con ciertos estándares de seguridad particulares.

En el plano fáctico, este régimen de responsabilidad eventualmente podría surgir de la relación existente entre el Administración y un prestador de servicio, por ejemplo, por el actuar arbitrario del primero en la licitación pública al no ceñirse a la normativa (Rol N.º 19.233-2017), o bien, en la relación existente entre la Administración y administrados, por filtraciones o usos inadecuados de los datos[38].

Bajo este orden de ideas, es esencial señalar que la LOCBGAE N°18.575 establece los principios generales en materia de responsabilidad de la Administración, tanto en su artículo 4° como en su artículo 44°, a este respecto se señala:

Artículo 4°: "*El Estado será responsable por los daños que causen los órganos de la Administración en el ejercicio de sus funciones, sin perjuicio de las responsabilidades (personales) que afecten al funcionario*".

Así, por ejemplo, el administrador del sistema es responsable penalmente si copia para uso particular la base de datos del servicio[39].

En lo referido a la segunda parte de este artículo, resulta importante resaltar que nuestra legislación contempla una serie de prohibiciones que afectan a los funcionarios de determinados órganos públicos en lo relativo a la revelación de información y cuya vulneración conlleva el surgimiento de responsabilidad personal. En este sentido, podemos mencionar a modo de ejemplo la revelación del secreto estadístico[40], o bien, la revelación de la reserva tributaria[41].

---

[38] Sin perjuicio de la responsabilidad que le atañe al prestador del servicio, conforme a lo estipulado a nivel contractual.

[39] Esto conforme el artículo 2° de la Ley N°19.223, el cual castiga el delito de hacking, estableciendo que se sanciona "*al que, con el ánimo de apoderarse, usar o conocer, indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él*".

[40] Consistente en la no divulgación y un estricto mantenimiento de esta reserva de los hechos que se refieren a personas o entidades de que hayan tomado conocimiento en el desempeño de sus actividades, esto es, en la recogida de la información.
Esta es una obligación legal, que contempla sanciones en el Código Penal (art. 247), y que se extiende a todos quienes accedan a esa información: organismos fiscales, semifiscales, empresas del Estado, y sus respectivos funcionarios.

[41] La reserva tributaria es entendida por el propio SII, como la "obligación que gravita sobre todos los funcionarios, que con motivo del cargo público que desempeñan, acceden al conocimiento de datos o antecedentes de índole tributaria de los contribuyentes, de no revelarlos o hacerlos públicos, salvo las excepciones legales".
Es necesario considerar, que el artículo 168 inciso tercero del Código Tributario hace aplicables a los funcionarios de Tesorería la obligación y sanciones que el mismo Código impone a los funcionarios del SII, en relación con el secreto de la documentación del contribuyente.
En lo relativo a la infracción de la obligación de reserva tributaria, las sanciones vienen previstas por el mismo cuerpo normativo, específicamente en los artículos 101 numeral 5° y en el artículo 102, el primero aplicable a los funcionarios del SII, en donde se prevé como sanción, la suspensión del funcionario de su empleo hasta por dos meses. Además de esto, atendida la gravedad de la falta, si se comprobare que el funcionario infractor hubiere solicitado o recibido una remuneración o recompensa, será sancionado con la destitución de su cargo, sin perjuicio de las penas contenidas en el Código Penal atendida la gravedad de la falta. La destitución tendrá lugar también en caso de reincidencia.
El segundo, es decir el artículo 102 del Código Tributario, contempla como titular de la norma a todo funcionario, sea fiscal o municipal o de instituciones o empresas públicas, incluyendo las que tengan carácter fiscal, semifiscal, municipal o de administración autónoma, que falte a las obligaciones que le impone el referido cuerpo normativo

Artículo 44.- "*Los órganos de la Administración serán responsables del daño que causen por falta de servicio.*

No obstante, el Estado tendrá derecho a repetir en contra del funcionario que hubiere incurrido en falta personal".

Este último artículo establece un sistema general de responsabilidad por falta de servicio, que resulta aplicable a todos los órganos que forman parte de la Administración del Estado, salvo aquellos que están excluidos expresamente: la Contraloría General de la República, el Banco Central, las Fuerzas Armadas y las Fuerzas de Orden y Seguridad Pública, los Gobiernos Regionales, las Municipalidades, el Consejo Nacional de Televisión, al Consejo para la Transparencia y las empresas públicas creadas por ley (artículo 21 de la Ley N.º 18.575).

En este caso, estos órganos se regirán por las normas constitucionales pertinentes y por sus respectivas leyes orgánicas constitucionales o de quórum calificado, según corresponda.

En lo que al *cloud computing* respecta, la falta de servicio podría configurarse debido a la inexistencia de prevenciones necesarias para acotar al máximo posible los daños que se puedan producir como consecuencia de algún incidente que afecte al proveedor. De esta forma, siguiendo lo establecido por el documento "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[42]*",* el cual establece criterios que tienen como propósito evitar el surgimiento de un acto dañoso en base a la consideración de un "aceptable funcionamiento del organismo público", como mínimo el órgano público deberá:

i) Contratar por separado un servicio de respaldo o back up 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.

ii) Velar por el encriptado de 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. 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.

Estas prevenciones se erigen como alguna de las bases de las expectativas de la comunidad, de aquello que tiene derecho a esperar respecto de los órganos de la

---

(entre las que se encuentra la reserva tributaria) o las leyes tributarias, prevé como sanción una multa del cinco por ciento de una unidad tributaria anual a cuatro unidades tributarias anuales. La reincidencia en un período de dos años será castigada con multa de media unidad tributaria anual a cuatro unidades tributarias anuales, sin perjuicio de las demás sanciones que puedan aplicarse de acuerdo con el estatuto que rija sus funciones.

[42] 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), p. 56. Disponible en: http://www.guiadigital.gob.cl/sites/default/files/2014_02_28_GuiaCloud_v1.0.pdf [Consultado el 27 de noviembre de 2018].

Administración en lo relacionado al tratamiento de sus datos e información consolidando la idea vinculada al hecho de que, si bien los órganos públicos pueden externalizar determinadas funciones vinculadas al tratamiento de datos, esto no lo exime de responsabilidad frente a los administrados.

Así las cosas, la noción de "responsabilidad por falta de servicio", la entendemos desde una noción amplia en la medida que abarca junto con la falta positiva del acto cumplido equivocadamente, la falta por omisión o retardo[43]. Se configura como aquella regla general de responsabilidad en lo que concierne a la Administración, sin entrar a la discusión clásica referida a si esta clase de responsabilidad posee la característica de ser subjetiva u objetiva, "particularmente a consecuencia de que el Derecho de Daños ha dado pasos hacia la consideración objetiva de la culpa: basta infringir la norma objetiva de cuidado para incurrir en culpa"[44].

Por ello es lógico calificar a la falta de servicio en base a un criterio de objetividad, en el sentido que lo que se exige para la imputabilidad por responsabilidad es la anormalidad, el comportamiento defectuoso en el funcionamiento de los órganos de la Administración, o bien, la simple omisión en el deber de actuar por parte de la Administración, en donde el Estado es responsable de los perjuicios ocasionados por la conducta de un tercero cuando estos podrían haberse evitado si el órgano administrativo hubiese cumplido cabalmente su misión[45] (en este caso en la adopción de medidas que eviten la divulgación de la información o el acceso no autorizado a esta), en donde el comportamiento volitivo del individuo no tiene injerencia para la determinación de tal responsabilidad.

Este criterio de atribución de responsabilidad implica que el Estado no se hace responsable por todo daño que puedan sufrir los ciudadanos producto de su relación con la actividad estatal. Por el contrario, para establecer la responsabilidad se realiza un juicio comparativo objetivo entre la actuación del servicio público y un estándar relativo a como este debería haber actuado. El juicio de responsabilidad en realidad atiende al establecimiento de la mala organización o el funcionamiento defectuoso del servicio, apreciando esas nociones en forma objetiva por referencia a lo que se está en derecho de exigir de un servicio público moderno. "Así las cosas, el criterio de falta de servicio tiene la virtud de servir como herramienta adecuada para equilibrar los intereses públicos y privados, pues exige definir lo que los ciudadanos pueden esperar de un servicio público moderno, es decir, la falta de servicio se derivaría de la contravención de las expectativas de la comunidad, de aquello que se tiene derecho a esperar"[46], así como en Arce Bahamondez con Servicio de Registro Civil e Identificación:

"(…) la existencia de la responsabilidad por falta de servicio del Estado (…) denota el incumplimiento de un deber de servicio que puede consistir en que no se preste el servicio que

[43] RIVERO, J., *Derecho Administrativo*. (9° edición, Caracas, Editorial Metropolitana, 1984), pp. 303,305,306.
[44] CORDERO VEGA, Luis, *Responsabilidad Extracontractual de la Administración del Estado* (Santiago, Ediciones Der, 2017), pp. 92-95.
[45] Ena Muñoz Contreras con Servicio de Registro Civil de Valparaíso, rol N°2068-2009- Casación en el fondo.
[46] Andrade Vera con Servicio de Salud Llanquihue Chiloé y Palena, Corte Suprema (2009), rol Nº3115-2008, considerando decimoséptimo; Villamán Riquelme con Tiznado Quintana y otro, Corte de Apelaciones de Concepción (2009), rol Nº917-2007, considerando decimosegundo; Burgos Araneda con Aroca Muñoz, Corte de Apelaciones de Concepción (2008), rol Nº1084-2007, considerando séptimo.

la Administración tenía el deber de prestar, se preste tardíamente o en forma defectuosa, de conformidad con el estándar de servicio que el público tiene derecho a esperar"[47].

De esta forma, es posible evaluar la falta de servicio desde la perspectiva del estándar. Lo que sucede es que, como esos estándares, por regla general, no están determinados explícitamente, es obligación del juez construirlos con criterios de razonabilidad[48].

2. Ley N°19.886, de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios

Un segundo aspecto a tener en consideración en la utilización de esta clase de tecnología, dice relación con el cumplimiento de la ley N°19.886, o "Ley de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios", la cual, conforme a su art. 1°, regula los contratos que celebre la Administración del Estado, a título oneroso, para el suministro de bienes muebles y de los servicios que se requieran para el desarrollo de sus funciones, estableciendo además, como se mencionó al referirse al tema vinculado a la "Naturaleza Jurídica del contrato de servicios de Computación en la Nube y régimen supletorio" del contrato *cloud*[49], la aplicación supletoria de las normas de Derecho Público y en defecto de aquéllas, las normas del Derecho Privado. Esto último resulta relevante en cuanto se explicita la posibilidad de aplicar categorías del Derecho Privado a situaciones no reguladas por la presente ley o en las cláusulas del respectivo contrato (Rol N°3.310-2009, Rol N°2525-2006).

En segundo término, un aspecto a analizar de este cuerpo legal, dice relación con la mención al art.13, el cual determina las causales de modificación o término anticipado aplicable a los contratos administrativos regulados mediante este cuerpo legal. En lo que a nosotros respecta, en este articulado se mencionan determinadas causales que representan el predominio de la Administración en relación a la persona del cocontratante particular, en el sentido de que es la propia Administración la que mediante resolución o decreto, ambos fundados, puede disponer tales medidas, dentro de las cuales figuran: "*a)La resciliación o mutuo acuerdo entre los contratantes; b) El incumplimiento grave de las obligaciones contraídas por el contratante ;c) El estado de notoria insolvencia del contratante, a menos que se mejoren las cauciones entregadas o las existentes sean suficientes para garantizar el cumplimiento del contrato; d) Por exigirlo el interés público o la seguridad nacional; y e) Las demás que se establezcan en las respectivas bases de la licitación o en el contrato".*

En tercer lugar, es necesario considerar los artículos 14 y 15 de la Ley N°19.886 y los artículos 74 y 76 del reglamento del mencionado cuerpo legal. En lo tocante a los artículos número 14 y 15, estos hacen referencia a la cesión y subcontratación de los servicios, señalando, a modo general, que no se permite que el contratista ceda en forma total la ejecución del contrato, sólo permitiendo una subcontratación parcial de los servicios por parte del encargado de tratamiento (el prestador de servicios de *cloud computing*)[50]. Este caso es común

[47] Arce Bahamondez con Servicio de Registro Civil e Identificación, Corte de Apelaciones de Santiago (2009), rol Nº9872-2006, considerando primero.
[48] CORDERO VEGA, Luis, cit. (n.44), p. 98.
[49] A este respecto cabe tener a la vista lo mencionado respecto a la "Naturaleza Jurídica del contrato de servicios de Computación en la Nube y régimen supletorio".
[50] Artículo 14.- Los derechos y obligaciones que nacen con ocasión del desarrollo de una licitación serán intransferibles.

en materias *cloud*, ya que muchos prestadores de servicios chilenos son "*resellers*" o asociados de los prestadores de los servicios *cloud*, por lo cual es necesario que el tercer oferente represente legalmente al prestador del servicio *cloud* para efectos de suscribir el contrato a nombre de este último[51].

Por su parte, los artículos 74 y 76 del reglamento de la ley N°19.886, vienen a reafirmar esta idea, en el entendido que el artículo 74 establece una prohibición de cesión total de los servicios, aplicable al contratista y el artículo 76, haciendo referencia a la subcontratación por parte del prestador de servicios, señala que, si bien esta procede, lo hace en forma parcial. Sin perjuicio de lo anterior, se menciona que la responsabilidad de su cumplimiento permanecerá en el contratista adjudicado. Esta regla no es absoluta, en cuanto se establece la prohibición de subcontratación en los casos que el propio artículo menciona[52].

