Dirección ChileCompra

DIRECCIÓN DE COMPRAS Y CONTRATACIÓN PÚBLICA

APRUEBA DIRECTIVA DE CONTRATACIÓN PÚBLICA N°32 RECOMENDACIONES PARA LA CONTRATACIÓN DE SERVICIOS EN LA NUBE.

RESOLUCIÓN EXENTA Nº 619-B /

SANTIAGO, 26 NOV. 2018

VISTOS: Lo dispuesto en la Ley N° 19.886, de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios; en el Decreto N° 250, de 2004, de Hacienda, que aprueba su reglamento; en la Resolución N° 1.600, de 2008, de la Contraloría General de la República, que establece normas sobre exención del trámite de toma de razón; y en el Decreto Supremo N° 1.599, de 2014, del Ministerio de Hacienda, que Nombra Directora Nacional de la Dirección de Compras y Contratación Pública.

CONSIDERANDO:

1. La función legal de la Dirección de Compras y Contratación Pública de asesorar a los organismos públicos en la planificación y gestión de sus procesos de compras, dispuesto en el artículo 30, letra a), de la ley N° 19.886.

2. La facultad de emitir orientaciones y recomendaciones generales, conducentes a difundir buenas prácticas y a fortalecer la probidad en las compras públicas, tanto por parte de los compradores como de los proveedores, contemplada en el artículo 104 bis, del Reglamento de Compras Públicas.

3. La necesidad de emitir una directiva con el objeto de entregar pautas y lineamientos generales a los organismos de la Administración del Estado respecto a las contrataciones de servicios en la nube.

4. La consulta pública realizada entre el 11 de enero y 2 de febrero de 2018, la cual entregó diversas recomendaciones que han sido consideradas en el análisis y elaboración de la presente directiva.

5. Que el nuevo proceso de evaluación de proyectos TIC llevado adelante por el Ministerio de Hacienda, la Dirección de Presupuestos y la División de Gobierno Digital del Ministerio Secretaría General de la Presidencia, incluye entre sus criterios de aceptación el uso de servicios cloud computing.

6. Que, para efectos de aprobar la señalada directiva, debe dictarse el correspondiente acto administrativo.

RESUELVO

1. **APRUÉBASE** la Directiva de Contratación Pública N°32 "Recomendaciones para la contratación de servicios en la nube", cuyo texto se transcribe a continuación:

DIRECTIVA DE CONTRATACIÓN PÚBLICA Nº 32
RECOMENDACIONES PARA LA CONTRATACIÓN DE SERVICIOS EN LA NUBE

1. CONTEXTO GENERAL

Las Directivas de Contratación son orientaciones y recomendaciones generales, elaboradas por la Dirección de Compras Públicas –en adelante, DCCP-, de acuerdo con su función asesora del artículo 30 letra a), de la Ley N°19.886.
Son lineamientos no vinculantes para los órganos públicos y los proveedores, pero su adhesión como buenas prácticas favorece una mejor gestión de los procesos de compra, dentro del marco legal vigente.
En 2015, consciente de las particularidades que se observan en la contratación de bienes y servicios relacionados con tecnologías de información, la DCCP elaboró la Directiva N°24, entregando pautas para la contratación de dichos bienes y servicios.
Sin embargo, se ha considerado oportuno profundizar las materias específicas relativas a la contratación de servicios en la nube (también llamados servicios *"cloud computing"*).
La elaboración de esta Directiva se ha realizado con el aporte de la ciudadanía a través de una consulta pública abierta, y en coordinación con instituciones como Investchile y la División de Gobierno Digital del Ministerio Secretaría General de la Presidencia, que tiene el mandato de coordinación interinstitucional en estas materias, procurando dar cuenta de las mejores prácticas de todo el Sector Público y de la política de uso de la nube que se implementará para todos los organismos del Estado.
Cabe agregar que esta Directiva recoge sólo aquellas propuestas que se encuentran dentro de la competencia asesora de la DCCP, excluyéndose las que correspondan a materias propias de ley o de modificación reglamentaria.

2. OBJETIVO DE LA DIRECTIVA

Esta Directiva de Contratación recomienda pautas y lineamientos generales a los organismos de la Administración del Estado, para que puedan utilizarlos en el diseño, la evaluación y la adquisición de servicios cloud. Con ello se espera que tales servicios resulten adecuados al propósito que se requiere cumplir, sean eficientes en sentido económico y que los riesgos sobre la información y sus activos sean adecuadamente gestionados.

3. *DEFINICIONES*

Cloud computing es un modelo para habilitar, a través de la red el acceso ubicuo, conveniente y a demanda de un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente provistos y liberados con un mínimo esfuerzo de gestión o interacción con el proveedor cloud[1]. Asimismo, pueden proveer estándares de disponibilidad, flexibilidad y seguridad significativamente superiores a las soluciones de datacenter implementados localmente por cada institución.

Para calificar un servicio como *cloud,* destacan las siguientes características:

1. **Autoservicio bajo demanda:** El cliente puede contratar sólo los servicios que requiere y cuando los necesite, sin tener mayor interacción con el proveedor.
2. **Amplio acceso a la Red:** Los servicios quedan disponibles ampliamente acorde a las reglas de acceso que se definan, pudiendo generar recursos compartidos de manera sencilla.
3. **Recursos Compartidos:** Los recursos tecnológicos del proveedor son agrupados para servir a múltiples clientes, siendo asignados y reasignados de forma dinámica y bajo demanda.
4. **Elasticidad:** Las capacidades requeridas se pueden asignar y retirar de forma elástica y, a menudo, automáticamente, respondiendo de forma flexible a la demanda de recursos de los clientes.
5. **Servicio medido:** Se aprovecha la capacidad de medición en algún punto apropiado del servicio para permitir al cliente consumir sólo lo que necesita.

En la actualidad, se advierten los siguientes modelos de servicio como principales, sin perjuicio de que existan otros o se combinen:

1. **Infraestructura como Servicio (IaaS)**: Los recursos para servidores en la nube son provistos como infraestructura que corresponde a cómputo, red y almacenamiento. Sin embargo, en algunos casos pueden llegar a proveer muchos otros servicios que deben ser evaluados.
2. **Plataforma como Servicio (PaaS)**: Las aplicaciones son ejecutadas en plataformas que tienen características estandarizadas y son capaces de mantener el ciclo de vida de una aplicación desde su desarrollo hasta su puesta en producción. Estas

[1] NIST: National Institute of Standards and Technology, United State, Department of Commerce http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

plataformas suelen ser servicios acotados y muy definidos, por lo que su uso debe ser evaluado según la circunstancia.

3. **Software como Servicio (SaaS)**: El servicio prestado en esta modalidad es referente al uso definido y limitado de un software hospedado en un lugar desconocido, a menos que el lugar sea especificado por el proveedor. La característica principal de este tipo de servicios es que son diseñados para usuarios que no mantienen por sí mismos un servicio específico. El servicio es accedido a través de un navegador o una aplicación provista por el proveedor, por lo que tienen una barrera de entrada muy baja.
4. **Funciones como Servicio (FaaS)**: El servicio se caracteriza por la ejecución de una función definida por el tiempo que ésta dure y se recomienda para el procesamiento de información volátil. La mayoría de las empresas capaces de proveer IaaS y PaaS podrían proveer FaaS, ya que su implementación requiere de las dos definiciones anteriormente mencionadas.

Por último, existen los siguientes modelos de implementación:

1. **Nube pública:** Los servicios cloud están abiertos a toda persona capaz de pagar por ellos a sus proveedores. Este tipo de cloud comparte el hardware o soporte físico con un número desconocido de usuarios, por lo que algunas veces -y dependiendo del proveedor- el servicio se puede degradar según la manera como el proveedor tenga distribuida la carga. Por ejemplo, empresas con datacenters TIER 3 y 4.
2. **Nube privada:** Cuando una institución tiene la capacidad tanto técnica como práctica para realizar la instalación y administración de un servicio cloud. Ella existe en la misma dependencia física de la institución con hardware de ésta, bajo su completa administración. Por ejemplo, algunos sitios gubernamentales.
3. **Nube comunitaria:** La infraestructura en la nube se aprovisiona para uso exclusivo de una comunidad específica de consumidores de organizaciones que comparten objetivos (por ejemplo, misión, requisitos de seguridad, política y consideraciones de cumplimiento). Por ejemplo, sitios en que instituciones han transferido recursos para realizar cómputo de forma optimizada.
4. **Nube híbrida:** Este es un término amplio que implica la utilización conjunta de varias infraestructuras en la nube de cualquiera de los tres tipos anteriores, que se mantienen como entidades separadas, pero que a su vez se encuentran unidas por tecnología estandarizada o propietaria, proporcionando portabilidad de datos y aplicaciones. Por ejemplo, instituciones financieras que tienen la información en sus datacenter, pero proveen servicios vinculados a sus transacciones en nubes externas para alta disponibilidad.

4. *RELACIÓN CON OTRAS DIRECTIVAS Y GUÍAS*

La presente directiva se vincula de forma armónica y complementaria con los siguientes documentos, por lo que se sugiere a los órganos compradores utilizarlos de manera integral:

- Directiva N°24: Instrucciones para la contratación de bienes y servicios relacionados con tecnologías de la información.
- Directiva N°26: Recomendaciones para una mayor eficiencia en la contratación de bienes y servicios.
- Directiva N°27: Recomendaciones para favorecer la generación de datos abiertos en la contratación pública.
- Directiva N°29: Recomendaciones para realizar compras conjuntas de bienes y servicios.
- Guía sobre buenas prácticas en materia de contratación de servicios cloud (MINSEGPRES, 2014).
- Guía Práctica de Uso de Servicios Cloud Computing en el Estado (MINSEGPRES, 2018). La División de Gobierno Digital de MINSEGPRES actualizará esta guía en la medida que se vayan alcanzando nuevas definiciones y actualizando las normativas relevantes.

5. *PRINCIPIOS APLICABLES A LA CONTRATACIÓN DE SERVICIOS EN LA NUBE*

Los procesos de compra pública y sus contratos deben desarrollarse respetando principios rectores como la estricta sujeción a las bases de licitación, la libre concurrencia al proceso y la igualdad de los oferentes. A partir de ellos, las cláusulas de un contrato no pueden contradecir lo dispuesto previamente en las bases de licitación; los procesos de compra no deben presentar barreras de entrada que impidan ofertar; y la entidad pública compradora no debe dar un trato arbitrariamente discriminatorio a los oferentes.

Tratándose de la contratación de servicios en la nube, además, se debe tener en cuenta otros principios relevantes, como la eficiencia, la legalidad, la neutralidad tecnológica y la seguridad, útiles para orientar la redacción e interpretación de las bases de licitación, los términos de referencia, las intenciones de compra de convenios marco y los contratos.

