PROPUESTA DE
ACUERDO MARCO
SOBRE LA NUBE

COMPRA SERVICIOS CLOUD EN ESPAÑA

JULIO DE 2020

Ametic
LA VOZ DE LA INDUSTRIA DIGITAL

Contenido

1 Acuerdo Marco es un método efectivo para la compra de servicios en la nube

La finalidad de esta propuesta es exponer las características de un posible Acuerdo Marco de servicios Cloud en España.

El surgimiento de la informática en la nube como primera opción para las necesidades tecnológicas del sector público hace necesario modernizar las estrategias de adquisición existentes. Si bien es cierto que las Administraciones públicas en España han sido exitosas en la adopción de nuevas tecnologías dentro de sus procesos y operaciones, la evolución de estas aplicaciones requerirá la adopción paulatina de servicios en la nube. Estos servicios ofrecen un amplio abanico de posibilidades, tanto desde el punto de vista de costes, como desde el punto de vista de agilidad y facilidad para innovar.

Los procesos de adquisición centrados en la nube permiten a las entidades obtener todos los beneficios de la nube, como el acceso a innovaciones punteras, velocidad y agilidad, mejoras en la seguridad y en la gestión del cumplimiento normativo. Todo ello logrando una mayor eficacia y ahorro de costes. Actualmente el proceso de adquisición de estos servicios es complejo y largo.

Los métodos de adquisición de TI tradicionales no son aplicables a la compra de servicios en la nube. La reutilización de enfoques actuales de compra de TI tradicional (incluido el llamado "hosting") pueden eliminar los beneficios inherentes de la nube.

Uno de los métodos más efectivos de adquisición de servicios en la nube en el sector público es el **Acuerdo Marco**. En España, este Acuerdo Marco puede configurarse como una licitación de dos pasos. La Administración responsable de centralizar las compras realiza una primera licitación, en la que habilita a varios proveedores de servicios en la nube (CSPs) y sus socios/distribuidores a prestar el servicio dentro de este Acuerdo Marco. Adicionalmente, los entes adscritos al Acuerdo Marco (la Administración contratante) realiza una segunda licitación, centrada en un proyecto concreto. De este modo se asegura que el servicio prestado a la Administración contratante cumple con los rigurosos estándares del sector público, al mismo tiempo que agiliza y facilita la contratación para las distintas administraciones adscritas a la compra centralizada.

2 La gobernanza de contratos de nube

2.1 Para garantizar la agilidad de la ejecución del contrato es necesario adoptar el modelo de responsabilidad compartida y delimitar bien los roles

En el caso de adopción del ejemplo propuesto anteriormente, en este Acuerdo Marco estarán involucrados diferentes actores con distintas responsabilidades. Es importante hacer que el modelo de organización implementado sea claro y transparente para todos los actores:

1. El tipo de relación entre los proveedores de servicios en la nube, los socios o distribuidores de estos proveedores (como revendedores e integradores), la autoridad de compra centralizada y las administraciones adscritas al Acuerdo Marco.
2. Los roles dentro de la Administración, por ejemplo: ¿quién compra?, ¿quién explota?, ¿quién presupuesta ?, ¿quién establece la seguridad ?, ¿controla los gastos?, ¿quién "distribuye"? ¿Cuál es el modelo económico de los agentes involucrados (revendedor, integrador, poder adjudicador) ?;
3. La responsabilidad de cada uno de los actores intervinientes.

La responsabilidad compartida es un aspecto fundamental en los contratos de servicios en la nube. Es muy importante, que dentro de los pliegos del Acuerdo Marco y de las segundas licitaciones el concepto de responsabilidad compartida sea perfectamente delimitada. Esto es importante, porque permite ganar agilidad a cada actor involucrado y centrarse en la parte del proyecto que le corresponde.

La responsabilidad compartida no solo aplica a la seguridad de las aplicaciones basadas en la nube, sino a todos los conceptos inherentes al proyecto como: control de consumo y costes, control de disponibilidad y recuperación de desastres, control y gestión de los datos, etc.

La Administración contratante debe ser consciente de cuál es la responsabilidad del proveedor de servicios en la nube y cuál seguirá siendo su responsabilidad. Por ejemplo, un CSP ofrece capacidades de cifrados, pero es responsabilidad de la Administración contratante o de un socio asegurarse de que los datos estén cifrados.

Además, los usuarios de la nube deben comprender cómo la red de socios de un CSP ayuda a los clientes a usar la nube y delegar sus responsabilidades. Por ejemplo, un proveedor de servicios gestionados (*Managed Service Provider* = MSP) puede ayudar a configurar en nombre de las administraciones los servicios de control ofrecidos por un CSP para cumplir con sus requisitos únicos de cumplimiento y auditoría.

El CSP **proporciona** los servicios.

La Administración contratante configura y **utiliza** los servicios.

Los socios (si es necesario) **ayudan** a la Administración contratante a **usar / configurar** los servicios.