Por último, otro punto importante a considerar, es que la referida ley de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios, crea la institución denominada Dirección de Compras y Contratación Pública, la cual viene a reemplazar a la antigua Dirección de Aprovisionamiento del Estado. Este organismo se constituye como un servicio público descentralizado, que dentro de sus funciones, "se encuentra el deber de asesorar a los organismos públicos en la planificación y gestión de sus procesos de compras y contrataciones y a su vez, 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 la normativa señalada, se efectúen consultas a dicho órgano"[53].

3. Ley N°19.628, sobre la Protección de la Vida Privada o Protección de Datos de Carácter Personal

Un tercer aspecto a tener en consideración, es lo vinculado al respeto que debe hacerse de nuestra legislación en lo que concierne al tratamiento y manejo de datos de carácter personales. En nuestro país, la Ley N°19.628, sobre Protección de la Vida Privada, se hace cargo de establecer en qué condiciones deben utilizarse las bases de datos personales en servidores de *cloud computing*. Por supuesto, no menciona expresamente a este modelo

---

Lo anterior se entiende sin perjuicio que una norma legal especial permita expresamente la cesión de derechos y obligaciones.

Los documentos justificativos de los créditos que de ellos emanen serán transferibles de acuerdo con las reglas del derecho común.

Artículo 15.- El contratante podrá concertar con terceros la ejecución parcial del contrato, sin perjuicio que la responsabilidad y la obligación de su cumplimiento permanecerá en el contratista adjudicado.

Con todo, no procederá la subcontratación en los casos especialmente previstos en el reglamento o ante una disposición expresa contenida en las respectivas bases de la licitación.

[51] QUIROZ Aránguiz, ALONSO Diego, cit. (n.15), p. 88.

[52] Artículo 76.- Subcontratación: El proveedor podrá concertar con terceros la subcontratación parcial del contrato, sin perjuicio que la responsabilidad de su cumplimiento permanecerá en el contratista adjudicado. Sin embargo, el Contratista no podrá subcontratar en los siguientes casos:

1. Cuando lo dispongan las bases, en particular, por tratarse de servicios especiales, en donde se ha contratado en vista de la capacidad o idoneidad del Contratista.
2. Cuando la persona del subcontratista, o sus socios o administradores, están afectas a alguna de las causales de inhabilidades e incompatibilidades establecidas en el artículo 92 del Reglamento.

[53] MINISTERIO 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), p.21.

tecnológico, pero constituye la normativa legal aplicable al tratamiento de datos personales que se realice en virtud de estos servicios.

Esta norma configura el estatuto jurídico general de lo que se conoce como "datos personales", los cuales son definidos por la propia ley en su artículo segundo letra f), entendiendo estos como "*los relativos a cualquier información concerniente a personas naturales, identificadas o identificables*". Esta definición posee como característica central la amplitud de los términos utilizados, así por ejemplo es posible considerar como dato personal inclusive la nacionalidad de una persona, el RUN, el domicilio, número telefónico, estado civil, condiciones de salud, entre otros.

En este punto, cabe precisar que el concepto de dato personal es distinto al concepto de dato sensible. De acuerdo a lo establecido en el artículo 2 letra f) de la Ley N°19.628, los datos sensibles son aquellos que se refieren a las "*características físicas o morales de las personas o a hechos o circunstancias relativas a su vida privada o su intimidad*" (como por ejemplo su orientación sexual, estado de salud psíquica, ciertas opiniones políticas, hábitos personales, entre otros). En este sentido, los datos personales pueden o no ser, a su turno, datos sensibles (existe una relación género-especie entre ellos)"[54], considerando además, que, respecto de estos últimos, el legislador dispone una protección reforzada, basada en la prohibición de su tratamiento, salvo autorización legal específica o consentimiento escrito del titular.

Continuando con el análisis, dentro de un esquema de contratos de CN, la aplicación de esta ley se comprende de mejor manera en la medida que se distinguen los roles de cada parte desde el punto de vista de la protección de datos personales y se establece quién efectúa el tratamiento de datos. Al respecto, observamos tres actores presentes en este cuerpo legal. "Por un lado, el responsable del registro o banco de datos (el cliente), el cual contrata estos servicios y que entrega una base de datos personales a la contraparte. Del otro, el proveedor del servicio (mandatario), quien recibe esos registros dentro de la información asociada a la ejecución del contrato, por ejemplo, para almacenarla, para realizar cruces, comparaciones o evaluaciones, o para comunicar datos a terceros si así lo contempla la prestación contratada. Por último, están las personas naturales (el titular) a quienes se refieren los datos contenidos en la base que entrega el cliente al proveedor"[55].

Especial consideración merece la figura del "cliente", el cual, desde el punto de vista de la Ley N°19.628, es quien entrega la base de datos personales al proveedor, siendo el responsable del registro o banco de datos, es decir, "*la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal*"[56]. En este sentido, "*en la figura del cliente descansa la decisión de externalizar algún tipo de tratamiento a través de servidores en la Nube y, precisamente, la materializa en el contrato que suscribe con el proveedor, estableciendo la forma en que ello se desarrollará*"[57].

---

[54] HÜBNER VALDIVIESO, Agustín, *Filtraciones Masivas de Datos Personales. Algunas ideas sobre el deber de confidencialidad y el régimen de responsabilidad aplicable*, en *Revista de Derecho Universidad San Sebastián* 25 (2019) 9, p. 103.
[55] HERRERA BRAVO, Rodolfo, *Cloud Computing y Seguridad: Despejando Nubes Para Proteger los Datos Personales*, en *Revista de Derecho Universidad San Sebastián* 17 (2011) 2, p. 49-50.
[56] Ley N°19.628, art.2°, letra n).
[57] HERRERA BRAVO, Rodolfo, cit. (n.55), p. 50.

En tal calidad, se le atribuye las obligaciones específicas que dispone esta legislación, como lo es: el velar por el respeto de la finalidad del tratamiento, además de la calidad de los datos, y la obligación de cuidado, especialmente en este caso, porque su entrega a terceros a través de una externalización encierra uno de los mayores riesgos para el titular, debido a que el control que puede ejercer sobre ellos se distancia o incluso desaparece por completo si no se respetan mínimas garantías de seguridad y debida diligencia al utilizarlos. En este sentido, cabe resaltar el hecho de que, si bien la Administración (el cliente) puede externalizar en otra entidad el tratamiento de esta clase de datos, no por eso deja de ostentar la calidad de "responsable de registro o banco de datos", lo cual viene a reforzar la idea planteada al hablar de la LBGAE, en el entendido que la Administración de cara a los administrados, no se exonera de responsabilidad frente a filtraciones o uso inadecuado de datos, alegando que dicha tarea vinculada al tratamiento de datos se encontraba externalizada, sin perjuicio de poder hacer efectiva ,posteriormente, la responsabilidad del proveedor de los servicios *cloud* conforme a lo estipulado a nivel contractual[58].

Un aspecto vinculado a lo recientemente mencionado, es lo concerniente a la obligación de secreto contemplada en el artículo 7° de esta Ley[59], referida al hecho de que todas las personas que trabajan en el tratamiento de datos personales se encuentran obligadas a guardar secreto sobre los mismos, cuando provengan de fuentes no accesibles al público, es decir, se trata de un aspecto compartido tanto por el responsable del registro o banco de datos, como por el prestador del servicio.

Esta obligación busca impedir que los datos sean conocidos ilícitamente, a través de revelaciones, infidencias o fugas de datos. Por ese motivo, se aplica no sólo al responsable del registro, sino que también al proveedor del servicio (mandatario), y a todos los que trabajen con esa información y no cesa por haber terminado el contrato o sus actividades en ese campo. Es decir, quien interviene en cualquier fase del tratamiento y deja de interactuar con la base de datos o, incluso, de prestar servicios al proveedor, debe guardar secreto de la información personal que conoció, indefinidamente[60]. De no hacerlo, la vulneración se sanciona indemnizando los perjuicios causados al titular del dato, en la medida que éste los acredite, e

---

[58] En la actualidad se encuentra en tramitación el proyecto de Ley N°11.144 -07, el cual tiene como objetivo general actualizar y modernizar el marco normativo e institucional en lo referido al tratamiento de datos personales de las personas naturales, en este sentido, este proyecto de ley viene a determinar de una mejor manera el régimen de responsabilidades de los responsables de datos, para lograr esta tarea se crean una serie de obligaciones y deberes para los responsables de datos, tales como acreditar la licitud del tratamiento que realizan; deberes de información; deberes de reserva y confidencialidad, de información y transparencia, y el deber de adoptar medidas de seguridad y reportar las vulneraciones dichas medidas.
Se regulan también la cesión o transferencia de las bases de datos personales que disponga o administre el responsable de datos, así como el régimen del tratamiento que efectúa un tercero o mandatario en representación o por encargo del responsable.
Por último, una de las principales innovaciones de esta nueva normativa en esta materia es la creación del "Registro Nacional de Cumplimiento y Sanciones", el cual es un registro nacional de carácter público administrado por la Agencia de Protección de Datos Personales, que consigna las sanciones impuestas a los responsables de datos por infracción a la ley, los modelos de prevención de infracciones que implementes los responsables y los programas de cumplimiento debidamente certificados.

[59] 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.

[60] HERRERA BRAVO, Rodolfo, cit. (n.55), p. 55.

incluso hasta podría configurarse un delito de revelación o difusión maliciosa de datos, que se castiga con presidio en su grado medio, pudiendo aumentarse en un grado si lo comete el responsable del registro o el mandatario[61].

De todo lo anteriormente mencionado cabe colegir, en primer lugar, que la propia ley excluye de la protección de los datos a las personas jurídicas, esto se debe a que a la Ley N°19.628 toma como marco referencial para su creación la legislación española de protección de datos, que establece la misma lógica; y, en segundo lugar, el hecho que la ley chilena no contempla expresamente la figura del "encargado" de datos personales (la persona que realiza el tratamiento de los datos y que responde frente al "responsable"), pero determina la figura del "mandatario" en el artículo 8°, análoga a la considerada en otras legislaciones, como la española, donde el encargado es caracterizado como "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento" (artículo 3 letra g. de la ley 15/1999). Dicho de otro modo, el proveedor no actúa como responsable del banco de datos sino como un mandatario de este.

Establece la ley en forma general, que a este mandatario le resultarán aplicables las reglas generales del mandato, el cual deberá ser otorgado por escrito con expresa constancia de las condiciones, respetando las estipulaciones de su encargo. Esto trae como consecuencia el hecho de que en el tratamiento de esta clase de datos no sería suficiente una cláusula genérica de mandato, sino que por el contrario, el contrato de servicios en la nube debe hacer mención expresa acerca del encargo de tratamiento de datos personales si lo hubiere. A partir de ello, las disposiciones de tratamiento de datos personales que se contemplen en un servicio de la nube tendrían carácter *intuito personae*, toda vez que existe un acto de confianza de parte del cliente (mandante) respecto del proveedor (mandatario), en la gestión de esas operaciones. Asimismo, "el mandatario, al igual que el responsable del registro, responderá hasta la culpa leve en su obligación de cuidar los datos personales, es decir, deberá indemnizar los daños que ocasione por la falta de la debida diligencia y cuidado que se emplea ordinariamente en los negocios propios"[62].

Esta exigencia legal también puede ser vista como una restricción legítima a la libertad de contratación, ya que el cliente, en cuanto responsable del registro y sujeto obligado a cuidar los datos personales, no podría suscribir un contrato de servicio *cloud computing* del tipo contrato de adhesión si éste no estipula las condiciones específicas de tratamiento bajo las cuales aquél está autorizado[63]. En ese sentido, estimamos que el cliente no podría limitarse a adherir contratos con cláusulas tipo elaboradas por el proveedor de servicios de computación en la Nube, porque difícilmente abordarían el tratamiento por mandato en la forma exigida por la Ley N°19.628 y, con ello, la externalización significaría una infracción legal del cliente responsable del banco de datos que lo expone a indemnizar los perjuicios que cause al titular.

---

[61] Ley N°19.223, que Tipifica Figuras Penales relativas a la Informática, artículo 4°: "*El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado*".

[62] HERRERA BRAVO, Rodolfo, cit. (n.55), p. 51.

[63] HERRERA BRAVO, Rodolfo, cit. (n.55), p. 51

4. Decreto N°83, sobre Seguridad y Confidencialidad de los Documentos Electrónicos

Este Decreto, elaborado por el Ministerio General de la Presidencia viene a desarrollar lo establecido en la Ley Nº19.799 (sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma), estableciendo las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos de los órganos de la Administración del Estado[64], para que de esta forma se garanticen estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución del documento electrónico; además de facilitar la relación electrónica entre los órganos de la Administración del Estado y la ciudadanía en general.

El Decreto número 83 es de aplicación general, es decir, aplicable a todo documento electrónico (considerado activo para la entidad que lo genera u obtiene) que se generen, intercambie, transporte y almacene en o entre los diferentes organismos de la Administración del Estado y en las relaciones de éstos con los particulares, cuando éstas tengan lugar utilizando técnicas y medios electrónicos[65], como sucede con los servicios de *cloud computing*. En este sentido, este cuerpo legal resulta aplicable a los órganos de la Administración Estatal, independientemente si han externalizado sus labores en manos de privados.