Principio de eficiencia

La tecnología impacta positivamente en la forma en que los órganos de la Administración del Estado ejercen sus funciones, con plena consonancia con los principios de eficacia y eficiencia, consagrados en el artículo 3° de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado, y en particular para la tecnología *cloud*, en la que la eficiencia computacional, producto de sus características intrínsecas, genera importantes ahorros que se traducen habitualmente no solo en menores costos, sino también en mayor rapidez de desarrollo de las soluciones, siendo importante considerar positivamente dichos aspectos para la contratación de servicios en la nube.

Principio de legalidad

De acuerdo con el principio de legalidad los organismos de la Administración del Estado sólo pueden actuar dentro de sus competencias legales, ciñéndose a las normas de la ley N° 19.886 (en adelante Ley de Compras), tanto en el desarrollo del proceso de compra como en la ejecución del contrato. Si no lo hicieran, su actuación sería nula, exponiéndose los funcionarios involucrados a las sanciones que contempla el ordenamiento jurídico.

Asimismo, la legalidad impone límites al uso de la tecnología, que deben ser respetados por las partes, principalmente para proteger derechos de las personas. Por esa razón, debe tenerse presente que las restricciones legales no pueden desconocerse en los contratos ni infringirse al utilizar el servicio cloud computing. *(Por ej. un órgano público no puede contratar el servicio de software para monitorear el comportamiento de los funcionarios públicos en el lugar de trabajo o para interceptar las comunicaciones privadas de los ciudadanos, más allá de sus competencias legales, ya que con ello se vulnerarían sus derechos fundamentales).*

En tal contexto, los proveedores de servicios tecnológicos deben tener presente que sus clientes del sector público no gozan de los mismos niveles de flexibilidad que sus clientes del sector privado. A modo de ejemplo:

- Si los organismos públicos no tienen expresamente asignada la facultad de someter las diferencias contractuales a un arbitraje, no podrán suscribir contratos que contengan cláusulas en dicho sentido;

- Los organismos públicos no pueden eximir o limitar la responsabilidad directa del proveedor incumplidor, porque implicaría una renuncia anticipada de derechos por parte del organismo público;

- La aplicación de multas o el cobro de garantías no es opcional, sino que responde a la aplicación de las cláusulas contractuales, donde se vincularán estas medidas concretas de multas, cobros de garantía o términos anticipados del contrato, según la gravedad, en especial, según acuerdos de nivel de servicio objetivos, medibles y directamente relacionados con las prestaciones contratadas (Véase la Directiva Nº 24, antes citada).

Principio de neutralidad o imparcialidad tecnológica

Los procesos de compra de servicios en la nube no deben dar preferencia a tecnología específica alguna, favoreciendo o perjudicando expresamente a un tipo de tecnología por sobre otra.

En este sentido, optar por tecnología estándar, entre otras ventajas, permite simplificar el proceso de cambio tecnológico. Para ver referencias se sugiere consultar la Guía Práctica de Uso de Servicios Cloud Computing.

Ahora bien, según este principio, si llega a ser necesario optar por alguna tecnología concreta, se debe justificar fundadamente que la selección de esa tecnología fue imparcial y objetiva *(Por ej. cuando el órgano comprador necesite contratar un servicio cloud que utilice una tecnología*

específica compatible con su infraestructura local, como OpenStack o Eucalyptus, podría justificar la exclusión de otras tecnologías distintas a las requeridas en las bases por razones de compatibilidad técnica para operar).

Para respetar el principio de neutralidad por regla general se debe evitar, tanto la mención de marcas específicas en las bases de licitación (considerar lo dispuesto en el número 2 del artículo 22 del reglamento de la ley N° 19.886), como el solicitar especificaciones técnicas "a la medida" de productos tecnológicos concretos que en la práctica solo podrían cumplir oferentes específicos. Además, las bases no deben contener reglamentaciones excesivas que impidan o limiten la participación de determinados oferentes que, por tener ofertas estandarizadas, no podrán adaptarse a definiciones tan específicas.

Así, por regla general se debe aludir a estándares técnicos más que a una marca propietaria, y a elementos a considerar más que a normas específicas, con el fin de propiciar una mayor participación de potenciales proveedores del Estado. En el caso de las tecnologías *cloud*, existe el concepto de *"cloud-neutral"*, es decir, tecnología que puede operar en los servicios cloud de distintos proveedores, o incluso nubes privadas o locales. *(Por ej. al utilizar un modelo IaaS, habitualmente es posible "exportar" las instancias para utilizarlas en otra infraestructura, pero cuando se contrata en modalidad SaaS no siempre pueden ejecutarse una instancia local o cambiar de proveedor).*

En el caso de tratos directos, se pueden solicitar productos de marcas específicas. Sin embargo, se sugiere no olvidar los beneficios de la neutralidad tecnológica al ampliar la posibilidad de recibir ofertas.

En definitiva, la neutralidad favorece mayor competencia y más participación, permitiendo ofertas por un mayor número de productos y, eventualmente, se puede acceder a más soluciones que atiendan correctamente el requerimiento, garantizando un trato igualitario hacia los actores del mercado.

Principios de Seguridad en la Nube

Debe recordarse que los usuarios de servicios *cloud* necesitan medidas que garanticen que los riesgos asociados al almacenamiento de sus datos y ejecución de sus aplicaciones en un ambiente *cloud* son comprendidos y gestionados adecuadamente.

Al ser responsabilidad del proveedor la implementación de algunas de estas medidas, los criterios de seguridad utilizados por éste deben ser reconocidos, transparentes y verificables. Para ello, el órgano comprador puede recurrir a auditorías o solicitar certificaciones externas vinculadas al cumplimiento de esas características.

Algunos aspectos de seguridad a considerar son:

- <u>Contar con seguridad física y lógica, controles de acceso, identidad y autenticación robustos:</u> Se espera que los centros de datos estén construidos bajo altos estándares de seguridad para proteger la información de las entidades, ante ataques y accesos no

autorizados. El acceso a todas las interfaces de servicio debe estar restringido a personal esencial para su operación, sujetos a autenticaciones y autorizaciones suficientes, para prevenir cambios no autorizados, modificación de datos, denegación de servicio u otras amenazas.

- Proteger los activos de información y datos, tanto en tránsito como en reposo: Los datos, activos y redes deben estar adecuadamente protegidos contra la manipulación, espionaje, pérdida o daño. En especial se espera contar con el cifrado de datos para mitigar riesgos de pérdida de confidencialidad.

- Considerar seguridad operacional, del personal y de subcontratistas: El proveedor del servicio debe contar con medidas de seguridad acorde al riesgo de sus procesos y establecer procedimientos para garantizar la seguridad en la operación del servicio, incluyendo la gestión de su personal y de los subcontratistas que utilice.

- Demostrar gestión segura de los clientes, incluyendo separación de los mismos y promoción del uso seguro del servicio: El proveedor debe 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. Entre las medidas a adoptar por el proveedor suele considerarse la separación de los clientes.

- Proveer información de auditorías a los clientes: Es importante proporcionar a los clientes de servicios cloud herramientas que les permitan acceder, razonablemente y respetando políticas de confidencialidad, a los registros de auditoría necesarios para controlar el acceso a su servicio y los datos contenidos en él.

- Implementar ciberseguridad: En servicios cloud es importante ejecutar una estrategia, tanto proactiva como preventiva, monitoreando constantemente las redes y centros de datos para mitigar ciberataques, en forma concordante con la Política Nacional de Ciberseguridad de Chile que se encuentre vigente.

- Reportar incidentes de seguridad: El proveedor debe transparentar al cliente información detallada 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.

- Considerar el uso de normas internacionales de seguridad: Se recomienda utilizar certificaciones estandarizadas de seguridad utilizadas a nivel mundial como ISO 27001, ISO 27017, ISO 27018, NIST Cybersecurity Framework, SOC, entre otras.

6. PAUTAS PARA LOS PROCEDIMIENTOS DE ADQUISICIÓN Y EJECUCIÓN DE LOS SERVICIOS

A continuación, se contienen pautas a aplicar en la contratación de servicios cloud, clasificadas de acuerdo con las distintas etapas del ciclo de compra:

6.1.- PAUTAS PARA LA FORMULACIÓN DEL REQUERIMIENTO:

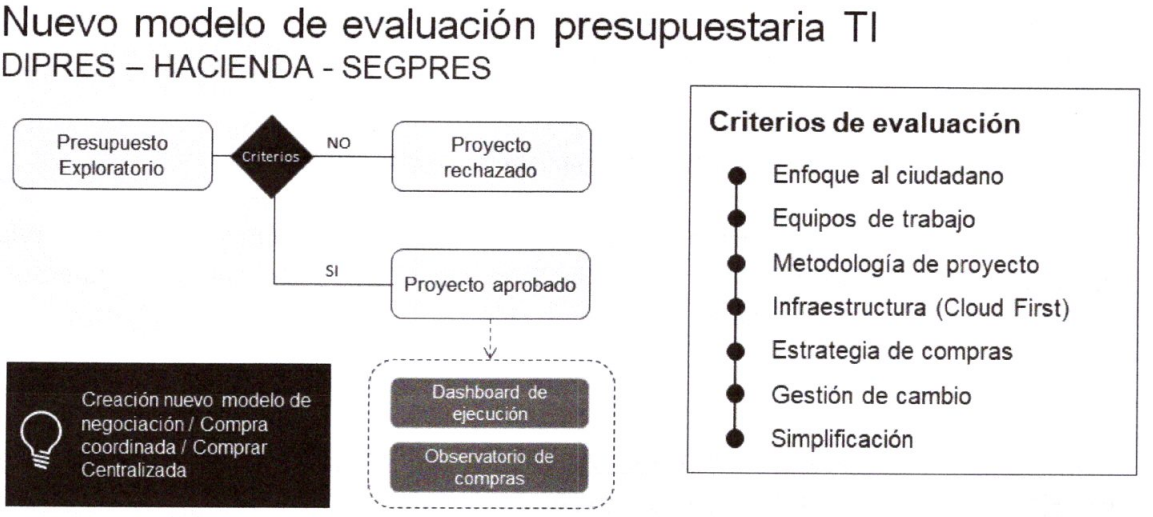
Se recomienda que la formulación del requerimiento de contratación de servicios *cloud* considere lo indicado al respecto por la Directiva N°24, junto con los siguientes aspectos específicos para servicios *cloud*:

Estrategia

Las contrataciones más complejas de tecnologías de información deben estar asociadas a una estrategia previa, validada por las jefaturas superiores del Servicio. Ello favorece procesos de compra alineados con los objetivos estratégicos de la institución, evitando que se transformen en proyectos aislados, aunque parezcan beneficiosos.

Ello significa que la estrategia no puede depender únicamente del área tecnológica de la organización, sino que debe ir en concordancia con una planificación más amplia de la institución. Además, exige que dichas áreas de tecnologías de información conozcan la totalidad de las bases administrativas, no sólo los aspectos técnicos, ya que en ellas también participan otras unidades como las áreas jurídicas y de compras.

Al respecto, cabe mencionar que la División de Gobierno Digital de MINSEGPRES, ha definido una serie de recomendaciones en virtud de lo definido en los artículos 10, 11 y 18, del decreto N°1, de 2015, del Ministerio Secretaría General de la Presidencia, que Aprueba Norma Técnica sobre Sistemas y Sitios Web de los Órganos de la Administración del Estado, que son responsabilidad directa del Jefe de Servicio según el artículo 19. Esto resulta relevante, ya que desde 2018 se está realizando un proceso de evaluación de proyectos TIC por parte del Ministerio de Hacienda, la Dirección de Presupuestos y el Ministerio Secretaría General de la Presidencia (División de Gobierno Digital), para los planteamientos que se hagan presupuestariamente. Estos lineamientos se encuentran detallados en la sección "Política Cloud" de la Guía Práctica de Uso de Servicios Cloud, ya mencionada.



En particular, para las soluciones *cloud* se requiere evaluar si estratégicamente son idóneas al problema que se desea resolver. Existen características clave que permiten identificar si un determinado proceso es apropiado para trasladarlo a entornos *cloud.* Algunos ejemplos de procesos idóneos para implementar en modalidad *cloud* son:

- Cargas de trabajo impredecibles o con potencial de crecimiento explosivo**.** En particular, aplicaciones altamente populares se benefician de disponer de capacidad de crecimiento elástica para no ser víctimas de su propio éxito.

- Fluctuaciones de carga predecibles durante los períodos de alta demanda. Si hay demanda con horas *peak* claramente definidas, es posible aumentar la capacidad sólo para esas horas y así ahorrar recursos durante las horas de baja demanda.

- Fácil paralelización del trabajo, permitiendo un escalamiento horizontal, más que vertical**.** Por ejemplo, procesamiento paralelo como *streaming*, codificación de video, solicitudes de contenido estático, entre otros, permiten utilizar múltiples instancias de procesamiento en lugar de una sola gran máquina.

- Disponibilidad de ambientes de contingencia. La nube es un medio ideal para disponer de infraestructura para algunos eventos de continuidad, puesto que se puede conservar ambientes a menor escala que los ambientes de producción con el objetivo de minimizar las interrupciones, y sólo activarlos cuando sea necesario, sin incurrir en el costo periódico de mantenerlos todo el tiempo disponible[2].

Del mismo modo, hay ciertas características de algunos procesos que hacen que las ventajas de llevarlos a *cloud* no sean tan claras, como, por ejemplo, aplicaciones que demanden muy baja

[2] Para más ejemplos de otros flujos de trabajo idóneos para la nube, revisar la Guía Práctica servicios de Cloud Computing, disponible en http://digital.gob.cl/guiacloud

latencia o requieran hardware especializado. En ocasiones se pueden reemplazar algunos servicios de estas características por servicios que operen de forma adecuada en ambientes *cloud nacionales* (por ejemplo, un servidor NFS que operaría de forma deficiente en la nube puede ser reemplazado por recursos tipo *S3* o *Gluster*, que permiten implementar una funcionalidad equivalente), pero esto debe ser analizado caso a caso por el organismo. En algunos casos, donde el servicio tenga un datacenter nivel Tier 3 o 4, se puede evaluar la posibilidad de generar una nube privada.

Dentro de esta evaluación se debe incluir la alternativa de contar con soluciones locales, en que las instituciones puedan presentar restricciones para datacenter que no cuenten con medidas adecuadas de control de acceso, temperatura, registro, respaldos, entre otras.

Alcance

Dentro del diseño del requerimiento de un proceso complejo de compra de tecnología *cloud* es necesario definir su alcance, desde distintas perspectivas. Para ello, se recomienda considerar los lineamientos definidos en la Directiva N° 24, además de los siguientes:

- Revisar las experiencias de otros organismos en migración o uso de tecnologías *cloud,* sin que esto se convierta en una barrera de entrada para los oferentes.

- Identificar qué restricciones técnicas imponen sus sistemas de información actuales a la solución *cloud* que se desee adquirir y cómo interoperarían entre ellas.

- Analizar la capacidad interna de la institución para la gestión de un proyecto de implementación o migración, si es el caso. No hay que olvidar que el éxito de estos proyectos requiere la colaboración del personal del órgano público.

- En caso de no contar con conocimientos suficientes para migrar a estos servicios, se recomienda contratar asesorías especializadas a modo de anteproyectos, por ejemplo, con un perfil consultor.

A partir de todo lo anterior se evitan proyectos con alcance difuso que generan dificultades durante la implementación.

Consulta al mercado (RFI)

Una de las principales dificultades con que se encuentran los organismos públicos en la etapa precontractual, en procesos de contratación de servicios en la nube, es ignorar aspectos técnicos necesarios y suficientes para definir su requerimiento, a partir del nivel de conocimiento inicial que poseen sobre el mercado actual. Es de particular atención que el mercado de los servicios en la nube es muy dinámico, y cuenta con una amplia variedad, por lo que hay que evaluar cuidadosamente las ofertas que presenta la industria para la problemática que se desea solucionar, siendo muy importante plantearla de forma clara y precisa, para facilitar una correcta presentación de las posibles soluciones disponibles, aplicando el principio

de neutralidad tecnológica y no atentando contra la libre competencia entre los diversos oferentes del mercado.

La normativa de compras exige que en licitaciones donde la evaluación de ofertas revista gran complejidad –que sería el caso de estos contratos-, las entidades licitantes realicen un análisis técnico y económico anterior a la elaboración de las bases de licitación, acerca de características que requieran para la confección de las bases, tales como:

- Las características de los bienes y servicios requeridos;
- Sus precios y formas de pago;
- Los costos asociados;
- El tiempo suficiente para la preparación de las ofertas;
- Alternativas para solucionar el problema;
- Posibles reglas para evaluar propuestas;
- Perfil de la Contraparte Institucional para administrar este servicio;
- Tiempos de referencia de implementación de la solución;
- Condiciones para el término anticipado de Contrato;
- Incumplimientos.

Este análisis técnico y económico puede realizarse a través de consultas al mercado –RFI-, u otro mecanismo, como informes internos especializados, que permiten al organismo público informarse de los estándares y servicios disponibles en la industria, así como la identificación de eventuales barreras de entrada o limitaciones a la competencia.

Como resultado de consultar al mercado, el órgano público puede recibir comentarios y respuestas de un universo suficiente y representativo de los eventuales oferentes, que aclaren sus dudas, confirmen aspectos definidos por la estrategia y el alcance y, fundamentalmente, le permitan contar con información adecuada para formular correctamente su requerimiento, en las bases de licitación o en los términos de referencia, según corresponda.

Gestión de los riesgos asociados a la contratación de servicios en la nube

Como parte del proceso, la institución debe realizar un proceso de gestión de riesgos para evaluar y contrastar los beneficios de utilizar servicios *cloud* con los riesgos que podría implicar, incluyendo tanto los riesgos tecnológicos, legales, la reputación (goodwill) y los de negocio. Se sugiere realizarlo como parte de la formulación del requerimiento y de forma estratégica, para luego revisar en detalle el caso particular de cada posible proveedor.

Además, se recomienda revisar con detenimiento los contratos de prestación de servicios, y que éstos especifiquen claramente las mitigaciones a los riesgos identificados y las medidas de seguridad utilizadas para proteger los datos del Servicio. Por otro lado, tratándose de productos o servicios estandarizados, se debe analizar si cumplen los aspectos técnicos mínimos requeridos en este sentido. Se debe prestar especial atención en la jurisdicción aplicable a los servicios contratados, considerando temas como la naturaleza de los datos tratados (en particular si se trata de datos personales), propiedad de los activos, leyes y regulaciones

normativas aplicables, responsabilidades contractuales, interoperabilidad de los sistemas, entre otros.

Adicionalmente, es necesario tener especial consideración de la estimación presupuestaria y el eventual riesgo de 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 llega a exceder el presupuesto original. Para evitarlo, hay que realizar una buena planificación de la 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.

En algunos casos el órgano público puede requerir certificaciones y auditorías de terceros. En ese caso se recomienda determinar cuáles de esas certificaciones o auditorías son relevantes o útiles para los fines del proceso de compra y del contrato. Cabe destacar que el alcance de algunas certificaciones o auditorías puede estar acotado sólo a ciertos procesos específicos, por lo que se deben solicitar todos los antecedentes que sean necesarios para garantizar adecuadamente la confianza en estas certificaciones o auditorías.

En caso de que el órgano público necesite auditorías específicas, como por ejemplo en materias de seguridad, se debe indicar claramente en las bases o el contrato quién asume el costo de ellas, quién selecciona al auditor, en qué condiciones se realizan, y si alcanzan solo al proveedor o también a sus casas matrices o filiales.

Finalmente, se deben considerar aspectos relevantes a la gestión de salida, en el proceso de terminación de un contrato de prestación de servicios, revisando temas como la duración máxima o mínima predefinida de los contratos, la posibilidad de finalizar el contrato anticipadamente, el plazo de aviso necesario para la terminación, el tratamiento posterior de los datos (incluyendo registros y metadatos), detallando el tiempo durante los cuales se conservarán los datos por parte del proveedor del servicio cloud luego de terminado el contrato, y la obligación de eliminarlos una vez vencido dicho plazo.

Algunos ejemplos de cláusulas que se pueden aplicar en estos contratos se encuentran en el anexo de esta Directiva.

Definición del requerimiento (descripción y caracterización)

Como ya se ha mencionado, se recomienda seguir los lineamientos establecidos en la Directiva N° 24. Una correcta definición del requerimiento permite:

- Entregar claridad a los proveedores sobre las necesidades del Servicio;
- Recibir ofertas mejor orientadas a las expectativas del órgano comprador;
- Facilitar la interpretación del contrato cuando comience su ejecución; y
- Disminuir el riesgo de compras mal dimensionadas, que provocan un uso poco eficiente de los recursos públicos.

La descripción del requerimiento tiene que quedar reflejada claramente en las bases técnicas, en los términos de referencia o en la intención de compra –si es una gran compra de convenio marco- considerando, a lo menos, los siguientes aspectos:

- Descripción del organismo contratante.

Es importante que los proveedores conozcan al órgano público contratante, porque suele existir desconocimiento respecto de las funciones que realizan, su estructura, su dotación, etc.

- Descripción del problema o necesidad que se espera resolver con la contratación.

Con ello se busca transparentar las expectativas del órgano contratante y que los proveedores elaboren propuestas de mejor calidad.

En este punto, indique si las características de los servicios a adquirir permitirán cumplir objetivos mayores, como la interoperabilidad de los sistemas, la portabilidad de las soluciones o el intercambio de información a través de estándares abiertos y de general aceptación por la industria.