El Decreto en cuestión estableció niveles "básicos" y "avanzados" de seguridad para los documentos electrónicos de los servicios públicos, o al decir del artículo 1º, las características o exigencias mínimas obligatorias que los servicios debían cumplir y otras avanzadas que simplemente fueron recomendadas.

---

64 En lo relativo al denominado "documento electrónico", es importante considerar que en el ámbito de la Administración Pública chilena, se ha dado un importante avance hacía su implementación general dentro de esta, mediante el boletín 11882-02, el cual introduce variadas modificaciones a la Ley N°19.880, configurándose como una estrategia de Transformación Digital del Estado, que trae aparejado un cambio de paradigma en la forma como el Estado concibe su actuar tanto entre órganos de la Administración del Estado como al relacionarse con terceros, ya sean ciudadanos o personas jurídicas.
Entre las variaciones más importantes que incorpora el boletín, se destaca la modificación al actual artículo quinto, de la Ley N°19.880, relativo al principio de escrituración, señalando que "[e]l procedimiento administrativo y los actos administrativos a los cuales da origen se expresarán por escrito a través de medios electrónicos, a menos que se configure alguna excepción establecida en la ley". De esta forma, se consagra como la regla general la escrituración por medios electrónicos, la cual se materializa en el documento electrónico, con lo que se genera una importante diferencia con el artículo quinto actual, que señala la existencia de la posibilidad de que el procedimiento administrativo y los actos administrativos a los cuales da origen, se expresen tanto por escrito como por medios electrónicos.
Lo anterior se complementa con la modificación del actual artículo 18 inciso 3°de la propia LBPA, el cual consagra que "todo el procedimiento administrativo deberá constar en un expediente, escrito o electrónico, en el que se asentarán los documentos presentados por los interesados, por terceros y por otros órganos públicos, con expresión de la fecha y hora de su recepción, respetando su orden de ingreso". La modificación respectiva dice relación con que se elimina esta posibilidad de hacer constar el procedimiento administrativo en un expediente en formato escrito o electrónico, es decir, con la aprobación del boletín todo procedimiento administrativo deberá constar solamente en un expediente en formato electrónico.
De esta forma, es sencillo reconocer que el sistema papel, que por años ha sido el sustento de nuestro sistema jurídico, poco a poco ha ido en retirada, lo que viene a hacer palpable esta forma actual de llevar los grandes flujos de información por vía de un manejo informático, a expensas de un formato papel el cual presenta como desventajas el hecho de traer aparejado un elevado costo económico, su ineficiencia y ser radicalmente obsoleto.
65 Artículo 2°, Decreto N°83, sobre Seguridad y Confidencialidad de los Documentos Electrónicos.

Estas "exigencias" y "recomendaciones", se formularon con el norte de cumplir tres fines expresamente declarados: (i) garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución del documento electrónico; (ii) facilitar la relación electrónica entre los órganos de la Administración del Estado, y entre estos y la ciudadanía o el sector privado; y, (iii) salvaguardar el uso del documento electrónico de manera segura y confiable.

En lo que respecta al nivel básico de seguridad (Título IV), en sus diversos párrafos se abordan tópicos como la Política de Seguridad, la seguridad organizacional, la clasificación, control y etiquetado de bienes, la seguridad física y del ambiente, la seguridad del personal, la gestión de las operaciones y las comunicaciones, el control de acceso, el desarrollo y mantenimiento de sistemas y la gestión de la continuidad del negocio.

Dentro de este nivel de seguridad, en lo referido a la "Gestión de la continuidad del negocio", este Decreto exige la adopción de medidas para mantener la continuidad de operaciones críticas para las instituciones[66].

De esta forma, 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 debiese revisar con cuidado los niveles de servicios (ANS) en que el prestador *cloud* está en condiciones de garantizar. En este sentido, al momento de la determinación del proveedor, se debiese privilegiar a aquellos proveedores de servicios que tengan la capacidad organizativa y técnica que pueda asegurar la continuidad del servicio"[67].

En cuanto al nivel avanzado de seguridad para el documento electrónico, el decreto exige el cumplimiento de las exigencias y condiciones reguladas en el Título IV para el Nivel Básico de seguridad, y las previstas en la Norma NCh 2777, que se entiende parte integrante del decreto en cuestión, con los ajustes que se establecen en el artículo N°37[68].

5. Ley N°20.285, sobre Acceso a la Información Pública. La Información Reservada, artículo N°21

Otro tema relevante a considerar a la hora de la utilización de esta clase de servicios por parte de la Administración, 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

[66] Véase, por ejemplo, artículo 35 del Decreto N°83, 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. 12.01.2005.

[67] MINISTERIO 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, 2014), p. 29.

[68] Este Decreto ha sido objeto críticas en el sentido de que no existe un órgano encargado de fiscalizar sistemáticamente dentro de la Administración del Estado su aplicación, salvo las auditorías aleatorias y no permanentes que realiza la CGR; y, además, el Decreto se encontraría obsoleto o requiere ser actualizado, para referirse a la actual Norma Oficial del INN (la NCh-ISO 27002 del 2013) y no a una del año 2003 (la NCh 2777).

regulados en la mencionada Ley N°19.688, sino que también cuando el órgano respectivo maneja información secreta o reservada de conformidad al artículo 21 de la Ley N°20.285[69].

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*. ¿Es dicha información pública o es reservada de conformidad a lo dispuesto en el artículo 21 de la Ley N°20.285?

Este articulado se configura como un listado taxativo, pero de causales genéricas o generales que requieren ser interpretadas, en virtud de las cuales cierto tipo de información y de antecedentes administrativos no pueden ser transparentados o publicados. De esta forma, la información reservada se consagra en el artículo 21 de la ley en cuestión, señalando al respecto:

i) Causales de los números 1, 3 y 4: El número 1 se plantea en la hipótesis de que su publicidad, comunicación o conocimiento afecte el debido cumplimiento de las funciones del órgano requerido, particularmente (más no exclusivamente) autoriza a eximirse de la entrega de los documentos o antecedentes en tres supuestos:

"a) Si es en desmedro de la prevención, investigación y persecución de un crimen o simple delito o se trate de antecedentes necesarios a defensas jurídicas y judiciales.

b) Tratándose de antecedentes o deliberaciones previas a la adopción de una resolución, medida o política, sin perjuicio que los fundamentos de aquéllas sean públicos una vez que sean adoptadas.

c) Tratándose de requerimientos de carácter genérico, referidos a un elevado número de actos administrativos o sus antecedentes o cuya atención requiera distraer indebidamente a los funcionarios del cumplimiento regular de sus labores habituales".

Por su parte, la causal N°3 alude al hecho de que su "*publicidad, comunicación o conocimiento afecte la seguridad de la Nación, particularmente (y no exclusivamente) si se refiere a la defensa nacional o la mantención del orden público o la seguridad pública*". Y el número 4 alude al hecho de que "*su publicidad, comunicación o conocimiento afecte el interés nacional, en especial* (pero no exclusivamente) *si se refieren a la salud pública o las relaciones internacionales y los intereses económicos o comerciales del país*".

ii) Causales de los números 2 y 5: La causal número 2 menciona que es causal de secreto o reserva "*cuando su publicidad, comunicación o conocimiento afecte los derechos de las personas, particularmente* (a modo de ejemplos lo cita la ley) *tratándose de su seguridad, su salud, la esfera de su vida privada o derechos de carácter comercial o económico*". En este punto la ley no hace referencia al tipo de persona que se trata (natural o jurídica), compartiendo la opinión de Jijena Leiva, la expresión "personas", debiese ser entendida en el sentido que abarca tanto a la persona natural como jurídica, debido a que no existe vinculación con el hecho de que la Ley N°19.628 sólo aluda o este restringida a los antecedentes nominativos de las personas naturales[70].

Además, es necesario considerar que cuando en esta causal se hace alusión a la "esfera de vida privada", normativamente existe un reenvío tanto a la Ley N°19.628 como a otras disposiciones.

---

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

[70] JIJENA LEIVA, Renato, *Tratamiento de datos personales en el Estado y acceso a la información pública,* en *Revista Chilena de Derecho y Tecnología* 2 (2013) 2, p 78.

En primer lugar, se hace alusión a la Ley N°19.628, porque ella se aboca desde su título a la protección de la vida privada, tanto en cuanto datos o antecedentes personales o nominativos, sensibles o no, de aquellos que la misma ley sujeta complementariamente a la obligación general de secreto o de reserva para el servicio público en el artículo 7, de aquellos que en los órganos de la Administración no están disponibles en fuentes de acceso público, y de aquellos que son especialmente reservados como los datos sensibles o personalísimos.

En segundo lugar, se hace un reenvío a otras disposiciones constitucionales, legales y reglamentarias, comenzando por el artículo 19 número 4 de la Constitución, y siguiendo con leyes especiales que establecen su calidad de antecedentes secretos.

Además, podemos mencionar el reglamento de la Ley N°20.285, el cual en su artículo 7° número 2 señala que es posible denegar la información cuando la publicidad, comunicación o conocimiento afecte los derechos de las personas, especial o particularmente tratándose de su seguridad, su salud, la esfera de su vida privada, sus datos sensibles o sus "*derechos de carácter comercial o económico*", entendiendo "por tales" a aquellos que el ordenamiento jurídico atribuye a las personas en título de derecho y no de simple interés (o de mera expectativa, podemos agregar)[71].

Por su parte, en virtud del número 5, es causal de secreto o reserva "*cuando se trate de documentos, datos o informaciones que una ley de quórum calificado haya declarado reservados o secretos, de acuerdo a las causales señaladas en el artículo 8º de la Constitución Política*". Esas causales del artículo 8 se refieren, al evento que la publicidad afecte "*el debido cumplimiento de las funciones de los órganos del Estado", "los derechos de las personas", "la seguridad de la Nación"* o *"el interés nacional"*.

De esta forma, si el órgano de la Administración adopta la decisión de subir dicha clase de información a la nube, se deben adoptar una serie de medidas de seguridad vinculadas al establecimiento de cláusulas de confidencialidad que tiendan a evitar su divulgación, dichas cláusulas serán analizadas venideramente.

6. Ley N°17.336, sobre Propiedad Intelectual

Continuando con el análisis, también un elemento esencial a considerar, dice relación con el respeto de la normativa chilena sobre propiedad intelectual, contenida en la Ley N°17.336, la cual es aquella ley especial que regula los derechos de autor y derechos conexos en Chile.

En el plano fáctico y en aplicación de este cuerpo legal, desde el punto de vista del *cloud* computing encontramos tres clases de información sujeta a propiedad intelectual. "Primero se tiene el sistema o software, que en el caso de ser un desarrollo específico de la institución, el código y la propiedad intelectual del mismo es de la institución pública. En segundo lugar, encontramos la información o documentos que pueden ser subidos o que se encuentran dentro del aplicativo o infraestructura *Cloud*. Por último, encontramos la información originada a partir del uso del sistema (bases de datos).

[71] JIJENA LEIVA, Renato, *Tratamiento de datos,* cit. (n.70), p.79.

Es necesario precisar, que estos tres tipos de información pueden ser considerados propiedad intelectual de la institución, pero en muchos casos no lo son. Dado la funcionalidad de las instituciones públicas, parte de la información que estas almacenan son datos de la ciudadanía, lo que implica que ninguna propiedad intelectual debiese ser reclamada sobre esta información. Esto corre tanto para almacenamiento de información como para documentos"[72].

En este sentido, el órgano contratante debe poner atención en mantener los derechos de propiedad intelectual de los documentos y demás informaciones que se suben a la nube, velando que el prestador de servicios respete lo establecido por la ley chilena en lo concerniente a la propiedad intelectual y a nivel contractual, estableciendo cláusulas que apunten en esta misma dirección (cláusulas de propiedad intelectual que serán analizadas en esta memoria posteriormente).

Respecto de la infracción de esta norma, las causales y sanciones vienen determinadas por los artículos 79 y ss. Ahora bien, es importante tener en consideración que nuestro país contempló dentro de esta ley, una serie de artículos referidos a la limitación de responsabilidad en favor de los prestadores de servicio de Internet[73] por las infracciones a los derechos de autor cometidas por sus usuarios[74]. En este sentido, cabe destacar el artículo 85 Ñ, referido a los prestadores de servicios que a petición de un usuario almacenan, por sí o por intermedio de terceros, datos en su red o sistema, los cuales no serán considerados responsables de los datos almacenados o referidos a condición que el prestador: a) No tenga conocimiento efectivo del carácter ilícito de los datos; b) No reciba un beneficio económico directamente atribuible a la actividad infractora, en los casos en que tenga el derecho y la capacidad para controlar dicha actividad; c) Designe públicamente un representante para recibir las notificaciones judiciales a que se refiere el inciso final, de la forma que determine el reglamento; y por último, d) Retire o inhabilite en forma expedita el acceso al material almacenado de conformidad a lo dispuesto en el inciso siguiente[75].

Creemos que esta limitante de responsabilidad no resulta aplicable a los proveedores de los servicios de *cloud computing* en el sentido que no se cumple con lo dispuesto por el art. 85 Ñ, letra b) en cuanto este proveedor recibe un beneficio económico directamente atribuible a la actividad infractora, en el sentido de que tal como se mencionó al hablar de las características del contrato de *cloud computing,* este se configura como un contrato de carácter oneroso[76], independientemente de quien contrate, generalmente remunerado de acuerdo con la monitorización que realiza el proveedor del consumo de recursos del cliente, o bien

---

[72] QUIROZ Aránguiz, Alonso Diego, cit. (n.15), p 125.