- Servicio requerido.

En caso de que el contrato comprenda más de una prestación (soluciones integrales), hay que indicarlas todas con claridad. Es importante declarar el modelo de servicio y el modelo de implementación requeridos claramente.

- Alcance del bien o servicio requerido.

En la medida que los proveedores conozcan datos suficientes para dimensionar la contratación, tales como, la cobertura esperada, la duración del proyecto, la vinculación con otros sistemas, por mencionar algunos, es factible esperar buenas ofertas.

- Acuerdos de nivel de servicio (SLA) definidos.

Los SLA constituyen cláusulas fundamentales para la ejecución del contrato, por tratarse de compromisos exigibles, medibles y demostrables. Por tanto, es necesario que el requerimiento sea claro al respecto, para que puedan ofertar aquellos proveedores cloud que se encuentran en reales condiciones de satisfacer dichos niveles, que digan relación con la gravedad y estén directamente relacionados con los servicios que se van a proveer, por este motivo resultará conveniente revisar las cláusulas tipo de los potenciales proveedores, analizando que ellas cumplan con las necesidades del servicio contratante y con el marco legal aplicable. Asimismo, pueden darse pautas generales con los criterios señalados que pueden ser complementados con aspectos específicos en cada oferta.

- Recursos institucionales disponibles.

Los proveedores pueden elaborar ofertas económicamente más convenientes, si conocen la situación del órgano contratante respecto de los recursos con que ya dispone (infraestructura, personal, bienes, documentación, etc.), ya que no tendría que incluirlos dentro de sus costos.

- Principales restricciones técnicas y normativas.

Es importante que el requerimiento indique las principales restricciones técnicas y normativas que afectan al proyecto, para que los proveedores elaboren sus ofertas informados de tal situación.

Para ello se debe revisar cuáles son las normas y estándares técnicos vigentes *(Por ej. para transferencia y almacenamiento documental electrónico; sobre accesibilidad a personas en situación de discapacidad; para datos abiertos; y para implementar medidas de seguridad de sistemas de información, entre otras).*

- Sistemas complementarios.

Indique si el proyecto a contratar incide en otros sistemas de la institución o externos, para que las ofertas incluyan acciones de integración -si son necesarias-, proyecten eventuales riesgos y puedan considerar medidas al respecto.

- Principales hitos o plazos del proyecto.

Es importante transparentar su estimación respecto de la duración del proyecto, teniendo presente que, en ciertos casos, la urgencia o los plazos muy exigentes pueden derivar en mayores riesgos, en precios más altos a los que se acostumbran en el mercado o en el desincentivo de participar cuando no resultan realistas. Por ello, es necesario planificar correctamente los procesos de compra.

- Presupuesto estimado o disponible.

Es útil dar a conocer el presupuesto estimado o disponible, para que el proveedor proyecte su margen de utilidades y pueda determinar los recursos que comprometerá en su propuesta.

Se recomienda que dicho presupuesto tenga presente cómo abordar cambios, crecimientos y desviaciones que pueda experimentar el proyecto, pudiendo aumentarse el contrato hasta un 30% del monto originalmente pactado, de conformidad con la normativa de compras públicas.

Asimismo, a fin de ampliar el número de oferentes, puede ser útil no restringir las ofertas a una moneda determinada o, a lo menos, no exclusivamente a la moneda de curso local (pesos chilenos).

Cubicación

Luego de definir los requerimientos funcionales del proyecto, según lo indicado en los párrafos anteriores, se procede a cubicarlo. En este punto es fundamental determinar si la contratación de un servicio *cloud* tiene aspectos de valor agregado comparado con un servicio tradicional. Al respecto, es importante ser consistente con lo planteado en la estrategia.

Dado que en modalidad *cloud* habitualmente se cobra por un servicio y no por la adquisición de un bien mueble, es importante considerar correctamente la imputación presupuestaria al subtítulo 22 o 29, de las Instrucciones Presupuestarias vigentes.

En este sentido, se sugiere realizar los puntos de cubicación recomendados en la Directiva N° 24, con los alcances que se establecen a continuación:

- Establecer el costo estimado del proyecto a contratar, tomando en cuenta la demanda estimada del servicio.

- Identificar en detalle las distintas actividades asociadas y sus plazos, para poder determinar los recursos involucrados en cada una de ellas. Los recursos necesarios en ambientes *cloud* pueden ser muy diferentes a los recursos tradicionales, en particular si se comparan modelos tradicionales con modelos PaaS o SaaS.

- Asignar los costos respectivos. En proyectos *cloud* se sugiere considerar costos específicos a los Prestadores del Servicio Cloud, que podrían variar *(Por ej. si se requieren instancias de ciertas características, se sugiere utilizar en la cubicación el valor de esas instancias y no de otras)*.

- Considerar con particular atención las posibles desviaciones del proyecto dentro de esta cubicación referencial, incluyendo estimación de demanda elástica y posible crecimiento de los recursos utilizados (sobreconsumo) y considerando que los costos podrían variar mes a mes. Para este propósito se recomienda estimar en base a las transacciones actuales de su servicio, midiéndolas con anterioridad mediante herramientas especializadas para ello, métricas de servicios similares que se encuentren disponibles, transacciones estimadas futuras y tasas de crecimiento de las mismas, entre otras. Asimismo, se sugiere contemplar expresamente en las bases de licitación las condiciones bajo las cuales aplica dicho sobreconsumo.

- Revisar si la cubicación está alineada con el presupuesto. En caso contrario, se deberá revisar el proyecto para adecuarlo a la disponibilidad presupuestaria.

- Realizar un análisis del mercado, evaluando las capacidades de los distintos proveedores disponibles. Como ya se mencionó, prácticas como las consultas al mercado o RFI pueden ser útiles, pero también lo puede ser el consultar experiencias similares previas en el mismo sector público.

Formalización del requerimiento

Resulta preciso elaborar un documento que formalice el requerimiento técnico, debiendo incluirse en él, a lo menos, las ideas centrales de la estrategia, los bienes o servicios a contratar, los plazos y costos vinculados al proceso y las principales etapas que demandará el proyecto.

Este documento permite mantener la consistencia en el diseño del proyecto y facilita la elaboración de otros documentos del proceso de compra (bases administrativas y técnicas, términos de referencia, intención de compra, respuestas para foros de consultas, etc.).

6.2.- PAUTAS PARA EL DESARROLLO DEL PROCEDIMIENTO DE COMPRA:

6.2.1.- En Grandes Compras de Convenios Marco:

Cuando el monto de una contratación a través de un Convenio Marco supera 1.000 UTM, la normativa de compras públicas exige que se realice un proceso de **Gran Compra**, es decir, es necesario que el organismo público comunique su intención de compra a través del sistema www.mercadopublico.cl, a todos los proveedores de este convenio marco adjudicados en la categoría del servicio requerido, con el objeto de que puedan presentar mejoras a sus ofertas. A partir de las propuestas recibidas, el órgano público confecciona un cuadro comparativo y selecciona aquella más conveniente, de acuerdo con los criterios de evaluación aplicables.

En particular, para el procedimiento de gran compra de convenio marco se sugiere:

- Conocer el alcance del convenio marco, para incluir correctamente en la intención de compra, los servicios adjudicados en él.
- Documentar la intención de compra y publicarla en el sistema www.mercadopublico.cl. Ella debe referirse exclusivamente a servicios adjudicados en ese convenio marco, incluidos los productos nuevos que se hayan incorporado. No corresponde este procedimiento si se necesita agregar otros servicios, además de los adjudicados en el convenio marco, caso en el cual se deberá realizar una licitación pública.
- Señalar claramente el requerimiento en la intención de compra, siguiendo los lineamientos de esta Directiva.
- El procedimiento de gran compra es parte de un Convenio Marco (no es una licitación). En tal sentido, la intención de compra puede solicitar marcas específicas, siempre que los productos formen parte del catálogo electrónico de ese convenio marco. Sin embargo, en ese caso, se recomienda analizar la conveniencia o no de restringir el objeto a una marca, de conformidad con lo señalado en esta Directiva, a propósito del principio de neutralidad tecnológica.
- Utilizar como criterios de evaluación únicamente los establecidos en las bases de licitación del convenio marco, sean todos o algunos de ellos. Esos criterios deben ser aquellos de tipo general que utilizó la DCCP para adjudicar el Convenio Marco. No se pueden utilizar criterios nuevos, distintos a los establecidos en las bases por la DCCP.

- Debe tenerse presente que, si se requiere considerar algún requisito técnico mínimo para las ofertas que reciba, en atención a condiciones específicas de la entrega de productos -como, pruebas en equipos específicos, demostración de certificaciones u otros-, corresponde establecerlo como requisito de admisibilidad y no como un nuevo criterio de evaluación, ya que esto último no se permite en los procedimientos de grandes compras de convenio marco.
- Elaborar un informe técnico a partir del cuadro comparativo de las ofertas recibidas, que sirva de fundamento para la selección.
- Evitar definiciones o reglamentaciones que ya hayan formado parte del proceso de licitación del Convenio Marco, a fin de simplificar el proceso.
- Suscribir un acuerdo complementario con el proveedor cloud seleccionado, en los términos señalados en las bases de licitación, con el objeto de detallar exclusivamente los aspectos particulares, tales como las etapas y plazos de implementación, los niveles de servicio, las medidas de seguridad y las garantías -si fueren diferentes a las del Convenio Marco y no estuvieren reguladas en los contratos estándar aplicables a dichos productos- entre otros aspectos, remitiéndose en lo demás a las definiciones del Convenio Marco.
- El pago de los servicios cloud debe ser efectuado directamente por cada Entidad, dentro de los 30 días corridos siguientes a la recepción de la factura respectiva, la cual deberá ser entregada acompañada de una copia de la Orden de Compra respectiva y de las Guías de Despacho en la cual se certifique la recepción conforme de los servicios. La recepción conforme deberá ser acreditada por la Entidad que hubiere efectuado el requerimiento. Las fichas de los servicios indican la forma de facturación en el documento técnico adjunto[3].

***6.2.2.- En las licitaciones*:**

En caso de que los bienes o servicios a contratar no estén disponibles en el catálogo de un convenio marco, los organismos deben licitar su contratación. Al respecto, puede considerar las siguientes pautas para redactar las bases administrativas y técnicas:

En las bases administrativas:

- Elaborar y/o utilizar bases administrativas tipo si el proceso de compras resulta más bien estándar y se proyecta repetirlo en términos similares. Sin embargo, si se advierte que existen particularidades distintas en cada compra, difícilmente estandarizables, deberán elaborarse bases administrativas especiales para cada proceso de compra.

- Redactar bases administrativas breves y claras, simplificando requisitos y evitando definiciones que restrinjan la participación de oferentes.

- Preparar la licitación en varias líneas, según los componentes del servicio licitado *(Por ej. Infraestructura como servicio, software como servicio, etc.)*, pero haciendo referencia a

[3] Para profundizar en más recomendaciones sobre el pago, se recomienda revisar la directiva N° 23 "ORIENTACIONES SOBRE EL PAGO OPORTUNO A PROVEEDORES EN LOS PROCESOS DE CONTRATACIÓN PÚBLICA".

los estándares técnicos, de manera amplia y considerando además categorías híbridas. Esto permite contratar todos los componentes a un solo Prestador del Servicio Cloud o a distintos Prestadores del Servicio Cloud, según la factibilidad técnica y las reglas que establezca la licitación.

- Diseñar estas licitaciones en dos etapas, la primera técnica y la segunda económica. Así, se evalúa en detalle la calidad técnica de las propuestas, sin sesgos originados por la oferta económica.

- No solicitar documentación administrativa en exceso, ya que ello desincentiva la participación de los Prestadores del Servicio Cloud. Por lo tanto, se sugiere pedir únicamente aquellos documentos que permitan acreditar elementos básicos para la validez de las ofertas *(Por ej. certificado de vigencia de la empresa, de la personería, o declaraciones juradas sobre las inhabilidades legales)*.

- Hay que recordar que la inscripción en el registro de proveedores es suficiente para acreditar gran parte de la documentación administrativa, de modo que no hay que pedir esos documentos si ya están en dicho registro.

- Considerar la posible participación de proveedores cloud extranjeros, flexibilizando las licitaciones y sus bases de manera de no imponer requisitos que les hagan difícil o imposible participar, como la necesidad de contar con certificaciones laborales no posibles de obtener para quienes no tienen RUT en Chile, exigencias de pago local u ofertas únicamente en moneda local, entre otras.

- Indicar en las bases la posibilidad de recibir antecedentes durante el período de evaluación, en conformidad a lo dispuesto en el artículo 40 del reglamento de la ley N° 19.886, para que los defectos meramente formales no ocasionen la imposibilidad de presentar ofertas o el rechazo de éstas, sino que sean evaluables.

- Incluir instancias informativas, como la publicación de videos, reuniones -sean presenciales o en línea-, para favorecer una mejor comprensión de las bases y, con ello, recibir mejores ofertas. Al respecto, hay que recordar a los interesados que las preguntas deben efectuarse dentro de la etapa formal de consultas señalada en las bases, y a través del sistema www.mercadopublico.cl.

- Responder clara, precisa y directamente las preguntas que reciba durante la instancia de consultas establecida en las bases de licitación. Al dar respuestas muy genéricas o que solo remiten al articulado de las bases, sin mayor explicación, las dudas de los proveedores se mantienen y las ofertas pueden ser mal elaboradas o bien parecer más rígidas de lo que son. En este sentido, resulta indispensable que tanto las entidades como los proveedores lean y comprendan la totalidad de las bases administrativas y

técnicas, y de las consultas planteadas, para evitar errores u omisiones al ofertar o interpretaciones que sean más restrictivas de lo que se pretende en las bases y que los pueden dejar fuera del proceso.

- Hay que recordar que la Entidad licitante tiene las facultades para determinar los criterios de evaluación, en la medida que sean objetivos. Al respecto, corresponde elegir aquellos criterios que permitan seleccionar la oferta más conveniente para satisfacer los intereses del Servicio, teniendo presente la estrategia documentada al formular el requerimiento. Por lo tanto, es una mala práctica utilizar criterios tipo sin antes analizar que sean los más adecuados en ese proceso en particular. Se recomiendan como criterios para estos procesos de compra:

    - La calidad de la propuesta *(Por ej. plazos, garantías, niveles de servicio, etc.)*;
    - La calidad técnica de la solución ofrecida;
    - La experiencia del equipo de trabajo, en especial del Jefe de Proyecto; y
    - El precio, entre otros.

- Establecer plazos realistas para recibir ofertas, para formular preguntas y responderlas, para evaluar y, sobre todo, para ejecutar el contrato.

- No exigir instrumentos de garantía específicos. Basta con que la garantía sea a la vista y de carácter irrevocable, asegure el pago de manera rápida y efectiva, y cumpla con el monto, plazo de vigencia, glosa –si procede-, y la moneda o unidad que señalen las bases.

- Establecer multas proporcionales a la gravedad del incumplimiento, fijando un tope máximo para su aplicación. Además, en las bases se debe incluir un procedimiento para aplicarlas, que contemple siempre la posibilidad de descargos por parte del Prestador del Servicio Cloud. Finalmente, dicte una resolución fundada para aplicar las multas, contra la que proceden los recursos administrativos dispuestos en la Ley N°19.880.

- Contemplar la posibilidad de modificar el contrato, ya que en proyectos complejos pueden aparecer requerimientos no dimensionados inicialmente, pero necesarios para la continuación del proyecto. Como las modificaciones no pueden contravenir la estricta sujeción a las bases y la igualdad de los oferentes, fije qué tipos de cambios son aceptables y en qué porcentaje máximo podrá modificar a través de un contrato complementario o un control de cambios. En el caso de montos, no podrá exceder el original en más de 30%.

- Algunos contratos de servicios tecnológicos representan un alto riesgo para la seguridad, privacidad y continuidad operacional, ya que inciden directamente en funciones críticas del órgano público. Por esa razón, la dependencia de éste, respecto del Prestador del Servicio Cloud lo vuelve vulnerable frente a eventuales incumplimientos contractuales (Por ej. de los SLA o de obligaciones de cuidado de los datos). Se recomienda incluir en las bases de licitación una instancia de verificación o

auditoría, previa a la suscripción del contrato, con el objeto de comprobar el real estado de las medidas de seguridad declaradas por el Prestador del Servicio Cloud -***due diligence o debida diligencia***-. Dicha verificación debe realizarse en coordinación con el proveedor cloud, en base, por ejemplo, a certificaciones, cuestionarios, checklist o listados predefinidos y velando por no entorpecer el correcto funcionamiento de éste. Además, debe referirse únicamente a aspectos estrictamente necesarios para la prestación de los servicios licitados.

- Se sugiere aplicar al Proveedor del Servicio Cloud un cuestionario sobre temas técnicos específicos de seguridad, protección de datos y continuidad operacional (Por ej. existencia de *site* de contingencia, planes de recuperación de desastres, controles frente a ataques de denegación de servicio, detección de intrusos, cifrado de datos, entre otros). Cuando existan, es posible e incluso recomendable reemplazar dicha auditoría por la presentación de certificaciones internacionales de reconocido prestigio que sea fácilmente comparables de un proveedor a otro o sus casas matrices en caso de filiales locales o de menor tamaño.

- En caso de incluir la aplicación de instrumentos de *due diligence*, se recomienda señalar expresamente en las bases de licitación las consecuencias que derivan de no cumplir con la entrega de información requerida.

<u>En las bases técnicas</u>:

- Describir clara y completamente el requerimiento. Para ello, se sugiere considerar los antecedentes recabados en la etapa inicial y que se encontrarán en el documento de formulación del requerimiento técnico. Si las bases técnicas no recogen correctamente el requerimiento, es probable que durante el desarrollo del proyecto surjan problemas de interpretación y dificultades para la ejecución del contrato.

- Establecer claramente y de manera realista, los niveles de servicio esperados (SLA). Estos niveles corresponden a aspectos operacionales del servicio contratado *(Por ej. uptime de aplicaciones, tiempo de respuesta frente a errores o tiempos de proceso, entre otros)*. Las variables relevantes deben ser modeladas a través de indicadores y cada indicador debe tener asociado un estándar mínimo aceptable. Los SLA definen el estándar de servicio que deberá cumplir la solución durante toda la vigencia del contrato, observando referentes nacionales e internacionales. No obstante, cabe recordar que mientras más exigentes sean los niveles de servicio, más alto podrá ser el precio del contrato. Sin embargo, la claridad y transparencia en los niveles esperados por el órgano comprador permiten a los proveedores analizar su real capacidad de cumplir.

- Incluir causales y mecanismos objetivos que permitan ajustar los niveles de servicio en caso de cambios tecnológicos o niveles operacionales, considerablemente distintos a los definidos originalmente, producto de cambios en el entorno.

- Asociar el incumplimiento de los SLA a multas que resulten proporcionadas a la falta *(Por ej. considerar el impacto del incumplimiento en la continuidad de servicio)*. Además, según la gravedad o la reiteración del incumplimiento, se recomienda considerarlo para el cobro de la garantía e, incluso, dentro de las causales de término anticipado del contrato.

- Aludir a estándares en vez de solicitar marcas específicas, lugar de procedencia del bien, o descripciones muy detalladas propias de tecnologías o productos concretos.

- Considerar criterios de accesibilidad para personas en situación de discapacidad *(Por ej. mejorando la claridad, alto contraste y velocidad en navegación por sitios web, e incorporando contenidos no sólo de texto, sino también de audio)*.

- Evitar que las exigencias técnicas impuestas a los oferentes sean barreras de entrada al proceso. Para ello, considérelas al evaluar y no para admitir una oferta *(Por ej. si se contratan servicios de integración y migración de datos, o de pruebas para medir la vulnerabilidad de sus sistemas, el riesgo puede llevar a justificar la exigencia de contratar seguros por daños. Sin embargo, ello puede ser considerado dentro de los criterios de evaluación y no para la admisibilidad de las ofertas)*.

- Sin perjuicio de lo anterior, en ciertos contratos complejos, por el nivel de riesgo involucrado, es posible fijar requisitos técnicos de admisibilidad, en la medida que sean objetivos y que no signifiquen arbitrariamente un trato discriminatorio a proveedores del servicio cloud. Así, quienes no cumplan satisfactoriamente tales requisitos no pasan a etapas de evaluación de sus ofertas.

<u>En los criterios económicos</u>*:*

- Evaluar la posibilidad de contratar bolsas de recursos o reserva de capacidad para servicios cuya cubicación o uso sea muy difícil de estimar. Esto es de fundamental importancia para la contratación de servicios *cloud* complejos, o cuando no se cuenta con experiencia en la estimación de la demanda.

- Considerar la posibilidad de adquirir servicios con más de un oferente, según la conveniencia de las ofertas, en este caso se recomienda evaluar las líneas de servicios a contratar de forma independiente.

- Facilitar que oferten proveedores del servicio extranjeros y/o fabricantes, permitiéndoles ofertar en otras monedas, aunque sin generar con ello un trato diferente respecto de los demás oferentes.

6.2.3.- En los tratos directos:

Excepcionalmente existen casos en los que, por la naturaleza de la contratación, hay circunstancias o características del contrato que hacen del todo indispensable acudir al trato directo, en vez de una licitación pública.