[73] Cabe recordar que una de las conceptualizaciones que se tienen sobre los servicios de *"Cloud Computing",* viene dada por el RAD Lab de la Universidad de Berkeley, el cual dispone que el servicio de la computación en la nube alude, por un lado, a las aplicaciones entregadas como servicio a través de Internet, y, por otro, al "hardware" y "software" de los centros de datos que proporcionan estos servicios.

[74] Ley N°17.336, sobre Propiedad Intelectual, artículos 85 y siguientes.

[75] Se entenderá que el prestador de servicios tiene un conocimiento efectivo cuando un tribunal de justicia competente, conforme al procedimiento establecido en el artículo 85 Q, haya ordenado el retiro de los datos o el bloqueo del acceso a ellos y el prestador de servicios, estando notificado legalmente de dicha resolución, no cumpla de manera expedita con ella.

[76] En este sentido véase, sección II, Características de los contratos de servicios de computación en la nube, pp.15-17.

estableciendo otras modalidades de tarifado, como una tarifa plana o una retribución en virtud del número usuarios.

7. Ley N°19.223, que Tipifica Figuras Penales Relativas a la Informática

Por último, conviene a tener a la vista lo relativo a la Ley N°19.233, la cual protege "un nuevo bien jurídico que ha surgido con el uso de las tecnologías computacionales: la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan[77]". Este cuerpo legal contempla cuatro artículos, que si bien corresponden cada uno a un tipo de conducta distinta, se pueden clasificar en tres grandes figuras delictivas: fraude informático, sabotaje informático y espionaje informático. A su vez, estas tres figuras se subdividen en categorías distintas, atendiendo al objeto contra el cual atentan y/o al modus operandi.

A continuación, se transcriben las disposiciones de la citada ley que tipifica los delitos informáticos:

"Artículo 1°. - El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Artículo 2°. - El que, con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3°. - El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4°. - El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado."

De esta forma, cuando se habla de las modalidades de criminalidad informática, como se mencionó, se suele distinguir entre el fraude informático, el sabotaje informático y el espionaje informático. Siguiendo a Jijena Leiva[78], dentro del primer grupo (artículo 3° Ley N°19.233) se encuentran las "posibles alteraciones o manipulaciones, tanto de los datos (al recopilarlos, procesarlos, estando almacenados o al transmitirlos telemáticamente), como de los programas de un sistema computacional". En segundo término, dentro del espionaje informático (artículo 2° y 4° de la Ley N°19.223), entran las figuras de "obtención ilícita, dolosa y sin autorización de datos o información relevante y de programas computacionales", es decir, este comprende aquellas figuras delictivas que atienden al modo operativo que se

[77] Moción parlamentaria del diputado José Antonio Viera-Gallo del 16 de julio de 1991, sesión 19, legislatura 322, Boletín 412-07.

[78] JIJENA LEIVA, Renato, *Delitos informáticos, Internet y derecho.* En RODRÍGUEZ COLLAO, Luis (coordinador), *Delito, pena y proceso* (Santiago, Editorial Jurídica de Chile, 2008), pp. 148-149.

ejecuta y que pueden ser, en primer lugar, delitos de apoderamiento indebido (apropiarse de la información), uso indebido (usar la información para cualquier fin) o conocimiento indebido de la información; cometidos interfiriendo, interceptando o meramente accediendo al sistema de tratamiento de datos. Estas figuras comprenden lo comúnmente conocido como "hacking". Finalmente, dentro del sabotaje informático (artículo 1° Ley N°19.233) caben las figuras de "atentados que causan daños, destruyen o inutilizan un sistema computacional", el atentado a estos objetos puede ser a través de su destrucción, inutilización, obstaculización o modificación[79].

Todas estas figuras penales debiesen ser consideradas por quienes tienen acceso a la información almacenadas en los servidores *cloud computing*, ya sean parte de la empresa que presta esta clase de servicios o bien por los funcionarios de la propia Administración.

IV. EL CLOUD COMPUTING EN LA ADMINISTRACIÓN ESTATAL

Para todo cliente que desea acceder a un servicio *cloud*, existen ciertas consideraciones que debe tener a la vista a la hora de la elección y contratación de un proveedor para sus servicios. Estas son de carácter generales, pero en el caso de las instituciones públicas, estas singularidades se ven esquematizadas en base a legalidades y políticas generales que las instituciones públicas deben cumplir dado su estatus de públicas, además de sus políticas internas. Es por esto que este apartado tiene por finalidad establecer las pautas que debiesen considerar las instituciones públicas a la hora de la redacción y suscripción de los contratos de CN en vista a la sensibilidad de los datos que manejan.

Para la concreción de lo anterior es necesario establecer algunas consideraciones previas, en el sentido de que, si bien esta memoria se enfoca principalmente los aspectos legales de la contratación de servicios *cloud*, cabe destacar que las previsiones legales señaladas con anterioridad se aplican no solo a la redacción de esta clase de contratos, sino que a todo el proceso de contratación pública. Por lo mismo, esas menciones, además de las sugerencias y observaciones que serán señaladas a la hora de hablar del contrato de CN, debieran considerarse, por ejemplo, al momento de redactar las Bases de Licitación (cuando

[79] Es importante considerar que actualmente se tramita en el Congreso Nacional, un proyecto de ley (número del boletín:12192-23), el cual pretende actualizar la legislación actual en base al Convenio de Budapest, un tratado internacional firmado hace ya bastante tiempo (2001) al cual Chile se sumó en abril de 2017 como parte de una renovada política de ciberseguridad.
Los nuevos delitos que se agregarán a la ley son ocho:
1.-Captación visual y sonora de información sin consentimiento
2.-Difusión de ese material
3.-Producción de programas o dispositivos para cometer delitos
4.-Difusión de información de un sistema informático
5.-Manipulación de claves confidenciales y de datos codificados en una tarjeta
6.-Uso de programas o dispositivos para vulnerar la integridad de datos
7.-Alteración o daño de sistemas informáticos
8.-Alteración de datos para acceder a un sistema informático

procediere[80]) y al momento la suscripción del respectivo Convenio Marco. Asimismo, debiesen considerarse al momento de la redacción del Acuerdo de Nivel de Servicio respectivo.

1. Convenio Marco de Data Center y Servicios Asociados

Los convenios marco son Lista de bienes y/o servicios y sus correspondientes condiciones de contratación, previamente licitados y adjudicados por la Dirección y puestos, a través del Sistema de Información, a disposición de las Entidades[81].

Se disponen en un Catálogo Electrónico de Productos y Servicios para que los organismos públicos accedan a ellos directamente, pudiendo emitir una orden de compra directamente a los proveedores "prelicitados", acortando los procesos de compra.

Corresponde a la Dirección de Compras y Contratación Pública, sea de oficio o a petición de uno o más organismos públicos, licitar bienes y servicios a través de la suscripción de convenios marco, los que estarán regulados en el reglamento de la ley N°19.886[82].

En materia de contratación de servicios de CN por parte de la Administración, es aplicable el "Convenio Marco Data Center y Servicios Asociados", el cual contempla una serie de empresas relacionadas a la temática, las cuales se encuentran pre-aprobados a nivel gubernamental para el uso estatal de los servicios que estas entregan. Mediante el portal *Mercadopublico*, los organismos del Estado tienen acceso a un listado de proveedores *cloud* disponibles, los cuales se encuentran diferenciados en dos categorías, el primero de Data Center y Servicios Complementarios y el segundo de Software como Servicio (SaaS), Plataforma como Servicio (PaaS) e Infraestructura como Servicio (IaaS). De esta forma, mediante este convenio es posible acceder a diferentes proveedores *cloud* sin necesidad de levantar un proceso de licitación, lo cual facilita su accesibilidad.

Cabe destacar que, dentro del espectro de proveedores disponible, existen diferentes niveles de *expertise*. Algunos de proveedores actúan como "resellers" de servicios *cloud*, otros prestan servicios *cloud* con infraestructura propia en búsqueda de satisfacer los requerimientos del cliente (la Administración) de mejor manera[83]. Idealmente se sugiere relacionarse con un proveedor diverso, que contemple diferentes herramientas para poder entregar un mejor diseño de la solución a la problemática planteada.

Además de lo anterior, conviene tener presente que el documento "Buenas prácticas en materia de contratación de Servicios de Computación en la Nube (*Cloud Computing*) al interior

[80] Cabe destacar que a pesar de la existencia del convenio marco *Cloud* Computing and Datacenter, instituciones públicas siguen recurriendo a licitaciones en el Mercadopublico para suplir sus necesidades *Cloud*. En concreto, desde la puesta en marcha del marco *Cloud*, la corporación administrativa del Poder Judicial y el Metro S.A han licitado servicios *Cloud*.

[81] Artículo 6°, Decreto N°250, Aprueba Reglamento de la Ley Nº19.886 de Bases Sobre Contratos Administrativos de Suministros y Prestación de Servicios.

[82] Artículo 30 letra d), Contratos Administrativos de Suministro y Prestación de Servicios; Ley N°19.886.

[83] QUIROZ ARÁNGUIZ, Alonso Diego, cit. (n.15), p 95.

de la Administración del Estado: Un documento para el apoyo de toma de decisiones[84]" establece, en lo referido al proceso de contratación pública mediante este convenio marco, una serie de recomendaciones entre la que se destacan:

i) La posibilidad de redactar los Acuerdos Complementarios que se puedan considerar en dicho convenio.

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"*[85].

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

ii) Pedirles 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[86] y los artículos 8° y 15 del reglamento de dicha ley[87].

2. Acuerdo de Nivel de Servicio

Ligado al contrato de CN, podemos encontrar lo que se conoce como el acuerdo de nivel de servicio (en adelante también ANS), el cual, desde el punto de vista técnico, el estándar ISO 20000-1:2011 lo definió como "el acuerdo documentado entre el proveedor y el cliente que identifica los servicios y los objetivos del servicio. Puede estar incluido en un contrato o en otro tipo de acuerdo documentado[88]".

La finalidad de cualquier acuerdo de nivel de servicio es la de objetivar, a través de definiciones, parámetros, estándares u otras referencias, todo o parte del deber de diligencia del proveedor, y no siempre llevará asociadas compensaciones económicas. Por otra parte, puede incluir otros contenidos que, igualmente, den concreción contractual al impreciso concepto de diligencia profesional del proveedor, como la descripción del servicio que se presta.

---

[84] MINISTERIO 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, 2014).

[85] Convenio Marco de Data Center y Servicios Asociados, Licitación ID: 2239-17-LP11. Disponible en línea en: <http://bit.ly/1lCERsS

[86] Ley N°19.886 de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios, D.O. 30 de julio de 2003.

[87] 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.

[88] Definición de acuerdo de nivel de servicio adoptada por el estándar ISO/IEC 20000-1:2011 en relación a los servicios de administración de sistemas: "Documented ageement between the service provider and customer that identifies services provider and a supplier, an internal group or a customer acting as a supplier.(…) A service level agreement can be included in a contract or another type of documented agreement". Disponible en: https://www.iso.org/iso/catalogue_detail?csnumber=51986.

Es en este documento donde el cliente debe especificar (o en su defecto encontrar) las necesidades y estándares que requiere del servicio que se busca suplir. Dependiendo del cliente y del objetivo del sistema a desplegar, algunos niveles de requerimientos resaltan más que otros. En el caso de los organismos del Estado, dado su carácter público, tienen el deber legal de atender las necesidades públicas en forma continua y permanente, por lo cual la disponibilidad es una necesidad que debe ser tratada dentro de este documento.

Entenderemos pues, que el acuerdo de nivel de servicio recoge cualesquier propósitos a los cuales se compromete el proveedor relacionados con la prestación del servicio, como por ejemplo, los niveles de seguridad que pueda garantizar a través de la adopción de estándares de seguridad, los tiempos previstos para la recuperación de datos del cliente, la realización de copias de seguridad, la localización de los datos en determinadas ubicaciones geográficas o los compromisos sobre el tratamiento de los datos personales[89],es decir, es en este instrumento en donde se detallan los aspectos técnicos de las obligaciones del proveedor *cloud*.

Al respecto es necesario destacar que la Comisión Europea, consciente de la naturaleza global de la computación en la nube y de la complejidad de algunos acuerdos de nivel de servicio dependiendo del tipo de implementación y del modelo de servicio *cloud* prestado, publicó el documento *Cloud Service Level Agreement Standardisation Guidelines*, el cual establece conceptos y definiciones que pueden ser utilizados para crear acuerdos de nivel de servicio que se incluyan en contratos y que ha servido para elaborar el estándar ISO 19086-1:2016[90].

Teniendo en cuenta lo anterior, pasaremos a detallar a continuación los aspectos relevantes a considerar por parte de las instituciones públicas a la hora de la redacción y suscripción de un contrato cuyo objeto es la prestación de servicios de *cloud computing*.