En este procedimiento cabe recordar:

· Fundar el trato directo exclusivamente en alguna de las causales señaladas en la Ley de Compras y su Reglamento.

· Acreditar la causal con antecedentes que demuestren la concurrencia de todos sus elementos. No basta con mencionarla en el acto administrativo que autoriza el procedimiento.

· Si se invoca como causal que la contratación sólo puede realizarse con proveedores que sean titulares de los respectivos derechos de propiedad intelectual, industrial, licencias, patentes y otros, se debe solicitar la documentación que lo demuestre *(Por ej. la inscripción de la obra en el registro respectivo; copia del contrato de distribución suscrito entre el proveedor del Servicio Cloud y la empresa titular de los derechos; u otra similar)*.

· Cuando la causal sea que el contrato es una reposición o complementación de servicios accesorios, o la renovación de éstos, se debe justificar en razones objetivas de compatibilidad técnica con los sistemas o infraestructura actual de la Entidad, a través de algún informe o revisión técnica.

6.3.- PAUTAS PARA LA SELECCIÓN DEL PRESTADOR DEL SERVICIO CLOUD

6.3.1.- Sobre las comisiones evaluadoras:

Las comisiones evaluadoras deben estar compuestas por personal del Servicio, con competencias técnicas suficientes. Si es necesario en los procesos más relevantes, se sugiere incluir expertos externos para realizar una evaluación técnica especializada.

Los miembros de la comisión deben ser imparciales y desinteresados *(por ej. no representar ninguna tecnología o corriente doctrinal particular en este campo)*.

Se recomienda que conozcan el documento de formulación de requerimiento, para que estén conscientes de la estrategia que motiva el proceso y lo esperado por el órgano público y contar con "check lists" de aspectos relevantes a ser considerados para efectos de comparación de ofertas y no limitar ello al precio de éstas.

Los integrantes de la comisión evaluadora, en el ejercicio de esas funciones, son sujetos pasivos de lobby o de gestión de intereses particulares, según la Ley 20.730. Por lo tanto, deberán registrar todo contacto que tengan con lobbistas o gestores de intereses particulares durante la evaluación. Sin embargo, se sugiere incluir en las bases administrativas la prohibición para estos miembros de aceptar reuniones solicitadas por terceros durante la evaluación, para que este tipo de contactos esté circunscrito exclusivamente a los casos que menciona la normativa de compras públicas y que se tienen que indicar previamente en las bases de licitación. De este modo se garantiza que la labor de la comisión evaluadora se realice sin presiones externas.

6.3.2.- Sobre los criterios de evaluación:

La evaluación debe realizarse con apego estricto a los criterios establecidos en las bases o indicados en la intención de compra, según el caso. En tal sentido, deben establecerse rangos objetivos para la asignación de puntaje al ponderar cada criterio o puntaje adicional a otorgarse a ofertas que comprendan criterios relevantes adicionales.

Deben considerarse criterios de evaluación inclusivos, que respondan a aspectos de alto impacto social *(Por ej. PYME, mujeres jefas de hogar, personas con discapacidad, entre otros).*
Si se desea evaluar la experiencia de la empresa, corresponde considerar proyectos similares al que se pretende contratar –independiente del sector en donde fueron realizados-, que sea posible comprobar.

El evaluar experiencia previa en un sector específico –como el sector municipal, de salud, defensa u otros- y, más aún, experiencia con la Entidad Licitante, constituye una barrera de entrada que infringe el principio de la libre concurrencia.

Si desea evaluar la presentación de servicios adicionales a la oferta principal, sus características básicas o generales tienen que estar descritas previamente en las bases.

Si evalúa el comportamiento contractual anterior de un Prestador del Servicio Cloud, deberá consultar el Registro de Proveedores, en donde las Entidades deben informar al respecto, de acuerdo con elementos objetivos *(Por ej. cumplimiento íntegro y oportuno de las obligaciones, de los plazos comprometidos, y sobre la aplicación de multas u otras medidas que hayan afectado al Prestador del Servicio Cloud).*, pero evitando exigencias de certificaciones que sean sólo aplicables respecto de proveedores locales.

Esta calificación no puede ser considerada como un requisito para participar en un proceso de compra, ya que sería una barrera de entrada para nuevos proveedores del Servicio Cloud o para aquellos que reflejen algunos aspectos negativos.

Se recomienda utilizar este criterio de comportamiento contractual anterior cuando sea relevante para la ejecución del contrato *(Por ej. en el caso del cumplimiento de plazos, de niveles de servicio y de la calidad de los bienes, entre otros).*

6.3.3.- Sobre las certificaciones

Si se considera que las certificaciones resultan relevantes para recibir ofertas de mejor calidad, deben solicitarse aquellas que estén directamente relacionadas con el requerimiento y sean internacionales, de manera de permitir comparación.

No deben exigirse esas certificaciones como requisito mínimo para participar del proceso, debiendo ser ponderadas como criterios de evaluación.

Debe verificarse que las certificaciones sean reconocidas en el territorio nacional y que estén relacionadas con el trabajo que se desarrollará.

Por último, se recomienda aceptar certificaciones determinadas y conocidas, pero abriendo la posibilidad a sus equivalentes, para favorecer la participación.

6.4.- PAUTAS PARA LA GESTIÓN DEL CONTRATO

6.4.1.- Sobre el pago:

El pago de los servicios debe ser efectuado directamente por cada Entidad, dentro de los 30 días corridos siguientes a la recepción de la factura respectiva, la cual deberá ser entregada acompañada de una copia de la Orden de Compra respectiva y de las Guías de Despacho en la cual se certifique la recepción conforme de los servicios. La recepción conforme deberá ser acreditada por la Entidad que hubiere efectuado el requerimiento.

Para el caso de contratación de bolsas, se entiende que la compra es por créditos de esas bolsas, cuyos pagos estarán sujetos a lo indicado en la respectiva cláusula de las bases.

Se recomienda establecer en las bases de licitación o en el contrato, el pago por uso de los recursos contratados.

Además, en este caso, se podría considerar expresamente la opción de extender el contrato si al final del periodo no fuesen consumidos todos los recursos presupuestados.

También puede considerar una sobre estimación de los recursos contratados, para evitar que éstos se consuman antes del término del contrato. En este caso, además, se consideraría la opción de no utilizar esos recursos y pagar solo aquello que efectiva se consuma.

Para evitar sobreconsumo de recursos contratados, se recomienda generar alertas periódicas de parte del proveedor, que informen anticipadamente cuando la bolsa se está agotando.

Para profundizar en más recomendaciones sobre el pago, se recomienda revisar la directiva N° 23 "Orientaciones sobre el pago oportuno a proveedores en los procesos de contratación pública".

Es útil considerar que los pagos eventualmente pueden realizarse a proveedores internacionales que resulten adjudicados, por lo que las bases no deberían dificultar su materialización a través de reglas que solo puedan aplicarse a proveedores nacionales.

6.4.2.- Contrato modular:

Cuando un contrato tecnológico incluye más de una prestación contractual, no siempre se ejecutan simultáneamente *(Por ej. soluciones integrales)*. Cada prestación o servicio puede tener plazos diferentes, además de exigencias técnicas y SLA propios.

Por ello, se recomienda redactar los contratos separando las cláusulas en distintas secciones, o bien permitir la referencia a los contratos estándar de los servicios que se oferten. Sin ese orden es más difícil interpretar el contrato e implementarlo, por lo que la estructura modular es importante para facilitar la gestión del contrato.

Se sugieren dos grandes secciones:

- ***Condiciones generales***

Incluye todas aquellas cláusulas esenciales y de carácter general, que abordan la totalidad del proyecto. (Por ej. individualización de las partes, personería, objeto del contrato, precio, vigencia, garantías, término anticipado, cláusulas de propiedad intelectual, cláusulas de confidencialidad, encargado del contrato, legislación aplicable y jurisdicción, entre otras).

Se recomienda tener especial cuidado al redactar el objeto del contrato y no omitirlo de las condiciones generales, incluso aunque después detalle los servicios en los respectivos anexos.

- ***Anexos***

Redacte el detalle de cada prestación, separadamente, a partir de anexos. De esta forma el contrato se ordena con más claridad, ya que es posible reunir en un documento las cláusulas específicas de una prestación determinada *(Por ej. la descripción del objeto, las etapas y plazos de ejecución, los plazos y pagos parciales, los SLA, las multas específicas, la carta Gantt, los diagramas, entre otros)*.

6.4.3.- Cláusulas relevantes

Los contratos sobre servicios en la nube pueden ser muy distintos unos de otros, al igual que las razones que motivan la contratación y el contexto en que los servicios serán ejecutados.

Sin embargo, existen ciertas cláusulas que se recomienda incluir, de resultar pertinente considerando el caso concreto:

- Cláusula de confidencialidad

Es importante incorporar una cláusula de confidencialidad si el proveedor cloud tiene algún tipo de acceso a información que almacena el órgano público, resultando indispensable si se tratan datos personales que provengan o hayan sido recolectados de fuentes no accesibles al público.

Para mayor certeza y eficacia de esta cláusula, se recomienda clasificar previamente su información. Así, esta cláusula aplicará exclusivamente a documentación reservada o confidencial.

Deben fijarse plazos máximos de confidencialidad concordantes con el tiempo de reserva que admite la Ley N°20.285, sobre Acceso a Información Pública. Sin embargo, debe tenerse presente que pueden existir plazos de reserva mayores, dispuestos por ley, como ocurre, por ejemplo, tratándose de datos de carácter personal, ya que la Ley N°19.628 sobre Protección de la Vida Privada establece que la obligación de confidencialidad se extiende de manera indefinida.

- Cláusula de tratamiento de datos personales por mandato

Si se contratan servicios de tratamiento de datos personales, debe incluir una cláusula de mandato hacia el proveedor cloud, que especifique las condiciones bajo las cuales puede utilizar esos datos, según el artículo 8 de la Ley N°19.628.

La cláusula debe indicar, a lo menos, la finalidad del tratamiento, el tipo de datos que entrega al Prestador del Servicio Cloud (mandatario), la duración del encargo y un procedimiento para la devolución de los datos y su eliminación efectiva por parte del proveedor del servicio cloud, al terminar el contrato.

Además, debe prohibir el uso de dichos datos para fines distintos a los que persigue el órgano público mandante y señalar expresamente que no se permite su comunicación a terceros.

- Cláusula de propiedad intelectual del software

Si hay intercambio de documentación u otros activos, es importante declarar en el contrato que los materiales preexistentes que aporta cada parte son de propiedad del que los provee.

Por su parte, en caso del contrato de Software como Servicio (SaaS), suele suscribirse el servicio durante un período determinado, en el cual únicamente se confieren derechos de uso temporal para el órgano comprador. Por lo tanto, los derechos de propiedad intelectual suelen conservarlos el desarrollador del software o el proveedor, según cada caso, por lo que el órgano público no recibe el código fuente.

En casos excepcionales, tratándose de SaaS prestados en la nube y, respecto de software no estándar, el órgano público podría evaluar el nivel de exposición al riesgo en la continuidad operativa de sus funciones y considerar medidas adicionales de resguardo. Por ejemplo, podría ver la pertinencia de incluir alguna cláusula de depósito del código fuente en una notaría -contrato *escrow*-, estableciendo aquellos casos taxativos y excepcionales en los cuales el organismo público respectivo pueda acceder al código fuente mediante la suscripción de instrucciones notariales (Por ej. por desaparición de la empresa prestadora del servicio cloud; ante la negativa injustificada a dar soporte o los servicios de mantención contratados dentro de los plazos establecidos; entre otros).

Si se comprenden up-grades (mejoras) o up-dates (actualizaciones), según las bases de licitación, es necesario reflejar claramente los requisitos para su procedencia.

Es importante que, tratándose de SaaS, se incluya una forma de exportar los datos, disminuyendo el riesgo de una figura de *vendor lock-in*, permitiendo usarlos si hay cambio de plataforma.

- Cláusula de acuerdos de nivel de servicio (SLA)

Es importante incluir cláusulas sobre el nivel de servicio que el proveedor cloud se compromete a cumplir, de acuerdo con tiempos realistas, según lo que ofrece el mercado.

Los acuerdos de nivel de servicio deben ser objetivos, medibles y estar relacionados directamente con el servicio que se va a proveer, pudiendo establecerse, si corresponde y de común acuerdo, según las necesidades del órgano público contratante y las características del servicio que brinda el proveedor.

No debe olvidarse vincular el incumplimiento de los niveles de servicio con medidas concretas como multas, cobro de garantía o término anticipado, según la gravedad.

- Cláusula de acceso a sistemas

Si el personal del proveedor del servicio cloud requiere acceso a los sistemas del órgano comprador, se sugiere fijar un procedimiento para ello, indicando claramente el tipo de información, sistemas, equipos y lugares sobre los que autoriza el acceso y aquellos que están prohibidos.

- Cláusula de responsabilidad

Se sugiere incluir cláusulas de responsabilidad por hechos imputables al incumplimiento directo del proveedor del servicio cloud. No obstante, también es importante considerar que algunas indisponibilidades de servicio pueden deberse a fallas propias del hardware o del software, o bien pueden ser ocasionadas por el propio usuario o por terceros, sobre las cuales no correspondería, en principio, imputar responsabilidad para el proveedor.

Sin perjuicio de lo anterior, cabe recordar que no se pueden establecer cláusulas que eximan de responsabilidad por incumplimiento o que limiten ampliamente la responsabilidad civil del proveedor, porque implicaría una renuncia anticipada de derechos por parte del órgano público, que no se permite.

- Cláusulas de políticas de uso aceptable

Las entidades deben comprometerse a utilizar los servicios cloud de forma adecuada y ajustándose a la legislación vigente, evitando usarlos:

- De alguna forma prohibida por ley, reglamento u otra normativa;
- Para infringir los derechos de las personas;

- Para intentar obtener un acceso no autorizado a —o causar disrupción en— cualquier servicio, dispositivo, dato, cuenta o red;
- Para enviar correo no deseado (spam) o distribuir software malicioso;
- De algún modo que pueda causar daños a la provisión de los servicios u obstaculizar el uso del servicio por parte de otras personas.

- Cláusulas más específicas para servicios en la nube (Cloud Computing)

Se sugiere contratar directamente con el prestador del servicio cloud, es decir, con quien se obliga a llevar adelante el servicio *(Por ej. quien almacena la información y protege la confidencialidad de los datos)*. Sin perjuicio que siempre deben considerarse las condiciones generales del servicio ofertado y las necesidades del órgano público contratante, independiente de si se trata de una contratación directa o a través de un representante o partner.

Es importante que el contrato con el proveedor del servicio cloud considere los estándares de seguridad y continuidad operativa comprometidos, en especial respecto del cuidado de los datos (Por ej. a través del cifrado en su almacenamiento y transmisión).

Incluya obligaciones de transparencia del proveedor del servicio cloud, por ejemplo, para conocer la ubicación geográfica de los servidores que almacenan los datos (señalando, al menos, la ciudad en que se encuentran sus servidores), recibir notificaciones oportunas frente a incidentes de seguridad y contemplar condiciones de acceso a reportes de auditoría y certificaciones internacionales independientes.

Se recomienda considerar la posibilidad de recuperar y descargar los datos que se encuentren en dependencias o sistemas del proveedor cloud o sus subcontratistas, para poder migrar la información, sin mayores costos, a un nuevo proveedor, una vez terminado el contrato.

- Cláusulas sobre control de cambios

Cualquier proyecto complejo puede requerir contratos adicionales al contrato principal, para cubrir posibles requerimientos no dimensionados originalmente. Sin embargo, este tipo de contratos pueden significar un cambio en las condiciones originales de la licitación y, por lo tanto, no pueden ser ilimitados y deben definir correctamente el procedimiento de compra aplicable. Por regla general, necesitará una nueva licitación pública, a menos que logre configurarse una causal de trato directo o se predefinan aspectos y límites de cambios pre acordados a fin de permitir agilidad de respuesta a nuevos requerimientos.

En virtud de lo anterior, puede fijar en las bases de licitación un porcentaje máximo para los controles de cambio o consumos adicionales. El referido porcentaje debe estar en relación con el monto y naturaleza del contrato y/o la complejidad del proyecto que se trate.

Sin embargo, en caso de que se modifique el contrato, dicha posibilidad debe encontrarse prevista en las bases de licitación y no podrá alterar la aplicación de los principios de estricta sujeción a las bases y de igualdad de oferentes, así como tampoco podrá aumentarse el monto del contrato más allá de un 30% del monto originalmente pactado.

- Cláusulas sobre gestión del contrato

Si procede, de acuerdo con la naturaleza del servicio contratado, se recomienda indicar en el contrato la constitución de un comité de administración del contrato, compuesto por funcionarios de alto nivel del órgano comprador, con facultades suficientes para poder realizar una adecuada administración del contrato.

Dicho comité es independiente del nombramiento de un encargado de proyecto que actúe como contraparte técnica frente al proveedor del servicio cloud. Dicho encargado suele reportar al comité. Se recomienda analizar cuidadosamente las habilidades y conocimientos necesarios para ejercer esta función. En caso de no existir un perfil adecuado en el organismo, se sugiere buscar apoyo externo.

- Cláusulas sobre cierre y traspaso del contrato

El cierre del contrato corresponde a la finalización de la relación contractual entre las partes. Es un proceso normal en cualquier relación contractual. Sin embargo, cuando la relación ha durado mucho tiempo, puede ocurrir que realizar este cierre no sea simple.

Por esa razón se recomienda incorporar en las bases de licitación y en el posterior contrato, o bien definirlo como un aspecto a ser ofertado individualmente por cada oferente y materia de evaluación, cláusulas que regulen este punto. Dichas cláusulas deben considerar, por ejemplo:

- Calendario de cierre: Establezca un evento o plazo prudencial a partir del cual se entiende que el contrato entre en etapa de cierre.
- Protocolo de fin de contrato: Dicho protocolo –suscrito por ambas partes- contiene el detalle de todas las actividades a realizar y los responsables de cada una de ellas, para lograr un cierre de contrato ordenado. Este protocolo puede incluir, según el tipo de proyecto, elementos como la entrega de códigos fuente, licencias, datos, documentación, soporte técnico, parametrización de sistemas, transferencia de *know how,* destrucción de información de propiedad del contratante, entre otros.
- Pagos finales: Dentro del esquema de pagos del servicio, una parte debería estar asociada al cumplimiento cabal por parte del proveedor cloud del cierre del contrato. Uno de estos hitos puede ser la firma de un documento donde las partes declaren que el contrato se ha cerrado sin inconvenientes.
- Transición de un contrato a otro: Cuando el contratante externaliza procesos operacionales o de negocio a un privado, el cierre de contrato puede estar asociado al traspaso de las operaciones de un proveedor del Servicio Cloud a otro.

- Cláusulas sobre término anticipado

Se recomienda que las bases establezcan causales de término anticipado del contrato basadas en incumplimientos objetivos y demostrables, según la naturaleza del servicio contratado, considerándose previamente un plazo razonable para subsanar el eventual incumplimiento. En lo posible, limitarse a causales legales, objetivas, a fin de evitar que la definición de dichas causales impida la posibilidad de participar de algunos oferentes.

Adicionalmente, se sugiere regular para estos casos la continuidad del servicio, estableciendo plazos y procedimientos que aseguren la transición al igual que para el cierre del contrato, o bien señalar que ello debe ser también materia para evaluar en las ofertas.

Las cláusulas de término anticipado por parte de la entidad pública deben ser objetivas y fundarse en el mutuo acuerdo o en incumplimientos graves por parte del proveedor cloud, que se encuentren claramente definidos en las bases de licitación, con el fin de no incurrir en incertidumbre.

Asimismo, se recomienda establecer la posibilidad del término anticipado unilateral por parte del órgano público, por razones de mérito que le permitan, por ejemplo, aprovechar nuevas tecnologías que ofrezca el mercado.

- Cláusulas sobre pago

Se recomienda a los compradores poner en conocimiento público las tarifas de los servicios contratados en la red. También, permitir la flexibilidad en los precios contratados, a través de modificaciones en los contratos en caso de que, por avances tecnológicos, los precios de los servicios entregados disminuyan y, en general, que se adecuen a las variaciones del mercado con servicios mínimos garantizados.

6.4.4.- Comportamiento contractual

El comportamiento del proveedor durante la ejecución de un contrato es una información útil para futuros procesos de compra de otros órganos públicos. Esa reputación comercial permite conocer mejor a los oferentes, especialmente a los más pequeños y nuevos, y podría ser un criterio de evaluación.

Por su parte, el comportamiento del órgano público comprador también es importante para la confianza de los proveedores, respecto del pago oportuno, el cumplimiento de plazos de validación u otros factores. Para ello, el órgano público podría incorporar una buena práctica de evaluación a su nivel de cumplimiento como comprador, por parte de sus proveedores.

6.4.5.- Transición de un contrato a otro

En ciertos servicios en que el órgano contratante externaliza procesos operacionales o vinculados directamente con sus funciones públicas a un proveedor del servicio cloud, el término del contrato puede estar asociado al traspaso de las operaciones de un proveedor a otro.

Por lo tanto, regule una transición colaborativa entre dichos proveedores (Por ej. que incluya entrenamiento a los agentes del nuevo proveedor, traspaso de procedimientos, apoyo en las nuevas configuraciones de los sistemas de soporte, etc.).