3. El contrato de *Cloud Computing* suscrito por la Administración

a) Generalidades

Respecto del tema que entraremos a analizar, debemos aclarar que, sin perjuicio de lo que aquí se mencione, las partes son libres, en razón del principio de autonomía de la voluntad, para darse la regulación que deseen, siempre que se encuadre dentro de los límites que el propio ordenamiento jurídico establece. Todo esto en el entendido de que nos encontramos ante actos administrativos de gestión, en virtud del cual la Administración se despoja de su poder y se pone a nivel de los particulares, y actúa como simple sujeto de derecho reflejando una situación contractual[91].

Por otra parte, es necesario advertir que en un trabajo como este solo podemos enunciar en términos generales las cláusulas propias de un contrato *cloud* celebrado por la

---

[89] ROSELLÓ, Francisca María, cit. (n.23), p.233.

[90] El documento del subgrupo de expertos en acuerdos de nivel de servicio de la *Cloud Computing Strategy* se publicó el 24 de junio de 2014. Este documento sirvió de referencia para la elaboración del estándar ISO 19086-1:2016 *Cloud Service Level Agreement Standardisation Guidelines* (en línea). Disponible en: https://ec.europa.eu/digitalagenda/en/news/cloud-service-level-agreement-standardisation-guidelines.
ISO 19086-1:2016. Disponible en: https://www.iso.org/standard/67545.html.

[91] OELCKERS CAMUS, Osvaldo, *En torno al concepto de acto administrativo*, en *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso* 3 (1979), p. 138.

Administración del Estado, las que deberán ser adaptadas a las específicas necesidades del órgano público respectivo.

Formuladas estas ideas, analizaremos a continuación las cláusulas más importantes a incluir en esta clase de contrato.

b) Individualización de las partes

Al igual que en todo contrato, es necesario determinar las partes a quienes afectarán sus cláusulas, haciendo constar la capacidad de cada una de ellas. Es importante en el caso de los proveedores de esta clase de servicios, individualizar los representantes que obren por ellos acreditando su personería.

En este sentido, es importante notar que, en esta clase de industria, frecuentemente 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.

Esto importa en cuanto ciertos autores extranjeros, para los contratos de Nube en los que se pone a disposición del cliente almacenamiento de espacio y aplicaciones, ha defendido que el oferente de estos servicios no debe responder si ha adquirido las aplicaciones y/o el hardware y éstos presentan luego deficiencias, invocando que en muchas ocasiones ni siquiera tiene el conocimiento necesario para reparar las citadas deficiencias[92]. Este desconocimiento se debe "al hecho que es el prestador del servicio *cloud,* y no el tercer oferente, quien realmente ejecuta la obligación de llevar adelante el servicio, almacena información, protege la confidencialidad de los datos del órgano contratante, entre otras labores"[93].

Si bien esta postura eventualmente podría sustentarse en el caso de productos como hardware y software y determinados servicios (por ejemplo, mantenimiento o soporte), en el caso de los servicios *cloud* estamos a una situación sumamente diversa: en base al carácter de contrato *intuito personae* y de tracto sucesivo[94] de los contratos de prestación de servicios *cloud*, es 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[95].

c) Definiciones

---

[92] VIDAL PORTABALES, José Ignacio, *Cloud Computing y su Problemática Jurídica*, en GARCÍA VIDAL, Ángel (director), *Actas de Derecho Industrial y Derecho de Autor* (Madrid, Editorial Marcial Pons, 2011), p.459

[93] MINISTERIO 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, 2014), p.23.

[94] En este sentido, véase sección I, "Características de los contratos de servicios de computación en la nube".

[95] MINISTERIO 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, 2014), p.23

Pueden definirse de común ciertos conceptos, de manera que las palabras técnicas que se utilicen tanto en el contrato como en sus apéndices signifiquen lo mismo para ambas partes, asunto de gran utilidad en esta clase de contratos en donde el uso de palabras técnicas ligadas a la informática es frecuente[96].

d) Objeto del Contrato

En el contrato deben quedar claramente la o las tareas informáticas que serán objeto del mismo, de modo que no quepan dudas de la obligación correlativa del proveedor *cloud*.

En este punto cobra relevancia el deber de información que tiene el proveedor *cloud*, el cual es correlativo al deber de colaboración del cliente (la Administración), ambos analizados previamente, los cuales deben quedar convenientemente estipulados en el contrato, con el fin de facilitar el cumplimiento de los objetivos planteados por las partes al celebrar el contrato[97].

e) Duración del Contrato

Hemos mencionado que el contrato de CN es de tracto sucesivo. Por ello es necesario indicar todo el tiempo durante el cual las partes estarán vinculadas por sus estipulaciones, el que por regla general es extenso, dada la complejidad del objeto.

En cuanto a la iniciación del contrato, se debe establecer una fecha exacta, fijando desde ya la fecha de transición e inicio propiamente tal. En lo que respecta a la duración del contrato, ésta dependerá de lo que se acuerde por las partes en virtud de las necesidades del cliente y del riesgo que deba asumir el proveedor *cloud*, aunque se considera importante que los órganos de la Administración del Estado mantengan la libertad de poner término a esta clase de contratos. De esta forma, "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"[98]. Esta libertad facilita al órgano que contrata el poder cambiar a otro proveedor en el supuesto de ser necesario. Además, podría decirse que se configura como un incentivo para el prestador del servicio, en orden a que tome medidas adicionales para mantener a su cliente.

f) Asunción de Riesgos Informáticos

Tal como sostiene "ChileCompra", la migración de servicios y aplicación a entornos de *cloud computing* debe ser objeto de un análisis de riesgos que, en función de la sensibilidad de los datos y el nivel de amenazas, determine, en primer lugar, la conveniencia de esta solución y, en caso afirmativo, los controles y salvaguardas que deben implementarse para mitigar los riesgos hasta un nivel que pueda considerarse como aceptable[99].

---

[96] En este sentido véase sección II, "Infraestructuras *Cloud*".
[97] En lo que respecta a estos deberes, puede verse sección II "Aspectos Jurídicos Generales".
[98] MINISTERIO 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, 2014), p. 44.
[99] Asistente para los servicios tecnológicos del *Cloud* Store del Estado, *Cloud* y Data Center.
Visible en internet:

En concordancia con lo anterior, los usuarios de servicios *cloud* necesitan garantías de que los riesgos asociados al almacenamiento de sus datos y ejecución de sus aplicaciones en estos ambientes son comprendidos y gestionados adecuadamente, en este sentido, se debería prestar particular atención a que los criterios de seguridad utilizados por el prestador del servicio sean reconocidos, transparentes y verificables.

Bajo esta lógica, conforme al nuevo documento elaborado por el Ministerio Secretaría General de la Presidencia, "Buenas prácticas en materia de contratación de Servicios de *Cloud Computing* al interior de la Administración del Estado, versión 2.0", es posible mencionar algunos principios de seguridad que los prestadores de servicios *cloud* debiesen cumplir[100]:

i) Controles de acceso, identidad y autenticación robustos: El acceso a todas las interfaces de servicio debería restringirse a personas autenticadas y autorizadas para prevenir cambios no autorizados en el servicio del consumidor, robo o modificación de datos o la denegación de servicio.

ii) Protección de los activos de información y datos, tanto en tránsito como en reposo: Los centros de datos deberían estar construidos bajo estándares reconocidos de seguridad, para que los datos, activos y redes estén adecuadamente protegidos contra la manipulación, espionaje, pérdida, daño o incautación. Deberían existir criterios claros sobre el uso de controles criptográficos sobre los datos. Asimismo, debería existir una política clara de retención de datos, y plazos específicos para su posterior eliminación.

Algunas instituciones públicas ya hicieron parte esta recomendación en su operatividad como, por ejemplo, el Servicio de Impuestos Internos (SII), que con el propósito de garantizar que todas las transacciones efectuadas entre los contribuyentes y su sitio Web, viajen en forma segura y confidencial, tiene implementado el sistema SSL (Secure Socket Layer), a través del cual la información transmitida viaja en forma encriptada, esto es, por medio de un sistema de codificación imposible de descifrar. Lo anterior significa que toda su información personal y tributaria, no podrá ser leída ni capturada por terceros mientras viaja por la red. La calidad de sitio seguro está garantizada a través del certificado de seguridad que ha sido otorgado por Verisign, Inc.

iii) Seguridad Operacional, del Personal y Proveedores: El Prestador de Servicios debería tener procesos y procedimientos establecidos para garantizar la seguridad en la operación del servicio, incluyendo la gestión de su personal y proveedores.

Los contratos de prestación de servicios de *cloud computing* deben especificar las medidas técnicas y organizativas que el prestador de servicios tiene previsto implantar para garantizar la seguridad de los datos. Asimismo, los especiales requisitos de disponibilidad, confidencialidad e integridad que puedan requerir ciertos servicios electrónicos prestados por las Administraciones Públicas deben reflejarse en el contrato mediante un acuerdo de nivel de

---

http://www.mercadopublico.cl/Portal/Modules/Site/TiendaCloud/pag_condiciones_gral.aspx

[100] MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA, *Buenas prácticas en materia de contratación de Servicios de Cloud Computing al interior de la Administración del Estado,* Versión 2.0 (Santiago, 2018), p.12. Disponible en: https://cdn.digital.gob.cl/Guia+Cloud+v2.pdf. [Visitado el 13 de enero de 2020]

servicio (ANS) en el que se especifiquen los indicadores de calidad de servicio que van a ser medidos y los valores mínimos aceptables de los mismos.

En ciertos casos, la complejidad de los servicios contratados puede aconsejar la designación de un responsable del contrato en los términos previstos según las normativas vigentes, con el fin de asegurar la correcta realización de la prestación pactada. No obstante, la designación de dicha figura no modifica el régimen de obligaciones y responsabilidades al que está sujeto el responsable del tratamiento en materia de protección de datos de carácter personal. La prestación de servicios por encargados de tratamiento en *cloud* debería quedar claramente identificada en el documento de seguridad. Asimismo, el acceso a la información debe reunir un nivel de medidas de seguridad equivalente al de los accesos en modo local, en la forma dispuesta por las normativas vigentes[101].

iv) Gestión segura de los clientes, incluyendo separación de los mismos y promoción del uso seguro del servicio: El Prestador de Servicios debería promover el uso seguro de sus servicios por parte de sus clientes, transmitiendo de forma clara las responsabilidades de cada parte cuando se use un servicio en la nube, para que este uso permanezca seguro y para que los datos de sus clientes estén adecuadamente protegidos. Parte de las responsabilidades del Prestador de Servicios en este ámbito es tomar las medidas adecuadas para garantizar la separación lógica o física de los clientes, según corresponda.

v) Marco de gobernanza: El Prestador de Servicios de servicios debería tener un marco de gobernanza de seguridad que entregue suficiente coordinación y dirija su enfoque en la gestión del servicio y la información que éste contiene.

vi) Reporte de incidentes de seguridad: El Prestador de Servicios debería transparentar al cliente información detallada y oportuna sobre los incidentes de seguridad que afecten el servicio contratado o a la información de éste y adoptar medidas para mitigar los posibles daños resultantes.

La verificación de estos criterios de seguridad, en caso de ser posible, pueden incluir cláusulas tendientes a que los órganos contratantes, puedan auditar las políticas, procesos, sistemas y servicios del prestador del servicio *cloud*.

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)"[102].

---

[101] Asistente para los servicios tecnológicos del *Cloud* Store del Estado, *Cloud* y Data Center
Visible en internet:
http://www.mercadopublico.cl/Portal/Modules/Site/TiendaCloud/pag_condiciones_gral.aspx

[102] MINISTERIO 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, 2014), p.41.

g) Posibilidad de subcontratación por parte del prestador de servicios cloud

Es necesario analizar la posibilidad de que en el contrato de CN se autorice al prestador de servicios *cloud* a celebrar un subcontrato, en orden a que una tercera persona realice ciertas tareas que en virtud de la externalización (contrato principal), le corresponden al prestador de servicios *cloud computing*.

En este sentido conviene recordar lo mencionado respecto a los artículos 14 y 15 de la Ley N°19.886, de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios, así como los artículo 74 y 76 del reglamento del mismo cuerpo legal, los cuales, a grandes rasgos, consagran la posibilidad de subcontratación de los servicios pero solo en forma parcial; además, conforme a la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), se deberían evitar las situaciones en las que un proveedor de servicios en la nube subcontrate los servicios pertinentes a un tercero. Al menos se deben incluir en el acuerdo de servicios, declaraciones y garantías sobre posibles subcontratistas[103].

En el caso que efectivamente se permita la subcontratación de los servicios por parte de la Administración, deben quedar establecidas claramente la o las tareas informáticas que serán objeto del mismo, de manera que no existan dudas acerca de la obligación correlativa del contratista, que el tratamiento de datos de carácter personal se ajuste a las instrucciones de la administración que actúa como responsable del tratamiento. Además, el órgano contratante debe asegurarse de 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[104].

h) Cláusulas de confidencialidad

Uno de los mayores riesgos del contrato de CN celebrado por la Administración del Estado, es la pérdida de confidencialidad a la que se ve expuesta esta última al entregar a un tercero las tareas destinadas a manejar y administrar la información, la que en algunos casos puede tener el carácter de reservado. Es importante señalar que la relación entre las partes del contrato *cloud* debe ser la de una cooperación para la consecución de fines que pasan a ser comunes, por lo que ambos involucrados en la celebración de este contrato, tienen el deber

---

[103] 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), p.46.
Disponible en línea:
https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/es_governmental_clouds_enisa.pdf [Visitado el 13 de enero de 2020]

[104] MINISTERIO 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, 2014), p.49.