Deberá regularse la compatibilidad tecnológica entre los proveedores cloud, especialmente respecto de la interoperabilidad de su infraestructura y datos. Asimismo, deberá regularse el

destino y traspaso de los registros y metadatos generados durante las operaciones para mantener la integridad de los datos y prevenir interrupciones del servicio.

Otro aspecto relevante será la regulación de la responsabilidad civil en la custodia de los datos, especialmente durante su transferencia entre proveedores cloud.

Se recomienda preferir soluciones interoperables y que sean herramientas tecnológicas estándares, ya que éstas van a facilitar la transición entre contratos que se necesitan de forma constante en el tiempo.

De igual manera, se recomienda determinar migraciones parcializadas, por hitos de ejecución de éstas, como SLA.

ANEXO

CLÁUSULAS SUGERIDAS

Los órganos de la Administración del Estado son libres de determinar las modalidades y cláusulas propias de la contratación de servicios cloud. Sin embargo, el presente documento propone cláusulas que podrían ser utilizadas y/o ajustadas al contratar un servicio de esta naturaleza:

1. Confidencialidad, protección y conservación de datos

Para los efectos del presente contrato, se entenderá por "Información Confidencial" a toda información, sea completa o parcial, verbal o escrita, independiente del medio en que conste o se transmita, que las partes reciban la una de la otra y que sea designada como tal.

La Información Confidencial será mantenida en estricta reserva por las partes, quienes deberán mantener la debida confidencialidad de los datos, bases de datos, documentos y a todos los archivos informáticos a que tenga acceso con motivo del presente contrato, quedándole expresamente prohibido divulgarlos, publicarlos, fotocopiarlos, copiarlos o distribuirlos a terceros extraños a este contrato o hacer cualquier uso indebido de ellos. Estas informaciones y datos sólo podrán ser revelados por instrucción de la parte divulgadora.

No se considerará Información Confidencial (1) la información que llegue a ser de dominio público sin que medie un incumplimiento de este contrato, (2) la información que la parte receptora reciba lícitamente de otra fuente sin una obligación de confidencialidad, (3) la información que se desarrolle de manera independiente, o (4) la información que constituya un comentario o sugerencia ofrecida voluntariamente acerca del negocio, los productos o servicios de la otra parte.

El proveedor guardará especial atención y se obliga a mantener la confidencialidad de los datos a que pueda tener acceso en virtud del presente contrato. En este sentido, el proveedor no podrá recolectar, almacenar, transferir, transmitir, comunicar, tratar, ceder o usar, de cualquier forma, los datos indicados anteriormente, salvo que dichas acciones sean necesarias para el cumplimiento de las obligaciones consignadas en el presente contrato y/o que medie una autorización escrita por parte del representante legal del órgano contratante.

En ningún caso se entenderá que el proveedor tiene algún derecho sobre datos personales que se le han entregado, ni se entenderá que su titular ha prestado su consentimiento para dicho tratamiento.

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

Los consultores y personal dependiente del proveedor, que de una u otra manera se hayan vinculado a la ejecución de los servicios contratados, en cualquiera de sus etapas, deberán guardar confidencialidad de la misma forma aplicable al proveedor.

Toda la Información Confidencial (incluyendo las copias tangibles y la almacenada por medios electrónicos y/o cualquier otro medio) proporcionada por el órgano contratante será devuelta a éste dentro de los 30 días corridos contados desde la recepción de un requerimiento escrito por el órgano contratante. Para dichos efectos, el proveedor entregará al órgano comprador todos los materiales que contengan o representen la Información Confidencial recibida. Hecho lo anterior, el proveedor no podrá mantener ninguna Información Confidencial del órgano contratante en su poder, debiendo eliminar de forma irreversible cualquier copia de dicha información que disponga en sus registros lógicos y físicos.

En todo momento durante el periodo de vigencia del contrato, el órgano comprador tendrá el derecho de acceder a sus datos almacenados, así como tendrá también la capacidad de extraerlos, a su cuenta y riesgo. El proveedor conservará los datos de la entidad almacenados en éste, en una cuenta con funcionalidad limitada durante los 60 días siguientes a la expiración o terminación del contrato, de tal modo que la entidad pueda extraer los datos. Una vez que finalice el periodo de conservación de 60 días, el proveedor deshabilitará la cuenta del órgano comprador y eliminará sus datos.

2. Seguridad de la información.

"El proveedor deberá adoptar todas las medidas técnicas y organizativas de seguridad que sean efectivas para efectos de evitar que la información del órgano contratante sea accedida por terceros no autorizados.

Lo anterior se extiende, además, a las comunicaciones electrónicas de dicha información entre el proveedor y el órgano comprador.

En tal caso, el proveedor deberá emplear las medidas seguridad que sean necesarias y adecuadas para que estas comunicaciones no sean interceptadas.

Para lo anterior, seguirá los estándares de seguridad establecidos en el decreto N°83, de 2004, del Ministerio Secretaría General de la Presidencia, sobre seguridad y confidencialidad de los documentos electrónicos, o aquella norma que lo reemplace".

3. Notificación de incidentes de seguridad

Si el Proveedor tuviese conocimiento de cualquier acceso ilícito a los datos de la entidad y sus datos de soporte, almacenados en sus equipos o instalaciones, o tuviese conocimiento de un acceso no autorizado a dichos equipos o instalaciones y, tuviera como resultado la pérdida, revelación o alteración de los datos de la entidad (en adelante cada uno un "Incidente de Seguridad"), el proveedor deberá sin demora (1) notificar el Incidente de Seguridad al órgano comprador; (2) investigar el Incidente de Seguridad y proporcionar a la entidad información

detallada sobre el Incidente de Seguridad; y (3) tomar medidas razonables para mitigar los efectos y minimizar los daños resultantes del Incidente de Seguridad.

Las notificaciones de Incidentes de Seguridad se remitirán a uno o más administradores de la entidad a través de cualquier medio que el proveedor seleccione, incluyendo correo electrónico. Es responsabilidad exclusiva de la entidad asegurarse de que sus administradores mantengan en todo momento datos de contacto exactos y actualizados. La obligación del proveedor de notificar o responder a un Incidente de Seguridad según lo previsto en esta sección no constituye reconocimiento por parte del proveedor en cuanto a incumplimiento o responsabilidad alguna con respecto al Incidente de Seguridad.

La entidad deberá notificar al proveedor, sin demora, acerca de cualquier posible uso indebido que se haya producido en sus cuentas o credenciales de autenticación, o acerca de cualquier incidente de seguridad relacionado con la prestación de los servicios contractuales.

4. Fuerza mayor o caso fortuito

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

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

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

(a) El embargo de los bienes del proveedor.
(b) Las acciones que pueda ordenar las autoridades competentes que impidan al proveedor desarrollar su labor por no cumplir con las disposiciones legales o reglamentarias que le correspondan.
(c) La huelga de los trabajadores del proveedor o de alguno de sus contratistas o subcontratistas.

5. Legislación aplicable y resolución de controversias.

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

Ante cualquier dificultad que se suscite entre las partes de este contrato respecto de la existencia, validez, exigibilidad, resolución, término, interpretación, aplicación, cumplimiento o suscripción del mismo o por cualquier otra razón relacionada con este contrato, las Partes se

someterán a la jurisdicción y competencia de los tribunales ordinarios de justicia de la ciudad de XX, comuna de XX.

6. Medidas para mantener la continuidad del servicio

En caso de término del contrato, anticipado o no, proveedor deberá entregar al órgano comprador la información utilizada en la prestación de los servicios hasta ese momento, de modo de habilitar cualquier solución que éste defina.

Durante el período que media entre la notificación de la terminación y la fecha en que se ésta se hará efectiva, el proveedor deberá prestar toda la colaboración que el órgano contratante *le requiera para que este último pueda traspasar a otro prestador la operación del servicio, de manera que se mantenga la continuidad de este, en todo momento.*

Adicionalmente, se podrán aplicar todas las medidas tendientes a mantener la continuidad de servicio que deba efectuar el órgano contratante*, por cuenta, costo y riesgo del proveedor, previa notificación al mismo y para aquellos casos en que la terminación le sea imputable a este último, de conformidad a las causales establecidas en el contrato.*

7. Protección de Datos Personales

El proveedor se compromete a observar lo establecido en la ley N° 19.628 de Protección de la Vida Privada y demás legislación chilena aplicable, respecto de la protección de datos personales.

En particular, deberá destruir o eliminar los datos de carácter personal o cualquier soporte o documento en que éstos se incorporen, a la finalización del presente contrato o por requerimiento expreso y por escrito del órgano comprador.

Las obligaciones derivadas de la presente estipulación se extinguirán en el momento en que los datos de carácter personal hayan sido completamente borrados o eliminados del equipo de almacenamiento de datos o de algún modo, destruidos o convertidos en inaccesibles.

El proveedor se compromete a adoptar, actualizar y mantener las medidas organizativas y técnicas que estime necesarias para garantizar la seguridad y confidencialidad de los datos de carácter personal, impidiendo cualquier alteración, perdida, tratamiento, procesamiento o acceso no autorizado. Esta obligación se desarrollará de conformidad con el estado de la tecnología, la naturaleza de los datos y los riesgos a los que estén expuestos ya sea que provengan de la acción humana o del medio físico o natural.

8. Tratamiento de datos personales por Mandato

Por la presente disposición se encarga al proveedor el efectuar tratamiento de datos personales, por cuenta del órgano contratante.

Dicho mandato tiene por objeto [indicar la finalidad del mandato] y recae sobre los siguientes tipos de datos personales: [indicar los tipos de datos personales que se utilizarán]

El tratamiento durará exclusivamente durante la vigencia del presente contrato o hasta cumplir la finalidad del encargo, si ello ocurriera antes. Ocurrido cualquiera de los casos mencionados precedentemente, el proveedor deberá realizar la devolución de los datos y su eliminación efectiva.

Por último, queda expresamente prohibido el uso de dichos datos personales para fines distintos a los indicados en esta cláusula, quedando además expresamente prohibida su comunicación a terceros.

9. Uso de los datos de la entidad pública

Los datos de la entidad se utilizarán únicamente para prestar al órgano comprador los servicios contratados, incluyendo finalidades compatibles con la prestación de dichos servicios.

El proveedor no utilizará los datos de la entidad —ni derivará información de ellos— para finalidades publicitarias o finalidades comerciales similares. Por lo que respecta a las partes, la entidad conserva todos los derechos, la titularidad y los intereses sobre sus datos.".

2. **PUBLÍQUESE** en www.chilecompra.cl.

Anótese, Comuníquese y Archívese

TRINIDAD INOSTROZA CASTRO
DIRECTORA
DIRECCIÓN DE COMPRAS Y CONTRATACIÓN PÚBLICA

DIRECTORA

RMZ/RHB/JCP/DRM/PMS/AVH
Distribución:
- Fiscalía
- División Convenio Marco
- División de Tecnología