ético-jurídico de abstenerse de ejecutar acciones que puedan causar perjuicio a su contraparte[105], como lo sería, por ejemplo, la filtración de información confidencial.

Sin embargo, no basta con confiar en el cumplimento de este deber ético-jurídico, por lo que se hace necesario incluir en el contrato respectivo ciertas cláusulas que aseguren la confidencialidad de la información que estará a cargo o a disposición de la empresa que presta servicios de *cloud*, específicamente señalando la sensibilidad de los datos a tratar, incluyendo si se trata de datos personales, datos reservados o datos referentes a la seguridad nacional, que podrían tener exigencias específicas que deben ser analizadas caso a caso, pudiendo ser necesario descartar algunos modelos de servicio o implementación en la nube. Lo anterior importa sobre todo respecto de la información catalogada como reservada (art. 21 Ley N°20.285).

Respecto al tratamiento específico de esta clase de información, deben siempre existir cláusulas de confidencialidad[106]acerca de los datos almacenados en el servicio *cloud*, prohibiendo que dicha información sea informada a terceros y que contemplen que esta información sea tratada por el prestador únicamente para la ejecución del contrato[107], además de cumplir con las demás previsiones legales, como por ejemplo lo establecido en el artículo 16 del decreto N°83 Sobre Seguridad y Confidencialidad de los Documentos Electrónicos, que señala que la salida desde un sistema de un documento electrónico que está clasificado como reservado o secreto, deberá tener una etiqueta apropiada de clasificación en la salida[108].

En este mismo sentido, es conveniente establecer en las respectivas bases de licitación, la exigencia a los oferentes relativa a que en el evento de ser adjudicados, suscriban una declaración jurada que contenga un compromiso de confidencialidad, además de establecer técnicas robustas de cifrado[109] (como, por ejemplo, bajo estándares tales como AES de 128, 192 o 256 bits) tanto a los datos en tránsito como de los datos almacenados. Estas se constituyen como medidas necesarias para garantizar la confidencialidad. Asimismo, el contrato de prestación de servicios en la nube debe contemplar la realización de copias de

---

105 INOSTROZA SÁEZ, Mauricio, cit. (n.28), p.157.

106 A modo de ejemplo, el minsegpres nos brinda una cláusula relativa a la protección de la confidencialidad, la cual puede configurarse de la siguiente manera: *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.* MINISTERIO 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, 2014), p. 54.

107 MINISTERIO 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, 2014), p. 34.

108 Decreto N°83, sobre Seguridad y Confidencialidad de los Documentos Electrónicos, art. 16.

109 Se define como encriptación de datos el proceso por el cual se aumenta la seguridad de información digital, representada tanto con un archivo como con un mensaje u otras formas de presentación. Dentro de este proceso, el contenido se protege bajo un sistema que se puede definir como de cifrado, codificado o encriptado, dado que todos los términos vienen a representar el mismo nivel de protección. Para conseguir esta seguridad se usa un algoritmo que evita que esta información o archivos puedan ser accedidos por personas externas que no dispongan de la contraseña específica de acceso. La información o las operaciones que se encriptan disponen de los mejores niveles de seguridad y son capaces de proteger operaciones de compra online, datos sensibles como el número de la tarjeta de crédito o la dirección de una persona.

respaldo de la información de forma que se garantice la plena disponibilidad e integridad de los datos almacenados[110].

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[111].

i) Cláusulas relativas a la integridad de la información

La integridad y la disponibilidad de los datos son elementos esenciales en la prestación de los servicios de computación en la nube. La integridad de la información se define como "la seguridad de que la información almacenada o transportada sea modificada por quienes están autorizados a hacerlo"[112]. Esto implica que no se debiese perder o corromper información ni por errores del sistema ni por terceros. Por ejemplo, conforme a lo establecido por "mercadopúblico", se debería proceder a la conservación de los documentos electrónicos en el formato en el que hayan sido elaborados, enviados o recibidos, y preferentemente en un formato correspondiente a un estándar abierto que preserve a lo largo del tiempo o la integridad del contenido de los documentos, de la firma electrónica y de los metadatos que lo acompañan[113]. En este sentido, el contrato debe estipular expresamente el deber de velar por la calidad de los datos, rectificándolos o actualizándolos cuando se advierta que son erróneos y, por supuesto, eliminándolos tan pronto hayan perdido vigencia, caduquen o cuando termine el contrato. Del mismo modo, hay que estipular la obligación de avisar a los terceros a quienes les ha transmitido los datos, el hecho de la eliminación o modificación que experimenten aquellos que están en su registro[114].

La integridad de la información se encuentra asociada a diferentes medidas que los proveedores *cloud* deben cumplir para poder garantizarla. Para esto, protocolos y política de protección de infraestructura son aplicadas, redes se deben mantener seguras e impenetrables, y hardware debe ser protegido en caso de sobrecargas o alguna otra causa que interfiera en su correcto funcionamiento. Estas medidas se confirman a través de certificados que los proveedores adquieren para validar la calidad de sus instalaciones. Un ejemplo de certificación seria la norma ISO 27000 sobre la seguridad de la información.

---

[110] Asistente para los servicios tecnológicos del *Cloud Store* del Estado, *Cloud* y *Data Center*. Disponible en línea: http://www.mercadopublico.cl/Portal/Modules/Site/TiendaCloud/pag_condiciones_gral.aspx

[111] MINISTERIO 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, 2014), p.28.

[112] 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), p.46. Disponible en línea en: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/es_governmental_clouds_enisa.pdf [Visitado: 13 de enero de 2020] p. 84.

[113] Asistente para los servicios tecnológicos del *Cloud* Store del Estado, *Cloud* y Data Center. Disponible en línea: http://www.mercadopublico.cl/Portal/Modules/Site/TiendaCloud/pag_condiciones_gral.aspx

[114] HERRERA BRAVO, Rodolfo, cit. (n.55), p. 55.

j) Cláusulas de propiedad intelectual

Anteriormente, al analizar la legislación aplicable a los servicios de *cloud computing*, se hizo referencia al hecho de que a la hora de contratar esta clase de tecnología es necesario tener a la vista la Ley N°17.336, Sobre Propiedad Intelectual, en el sentido que el órgano contratante debe poner atención en mantener los derechos de propiedad intelectual de los documentos y demás informaciones que se suben a la nube, velando que el prestador de servicios respete lo establecido por la ley chilena con respecto a la propiedad intelectual[115].

Sin perjuicio de las previsiones legales, es recomendable que a nivel contractual, se ponga especial énfasis de que es el titular de los derechos de propiedad intelectual sobre la documentación y bases de datos quien ampara que se suban estos elementos al servicio *cloud* y que éstas solo podrán ser utilizadas por el proveedor del servicio *cloud* para efectos de la ejecución del contrato, y cualquier otro uso debiera contar la autorización escrita del órgano contratante[116]. También es importante especificar que independiente del tipo de información, todo debe ser considerado como propiedad intelectual de la institución. Además, consideramos recomendable estipular cláusulas correspondientes a licencia de uso restringido y prohibiciones sobre infracciones de derechos de propiedad intelectual y realización de ingeniería inversa[117]. Adicionalmente, y siguiendo los criterios formulados por la ENISA[118], se estima aconsejable negociar cláusulas en donde el prestador del servicio *cloud* es penalizado por la violación a los derechos de propiedad intelectual.

k) Cláusulas de exclusividad

Dada la estrecha vinculación que se forma entre las partes como consecuencia del contrato de *cloud computing* y el acceso a información reservada o confidencial, o bien, debido al manejo de datos de carácter personal, además de las cláusulas de confidencialidad, puede ser necesario establecer ciertos pactos de exclusividad, en virtud de los cuales se restrinja a la entidad que presta los servicios *cloud* la posibilidad de celebrar contratos de la misma o similar naturaleza con ciertas empresas, a fin de resguardar la confidencialidad de la información. Este pacto será más o menos amplio, pero no puede llegar al punto de prohibir absolutamente la

---

115 A este respecto conviene tener a la vista las consideraciones realizadas respecto a la Ley N°17.336, sobre Propiedad Intelectual.

116 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: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/cloudbestpractices.pdf [Consultado el 20 de diciembre de 2019].

117 El proveedor Google establece unas condiciones comunes para todos sus servicios (Gmail, YouTube, Buscador Google, etc.). En ellas se concede esta licencia a sus usuarios: "Google te concede una licencia personal mundial, libre de royalties, intransmisibles y no exclusiva para usar el software que se te proporcione como parte de los servicios. No podrás copiar, modificar, distribuir, vender ni prestar ninguna parte de nuestros servicios, ni extraer el código fuente de dicho software, salvo si la legislación prohíbe dichas restricciones o si tienes consentimiento de Google por escrito". Disponible en http://www.google.com/police/terms/.

118 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), p. 46.
Disponible en línea en:
https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/es_governmental_clouds_enisa.pdf [Consultado el 13 de enero de 2020] p. 109.

realización de una actividad económica, atendiendo lo dispuesto en el art. 19 n°21 de la Constitución Política de la República[119].

l) Adaptabilidad del clausulado a las necesidades de la Administración

Esta especie de contrato posee la característica de ser flexible, no solo en lo que se refiere a las tecnologías aplicables, sino también en cuanto a la posibilidad de adaptar los límites de la labor del prestador de servicios *cloud*. De esta forma se puede pactar la adecuación de su actividad, dentro de ciertos límites, a las condiciones que necesite el organismo de la Administración para llevar a cabo su respectiva labor, de manera que este último pueda exigir una mayor intensidad de trabajo al primero cuando aumente su nivel de actividad por las causas establecidas en el contrato.

En este mismo sentido, se puede fijar una norma flexible que, acorde con la asunción de los riesgos informáticos por parte del prestador de servicios, dé a esta última facultad para desarrollar nuevas tareas, en virtud de las necesidades que vayan surgiendo, sin que se deba incurrir en los gastos que conlleva una modificación del contrato. Se debe tratar, en todo caso, de tareas muy rutinarias y menores, pues la realización de nuevas tareas de mayor envergadura debe implicar una modificación del contrato, ya que al constituir las funciones informáticas el objeto de la convención, deben estar necesariamente incluidas en ella[120].

Lo anterior se vincula con la elasticidad del servicio, en virtud de la cual es necesario tener especial consideración el riesgo presupuestario que conlleva una planificación inadecuada de la capacidad. Especialmente en infraestructuras *cloud*, dada su naturaleza de servicio bajo demanda, no es difícil llegar a un punto en el que se pide más capacidad de lo presupuestado y como consecuencia, el costo asociado también podría exceder el presupuesto original, por lo que se debería tomar medidas adecuadas para que esto no ocurra, tales como hacer una buena planificación de la capacidad, reservar capacidad con anticipación o adoptar otras medidas que permitan definir en el contrato valores de crecimiento de manera flexible, que no obliguen necesariamente a realizar un nuevo proceso de compra.

Para establecer el costo estimado del proyecto a contratar se debería tomar en cuenta la demanda estimada del servicio, lo que nos obliga a identificar en detalle las distintas actividades asociadas y sus plazos, para poder determinar los recursos involucrados en cada una de ellas. Considerando que los recursos necesarios en ambientes *cloud* pueden ser vastamente diferentes a los recursos tradicionales, en especial si comparamos modelos tradicionales con modelos PaaS o SaaS[121].

m) Prohibición de modificación unilateral

En muchas ocasiones cabe la posibilidad de encontrarse con términos y condiciones, en donde al prestador de servicios *cloud* se le otorga la facultad de modificar unilateralmente los términos de contratación.

---

119 INOSTROZA SÁEZ, Mauricio, cit. (n.28), p. 160.

120 INOSTROZA SÁEZ, Mauricio, cit. (n. 28), p.162.

121 MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA, *Buenas prácticas en materia de contratación de Servicios de Cloud Computing al interior de la Administración del Estado,* Versión 2.0 (Santiago, 2018), p.13.

Lo anterior, no puede ser aceptado por el órgano contratante. Ello porque, de acuerdo a la propia 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[122].

Por lo mismo es recomendable estipular en el contrato el hecho relativo a que cualquier modificación deberá realizarse de común acuerdo por las partes del contrato, de forma expresa y por escrito, debiendo aprobarse por el acto administrativo correspondiente[123].

ñ) Cláusula de responsabilidad

Un aspecto muy importante a regular en cualquier contrato, es lo relativo a la responsabilidad emanada de algún acto que pueda causar daño. En este sentido, cada parte debe responder por todos aquellos actos dolosos o culposos por medio de los cuales se cause un perjuicio a su contraparte o a terceros, de acuerdo a las normas que se establezcan en el contrato y las que resulten aplicables de acuerdo a la regulación positiva vigente.

En lo que respecta a las normas contractuales, éstas pueden ir en varios sentidos. Así, por ejemplo, se suele explicitar la responsabilidad que cabe por ciertos actos, aplicando allí las reglas generales de responsabilidad, clarificando de este modo las dudas que pudieran surgir al respecto y evitando conflictos posteriores en cuanto a determinar la parte que debe responder por tales acciones[124].

Lo relativo a esta materia es importante tenerlo a la vista, en cuanto que dado la naturaleza de la tecnología *cloud computing*, todo el procedimiento relativo al almacenamiento, procesamiento y transferencia de la información y datos, concierne al mismo proveedor *cloud*, en el sentido que es este quien posee completo acceso a ella, y por ende, es el proveedor quien se hace responsable de velar por el mantenimiento del acceso de la información del cliente evitando que esta caiga en manos de personal no autorizado[125] (todo esto, sin perjuicio de la responsabilidad que le quepa a la Administración del Estado[126]).

En lo tocante a la responsabilidad que afecta al prestador de servicios, como se mencionó, es posible explicitar la responsabilidad que le cabe por ciertos actos, de esta forma

---

122 Véase CONTRALORÍA GENERAL DE LA REPÚBLICA, Dictamen N°26.479 de 20 de agosto de 1996.

123 MINISTERIO 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, 2014), p.41.

124 INOSTROZA SÁEZ, Mauricio, cit. (n.28), p. 164.

125 Aunque es importante dejar en claro que el proveedor de servicios *cloud* no tiene la obligación de realizar búsquedas activas o indagación de datos migrados por los clientes. Además, quedará a su discrecionalidad la suspensión del servicio o la retirada de contenidos ilícitos del usuario, y la instauración de mecanismos que permitan a otros usuarios avisar al proveedor de la existencia de contenidos lesivos. Por nuestra parte, consideramos recomendable para el prestador de servicios, la adopción de mecanismos que permitan a otros usuarios informar sobre la difusión, a través de servicios *cloud*, de eventuales contenidos ilícitos, y que se lleve a cabo la efectiva investigación interna de tales avisos remitidos por otros usuarios, a modo de buenas prácticas, y como demostración de su deber de diligencia profesional ante eventuales reclamaciones de responsabilidad.

126 A este respecto véase, sección III. Normativa Aplicable a los Servicios de *Cloud Computing* utilizados por la Administración del Estado. Ley N°18575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

se puede establecer a vía ejemplar, que el prestador de los servicios *cloud* será responsable del uso de información del cliente para un fin distinto al establecido en el contrato, de la pérdida o difusión no autorizada de información, del cumplimiento de las medidas de seguridad estipuladas, de las medidas inadecuadas que haya adoptado para el ejercicio de sus labores, etc., debiendo en todos estos casos responder al cliente por los perjuicios que , dolosa o culposamente , tales acciones le hayan ocasionado[127].

De esta forma, para evitar el surgimiento de responsabilidad, el prestador de los servicios *cloud*, debe establecer garantías propias para velar por la seguridad de sus sistemas informáticos, entendiendo estas como el conjunto de reglas a las que se compromete, siendo definidas dichas garantías en el mismo contrato vinculante o bien en el respectivo Acuerdo de Nivel de Servicio (ANS). En este instrumento, el proveedor debe estipular su completo accionar con la información, las personas o entidades que tendrán acceso a esta información almacenada, los protocolos y mecanismos utilizados para resguardar dicha información de posibles violaciones de terceros, estableciendo medidas que brinden garantías de resguardo, como por ejemplo, el establecimiento de mecanismos de seguridad de red (implementación de cortafuegos y otras tecnologías que aseguren los accesos al servicio desde la red global), mecanismos de seguridad lógica (software de protección ante ataques al sistema y de prevención o paliación de errores), segregación de datos, encriptado a través de algoritmos, entre otros[128].

Tratándose de los casos en donde se maneja información de carácter personal, regulada por la Ley N°19.628, es necesario realizar un paréntesis, en el sentido de que como se mencionó previamente[129] a la relación existente entre el cliente y el prestador del servicio, se le aplica la figura del mandato, en este sentido, el mandatario, al igual que el responsable del registro, responderá hasta la culpa leve en su obligación de cuidar los datos personales, es decir, deberá indemnizar los daños que ocasione por la falta de la debida diligencia y cuidado que se emplea ordinariamente en los negocios propios, sin perjuicio del establecimiento de cláusulas que hagan civilmente responsable al prestador del servicio *cloud* acerca de la filtración o uso inadecuado de los datos personales que le son confiados[130].

Continuando con el análisis, en aplicación del inciso final del art. 1547 del Código Civil, las partes pueden modificar contractualmente las normas legales de responsabilidad, las cuales deben tender a que el prestador de servicios *cloud* responda de un grado mayor de culpa del que le corresponde (lo normal en los contratos conmutativos como éste es que las partes respondan por culpa leve), estableciendo que en determinados casos responda incluso del caso fortuito o fuerza mayor, que responda de los perjuicios imprevistos, etc.[131]. También se pueden pactar ciertos casos de responsabilidad objetiva, en virtud de los cuales el prestador de servicios responda por fallas del sistema o falta de servicio sin necesidad que medie culpa o dolo de éste. Estos casos de responsabilidad objetiva que afecta al prestador de servicios *cloud*,

---

127 INOSTROZA SÁEZ, Mauricio, cit. (n.28), p.162.

128 Todo esto sin perjuicio de la responsabilidad legal que surja en el marco del artículo 23 de la Ley N°19.688, el cual establece que los responsables del registro o banco de datos personales (prestador del servicio *cloud computing*) deberán indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos.

129 A este respecto conviene tener a la vista las consideraciones ya realizadas respecto a la ley N° 19.628, Sobre la Protección de la Vida Privada o Protección de Carácter Personal.

130 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), p.33.

131 INOSTROZA SÁEZ, Mauricio, cit. (n.28), p.164.

deben estar expresamente pactados, pues si no lo están, se deben aplicar las reglas generales de responsabilidad, las cuales siguen, como es sabido, un sistema subjetivo y por ende, será necesario probar dolo o culpa[132].

Independientemente de lo mencionado, es importante señalar que si bien es posible pactar cláusulas que modifiquen el régimen de responsabilidad que tiendan a que el prestador de los servicios *cloud* responda por un grado mayor de culpa que el que le corresponde, no es posible por parte de la Administración pactar cláusulas que limiten o exoneren la responsabilidad civil del prestador de los servicios 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[133]. En este sentido, cabe destacar que, de conformidad a la jurisprudencia administrativa de la 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[134].

o) Cláusulas penales

Vinculado al punto anterior, es posible y a la vez recomendable avaluar de forma convencional y anticipada los perjuicios producto de un incumplimiento o cumplimiento tardío de las obligaciones que impone a las partes el contrato *cloud*. La forma más apta de cumplir este objetivo es estableciendo multas en el contrato, a modo de cláusula penal.

En lo referido a las causales de aplicación de las cláusulas penales, el establecimiento de estas dependerá de lo que mencionen las partes. Entre las posibles causales podemos mencionar la infracción de normas de seguridad, la subcontratación de ciertas tareas por parte del prestador *cloud* sin la autorización del cliente (la Administración), infracción de las normas de calidad de servicios, entre otros. Además de esto, resulta importante mencionar que, al avaluarse convencionalmente los perjuicios, aquella parte que tenga derecho a exigir la pena no tiene necesidad de probar los perjuicios[135] (art. 1542 del Código Civil).

Sin perjuicio de lo anterior, es importante que quede establecido en el contrato que la aplicación de una pena para el caso de incumplimiento o cumplimiento tardío, no exonera a la parte infractora de cumplir la obligación de que se trate, ya que, de otro modo, y de acuerdo al art. 1537 del Código Civil, la parte afectada solo podría pedir el cumplimiento o la pena, a su arbitrio, pero no ambas cosas. A este respecto se pueden pactar remisiones totales o parciales de la pena y/o de la indemnización de perjuicios que resulte aplicable, si la parte infractora cumple la obligación a satisfacción de la contraria en un tiempo prudente que se estipule.

---

132 INOSTROZA SÁEZ, Mauricio, cit. (n.28), p.165.

133 Esta práctica se extiende sobre todo en lo referido a la celebración de un contrato de nube pública entre particulares.

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

135 INOSTROZA SÁEZ, Mauricio, cit. (n.28), p. 167.

También puede pactarse que la parte afectada por la infracción quede facultada para pedir, a la vez, la pena y una indemnización de perjuicios, en aplicación del art. 1543 del Código Civil[136].

p) Legislación aplicable en caso de conflicto

A la hora de hablar de la legislación que resulta aplicable para dirimir las controversias que surgen en torno al contrato de CN, es importante considerar que en la nube los datos se sitúan en un lugar indeterminado, es decir, en un determinado servidor cuya ubicación física es desconocida por parte del responsable. Ahora bien, los datos necesariamente deberán estar situados en un servidor posicionado en algún punto del mundo[137]. Determinar tal ubicación es significativo por dos motivos, por un lado, debido a las consideraciones normativas que se plantean a propósito de la protección de datos de carácter personal, estadísticos, reservados, entre otros. Y, por otro, la determinación del órgano jurisdiccional competente para conocer de un determinado litigio.

La delimitación correcta de ambos aspectos resulta muy significativa, ya que cada sistema jurídico tiene establecido un sistema de normas en conflicto por el daño que, en su caso, se derive de la intromisión ilegítima en el derecho a la protección de datos, manifestado en el uso indebido o ilegítimo de estos derivado de la prestación de servicios tecnológicos en la nube, sobre la base de la existencia o no de una concreta relación jurídica entre el causante del daño, pudiendo el afectado determinar a la exigencia de responsabilidad civil contractual o extracontractual .

Una situación común que puede presentarse en los contratos de servicios *cloud* es la estipulación de cláusulas tendientes a establecer la aplicación de jurisdicción extranjera en virtud de los servicios contratados y que de acontecer una determinada disputa entre el cliente y el prestador del servicio, esta 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*.

En este sentido, en base a lo dispuesto por la Contraloría General de la República, los órganos de la Administración del Estado no tienen potestades públicas para someterse a las leyes y jurisdicciones extranjeras[138]. De esta forma surge la imposibilidad de contratar servicios que contemplen cláusulas de esta índole. Por lo mismo, tanto en las licitaciones como en los contratos se debe establecer expresamente que cualquier disputa entre las partes se somete a las leyes y tribunales chilenos[139].

---

136 INOSTROZA SÁEZ, Mauricio, cit. (n.28), p.168.

137 Tal extremo no debe servir, en modo alguno, para liberar a las empresas que prestan servicios de "computación en la nube" de la observancia de los principios de la protección de datos que amparan a los ciudadanos.

138 En este sentido, véase CONTRALORÍA GENERAL DE LA REPÚBLICA, dictamen N°32.447 de 11 de diciembre 1987 sobre la materia.

139 Un modelo de cláusula a emplear por los órganos de la Administración del Estado relativa a la legislación aplicable en lo relativo a la solución de disputas, puede ser:
El presente Contrato se rige por las leyes y normas jurídicas de la República de Chile.

Todo lo anterior no implica una prohibición para el uso de tecnologías *cloud* alojadas fuera del territorio nacional, ya que mientras la consideración mencionada relativa a no someterse a una jurisdicción extranjera sea contemplada, el uso de infraestructura extranjera queda a libre criterio de las propias instituciones. La toma de esta decisión debe ser basada en el tipo de información que se desea almacenar, los términos y condiciones que el proveedor en cuestión implementa y si estos abarcan los resguardos necesarios a dicha información. No es recomendable descartar a los proveedores *cloud* extranjeros sin revisar y entender que información es la que se desea guardar y si estos proveedores satisfacen los requerimientos en base a la información[140].

Por otro lado, la normativa de la seguridad de la información establece que cada servicio público debe tener sus propios protocolos de resguardo de información[141]. Esto implica que internamente muchas de las instituciones puedan tener como política la no utilización de "datacenters" fuera del país, por lo cual es necesario revisar los protocolos particulares de la organización para verificar el posible uso de estos servicios.

q) Terminación del contrato.

Lo normal será que el contrato termine por el término del plazo pactado para su duración. En este supuesto el contrato terminará de pleno derecho cuando se cumpla dicho plazo.

No obstante, como se mencionó al hablar del art.13 de la Ley N°19.886[142], el cual determina las causales de modificación o término anticipado aplicable a los contratos administrativos regulados mediante este cuerpo legal, es la propia ley la que establece una serie de causales destinadas a lograr este objetivo. Destaca principalmente el art. 13 letra b), que señala: "*el incumplimiento grave de las obligaciones contraídas por el contratante"*. Dicho incumplimiento se estima que sea de cierta magnitud, ya que no es posible que esta cláusula sirva para la Administración para "desprenderse" del prestador de servicios *cloud*. Importante es considerar que debiese informarse en el contrato, que, de suscitarse esta causal, será informado a la Dirección "ChileCompra" a fin de que ésta estudie su eliminación del Registro de Proveedores[143] y al resto de los órganos que actualmente son clientes del prestador del servicio *cloud* para que estos tomen las medidas que estimen pertinentes.

En esta misma línea, también resulta importante destacar el art. 13 letra e), que señala: "*las demás que se establezcan en las respectivas bases de la licitación o en el contrato"*.

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 someten irrevocablemente a la jurisdicción de los tribunales ordinarios de justicia de la ciudad y comuna de Santiago.

[140] QUIROZ Aránguiz, Alonso Diego, cit. (n.15), p.91.

[141] Para obtener un ejemplo, revisar las política seguridad de información del Ministerio del Interior y Seguridad Pública: http://www.seguridadpublica.gov.cl/media/2018/12/politicaseguridadinformacion.pdf ver Software NCH ISO 27001.

[142] A este respecto conviene tener a la vista lo ya mencionado respecto a la ley N° 19.886, de Bases sobre Contratos Administrativos de Suministros y Prestación de Servicios.

[143] 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.

Llegado a este punto, podemos mencionar alguna de las causales que se pueden establecer como aptas para producir (o dar derecho a pedir) la terminación[144] anticipada del contrato de *cloud computing*. Entre ellas encontramos:

i) Incumplimiento del deber de colaboración por parte de la Administración, en una magnitud que haga imposible o extremadamente gravoso el cumplimiento de las obligaciones del prestador de servicios *cloud*; la quiebra por parte de la empresa que presta servicios *cloud*.

ii) El tornarse innecesaria para la Administración la función externalizada.

iii) Cambio de propiedad de la empresa que presta los servicios: en esta hipótesis, se puede otorgar un derecho a la otra parte para elegir entre hacer subsistir el contrato en las nuevas condiciones o darlo por terminado, haciendo la salvedad que si opta por continuarlo, el nuevo propietario o socio mayoritario debe comprometerse a proseguir con el contrato en las mismas condiciones.

En concordancia con lo anterior, un elemento importante a considerar a la hora de finalizar este tipo de contratos, dice relación con la confidencialidad de los datos más allá de la terminación del contrato. Tras el estudio de diversos "contratos *cloud"*, no hemos encontrado proveedores que extiendan su obligación de mantener la confidencialidad de la información de forma posterior a la terminación del contrato y que abarque el plazo que comprende desde el momento del fin de la relación contractual hasta que ha tenido lugar el borrado seguro de la información. Por nuestra parte, recomendamos que se prolongue este deber como mínimo hasta que se haya hecho efectivo el borrado de los datos una vez facilitada la portabilidad de estos a otro proveedor o su devolución al cliente (la Administración), especialmente si se trata de datos de carácter personal o de índole confidencial, manteniendo el prestador de servicios *cloud* su obligación de confidencialidad de forma indefinida[145].

Por último, cabe destacar que más allá de que pueda contratarse esta clase de servicios, conforme a los criterios elaborados por la Contraloría General de la República, lo anterior no faculta a los servicios públicos a ceder o transferir tales datos personales al prestador del servicio[146]. Por lo mismo, se debe tomar especial cuidado de que al momento de poner fin a la

---

144 Recordemos que, en los contratos de tracto sucesivo, la resolución pasa a llamare "terminación", porque sus efectos no operan retroactivamente, sino que para el futuro.

145 A modo de ejemplo de esta clase de clausula podemos mencionar:

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. MINISTERIO 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, 2014), p.60

146 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.

relación contractual quede absolutamente claro que la propiedad sobre tales bases de datos se mantiene en el servicio público y, bajo ninguna circunstancia, son cedidas al prestador del servicio *cloud*[147].

r) Condiciones de recuperación de los sistemas de información

Por último, una vez terminado el contrato, la Administración debe quedar en condiciones de poder optar entre renovarlo, o bien contratar el mismo servicio con otro proveedor. En el último caso se deben establecer las condiciones según las cuales el proveedor de los servicios *cloud computing* transferirá el manejo de la función informática a otro prestador de servicios. En este sentido, y tal como lo establecen los contratos de C.S.S.A. (*Computing Service and Software Association*), a su término, los proveedores deben proporcionar "toda la asistencia razonable para cumplir este objetivo[148].

V. CONCLUSIONES

De la lectura de esta memoria, es posible apreciar que esta se constituye como una propuesta dirigida a ser una guía para la utilización de tecnologías *cloud computing* en el sector público chileno. Esta motivación surge por el hecho de la falta de documentos guías sobre esta dentro de las instituciones públicas chilenas y la escasez actual de bibliografía referentes al tema.

La contribución viene dada por la identificación de los elementos esenciales de esta clase de tecnología, extrayendo elementos comunes aplicables tanto a organismos públicos como privados, pero que, en la medida que se va desarrollando, se enfoca en los organismos de carácter público en una estructura lógica referida al establecimiento de criterios para una eventual implementación y/o evaluación de esta clase de tecnología dentro de la Administración. Para lograr este objetivo, en un primer término, se establecieron y detallaron algunos aspectos esenciales sobre la tecnología *cloud* desde un punto de vista técnico, lo cual tuvo como propósito ilustrar al lector sobre temática a abordar. Dentro de esta primera parte, especial relevancia cobra lo mencionado acerca del "contrato *cloud*" en lo referido a sus aspectos jurídicos generales, ya que sobre este tema se centra gran parte de este trabajo.

Posteriormente, para desarrollar esta memoria, fue necesario establecer y desarrollar los aspectos esenciales, a nivel legal, que una institución pública debiese considerar para la implementación y/o evaluación de esta clase de tecnología. Como el lector podrá extraer de la lectura de esta parte del documento, es posible extraer ciertas ideas interesantes, como lo son el hecho de que nuestra legislación en ningún caso prohíbe la utilización de esta clase de tecnologías, ni siquiera se preocupa de establecer parámetros para la utilización de nube pública o privada, quedando a criterio de cada institución su implementación en razón de la calidad de los datos que maneje, tomando los resguardos correspondientes. Adquieren así importancia los pactos detallados sobre la obligación de cumplimiento de nuestra normativa

[147] MINISTERIO 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, 2014), p.44.
[148] ROBERTSON, Ian, ROTHERY, Brian, *Outsourcing,* (Editorial Limusa S.A, México D.F, 1996), p. 70.

vinculada a esta clase de tecnología. De esta forma, es recomendable tener a la vista la serie de variables legales tratadas a lo largo del presente documento para de esta forma hacerse un panorama acerca de lo que es factible o no de hacer en el marco de las tecnologías *cloud computing*, en el entendido que la Administración, pese de que hablamos de tareas que suponen la externalización del tratamiento de datos e información, se configura a nivel legal indefectiblemente como responsable del resguardo de estos datos, en razón de lo expuesto y desarrollado en este documento, sin perjuicio de la responsabilidad a nivel contractual que concierne al proveedor *cloud*.

Por último cabe resaltar, que más allá del cumplimiento de la normativa vinculada a las tecnologías *cloud,* el establecimiento de cláusulas tendientes a fijar determinados aspectos relevantes como lo son la protección de datos o el establecimiento de reglas claras sobre distribución de la responsabilidad, o bien la jurisdicción aplicable en caso de conflicto, así como también la regulación a nivel contractual a la hora de la terminación del contrato, todas ellas desarrolladas en la última parte de este documento. Resulta clave en cuanto la ya mencionada escasa regulación y despreocupación existente en nuestro país por parte de las autoridades sobre la utilización de esta clase de tecnologías cuya utilización es cada vez más frecuente, siendo los esquemas de autorregulación concebidos con carácter complementario de una legislación que hoy por hoy no sigue el desarrollo de la nube, claves para eliminar parte de la conflictividad entre proveedores de nube y el cliente.

BIBLIOGRAFÍA

APARICIO VAQUERO, Juan Pablo, *La nueva contratación informática. Introducción al outsourcing de los sistemas de información* (Granada, Editorial Comares, 2002).

BARROS, Alejandro, *Servicios Compartidos (Share Services): la reforma faltante*. [Disponible en https://www.alejandrobarros.com/servicios-compartidos-share-services-la-reforma-faltante/].

BRANTT, María Graciela, MEJÍAS ALONZO, Claudia, *El contrato de servicios como categoría general en el derecho chileno. Su contenido y rasgos distintivos,* en *Revista Ius et Praxis* 24 (2018).

CORDERO VEGA, Luis, *Responsabilidad Extracontractual de la Administración del Estado* (Santiago, Ediciones Der, 2017).

DOMÍNGUEZ ÁGUILA, Ramón, *Teoría general del negocio jurídico* (Santiago, Editorial Jurídica de Chile, 1977).

HERRERA BRAVO, Rodolfo, *Cloud Computing y Seguridad: Despejando Nubes Para Proteger los Datos Personales*, en *Revista de Derecho Universidad San Sebastián* 17 (2011) 2.

HÜBNER VALDIVIESO, Agustín, *Filtraciones Masivas de Datos Personales. Algunas ideas sobre el deber de confidencialidad y el régimen de responsabilidad aplicable*, en *Revista de Derecho Universidad San Sebastián* 25 (2019) 9.

INOSTROZA Sáez, Mauricio Andrés, *El Contrato de Outsourcing Informático* (Memoria Universidad de Concepción, Concepción, Chile, 2004).

JIJENA LEIVA, Renato, *Delitos informáticos, Internet y derecho,* en RODRÍGUEZ COLLAO, Luis (coordinador), *Delito, pena y proceso* (Santiago, Editorial Jurídica de Chile, 2008).

JIJENA LEIVA, Renato, *Tratamiento de datos personales en el Estado y acceso a la información pública,* en *Revista Chilena de Derecho y Tecnología* 2 (2013) 2.

JOYANES, Luis, *Computación en la nube, estrategias de cloud computing en las empresas* (México DF, Editorial Alfaomega, 2012).

LÓPEZ JIMÉNEZ, David, *La computación en la nube o cloud computing examinada desde el ordenamiento jurídico español,* en *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso,* 24 (2013) 20.

MELL, Peter, GRANCE, Thimoty, *The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology*, U.S. Department of Commerce. [Disponible en https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf].

OELCKERS CAMUS, Osvaldo, *En torno al concepto de acto administrativo*, en *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso* 3 (1979).

QUIROZ ARÁNGUIZ, Alonso Diego*, Guía metodológica para el uso de cloud computing en instituciones públicas chilenas* (Santiago, Chile, Memoria Departamento de Informática, Universidad Santa María, noviembre 2016).

RIVERO, J., *Derecho Administrativo* (9° edición, Caracas, Editorial Metropolitana, 1984).

ROBERTSON, Ian, ROTHERY, Brian, *Outsourcing* (Editorial Limusa S.A, México D.F, 1996).

ROSELLÓ, Francisca María, *Cloud Computing. Régimen Jurídico Para Empresarios* (Pamplona, Editorial Thomson Reuters, 2018).

STELLA RODRÍGUEZ, Gladys, *Computación en la nube: algunas consideraciones técnico-jurídicas,* en *Revista Lex de la facultad de Derecho y Ciencias Políticas de la Universidad de Alas Peruanas,* 17 (2019) 23.

VIDAL PORTABALES, José Ignacio, *Cloud Computing y su Problemática Jurídica*, en GARCÍA VIDAL, Ángel (director), *Actas de Derecho Industrial y Derecho de Autor* (Madrid, Editorial Marcial Pons, 2011).

YANGUAS GÓMEZ, Roberto, *Contratos de conexión a Internet, Hosting y búsqueda* (Navarra, Editorial Thomson Reuters, 2012).

OTRAS FUENTES

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: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/es_governmental_clouds_enisa.pdf].

ASISTENTE PARA LOS SERVICIOS TECNOLÓGICOS DEL *CLOUD* STORE DEL ESTADO, *CLOUD* Y DATA CENTER. [Visible en internet:http://www.mercadopublico.cl/Portal/Modules/Site/TiendaCloud/pag_condiciones_gral.aspx].

BOLETÍN 412-07, Delito informático. [Disponible en https://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=412-07].

BOLETÍN E-GOBIERNO RED GEALC, *e-Gobierno en la nube,* edición 118, (2016) [Disponible en http://portal.oas.org/LinkClick.aspx?fileticket=Z6hkABKDNfs%3D&tabid=1729].

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).

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.

CONTRALORÍA GENERAL DE LA REPÚBLICA, Dictamen N°26.479 de 20 de agosto de 1996.

CONTRALORÍA GENERAL DE LA REPÚBLICA, Dictamen N°32.447 de 11 de diciembre 1987.

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

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: https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/2016/10/cloudbestpractices.pdf].

GRUPO DE TRABAJO IV (COMERCIO ELECTRÓNICO), CNUDMI, *Aspectos contractuales de la computación en la nube.* [Disponible en: https://undocs.org/es/A/CN.9/WG.IV/WP.142].

MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA, *Buenas prácticas en materia de contratación de Servicios de Cloud Computing al interior de la Administración del Estado,* Versión 2.0 (Santiago, 2018). [Disponible en: https://cdn.digital.gob.cl/Guia+Cloud+v2.pdf].

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, 2014). [Disponible en: http://www.guiadigital.gob.cl/sites/default/files/2014_02_28_GuiaCloud_v1.0.pdf].

FUENTES NORMATIVAS

Decreto N°83, sobre Seguridad y Confidencialidad de los Documentos Electrónicos. [Obtenido de: https://www.leychile.cl/Navegar?idNorma=234598].

Ley N°17.336, sobre Propiedad Intelectual. [Obtenido de: https://www.leychile.cl/Navegar?idNorma=28933].

Ley N°18575, Orgánica Constitucional de Bases Generales de la Administración del Estado. [Obtenido de: https://www.leychile.cl/Navegar?idNorma=29967].

Ley N°19.223, que Tipifica Figuras Penales Relativas a la Informática. [Obtenido de: https://www.leychile.cl/Navegar?idNorma=30590].

Ley N°19.628, sobre la Protección de la Vida Privada o Protección de Datos de Carácter Personal. [Obtenido de: https://www.leychile.cl/Navegar?idNorma=141599].

Ley N°19.886, de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios. [Obtenido de: https://www.leychile.cl/Navegar?idNorma=213004&buscar=19886].

Ley N°20.285, sobre Acceso a la Información Pública. [Obtenido de: https://www.leychile.cl/Navegar?idNorma=276363].