2.2 La estructura contractual debe favorecer una ágil y rápida contratación en las segundas licitaciones

Como se ha comentado anteriormente, la estructura ideal de este acuerdo marco requerirá dos licitaciones: una para homologar los distintos CSPs y sus distribuidores y otra para elegir la solución concreta en cada caso. Para crear condiciones favorables para el éxito de esta iniciativa, la estructura del contrato en la nube debería:

- Permitir a las administraciones públicas elegir entre varios CSP.
- En la primera licitación es necesario hacer la suficiente precalificación para asegurar el nivel de requisitos (administrativos, financieros, técnicos de seguridad y cumplimiento normativo) necesario para la gran mayoría de usos en el sector público. Definir un alto estándar de calidad de servicio para los CSP y los socios de CSP (integrador / MSP / distribuidor), de modo que los proyectos relacionados con la nube en España se lleven a cabo de manera eficiente y que la adopción se acelere gracias a ejemplos positivos de los primeros proyectos.
- Evitar un modelo en el que una única empresa (tipo "agente de la nube") venda servicios de varios CSP garantizando de esta forma que haya diversidad de ofertas de agentes homologados.
- Asegurar que las segundas licitaciones sean rápidas y flexibles, cubriendo una gran parte de requisitos generales en la primera licitación del Acuerdo Marco.

3 Comparación de ofertas

3.1 Los requisitos administrativos deben garantizar que la Administración contratante accede a las mejores soluciones en el mercado (primera licitación)

Para asegurar que las Administración Públicas reciban los mejores servicios de TI en la nube, es necesario establecer un riguroso proceso de precalificación de los CSPs y sus distribuidores o socios. El objetivo es crear una lista restringida, con criterios objetivos para poder comparar a los CSPs o sus distribuidores y elegir, en una primera licitación, una lista de las tecnologías y distribuidores que formarán parte del Acuerdo Marco. Esta dentro de la responsabilidad de la entidad gestora del Acuerdo Marco definir estos criterios.

Ejemplos de tales criterios podrían ser que el CSP debe tener certificaciones ENS nivel alto o certificaciones ISO 27017 y 27018, experiencia en proyectos similares, estar en los informes de los analistas independientes, como el Cuadrante Mágico de Gartner, etc. En el **Anexo 1 – Criterios de evaluación** se describen los criterios aplicables en esta fase junto con los motivos de inclusión.

3.2 Los requisitos técnicos deben garantizar que la solución es la mejor para un proyecto concreto (tanto en la primera como en la segunda licitación)

Dentro de la fase de primera licitación se podrán delimitar criterios técnicos generales aplicables a la infraestructura y capacidades de los CSPs. Criterios técnicos más específicos para cada proyecto concreto tendrán que establecerse en las segundas licitaciones.

Para todas las posibilidades que ofrece la industria, es recomendable evitar ser muy prescriptivo sobre las características técnicas, la implementación de la seguridad, los modelos de precios, los niveles de servicio (SLA), las cláusulas contractuales (en particular, las condiciones de uso de los servicios). Se debe tener en cuenta que los productos y soluciones basadas en la nube evolucionan rápidamente y no son homogéneas entre ellas.

Con preguntas abiertas cada proveedor podrá ofrecer su oferta de servicios estándar. En el **Anexo 1 – Criterios de evaluación** se describen los criterios aplicables en la fase de primera licitación junto con los motivos de inclusión.

3.3 Comparación por criterios de coste (segundas licitaciones)

3.3.1 Los criterios de coste deben incluir todas las características del servicio a comparar ya que estos ofrecen diferentes prestaciones dependiendo del CSP

Al diseñar los criterios para comparar los distintos CSP, es importante desarrollar un enfoque que tenga en cuenta las características únicas de la nube. Por ejemplo, entender que simplemente comparar unidades de trabajo entre ofertas del proveedor de la nube (por ejemplo, instancias de cómputo o almacenamiento) no es una forma efectiva de comparar ofertas. De hecho, (1) el catálogo de precios de un CSP puede ser muy variado y amplio (2) los modelos de precios son diferentes de un proveedor a otro para servicios similares, (3) a priori, servicios similares ofrecen distintos niveles de servicio. Por ejemplo, en caso de servicios de almacenamiento de objetos, no es suficiente con solo comparar el coste por GB. Diferentes proveedores de nube pueden tratar de forma distinta la información almacenada: por ejemplo,

algunos proveedores pueden ofrecer replicación automática entre tres clústeres de centros de datos en una misma región geográfica para ofrecer una alta durabilidad y disponibilidad de objetos, mientras que otros almacenan la información en un solo centro de datos.

3.3.2 Es importante valorar el coste total de propiedad

Recomendamos que la comparación se enfoque en el coste total de propiedad (TCO) en un caso de uso definido, que tenga en cuenta todos los aspectos de una solución (incluidos los servicios de los socios), descuentos estándar de los CSP disponibles comercialmente (como reservas de instancias o pagos por adelantado), características técnicas que pueden reducir y optimizar costes, etc.

3.3.3 Pueden definirse casos de uso típicos y las características principales para comparar las ofertas

El proceso de evaluación puede considerar los escenarios típicos que corresponden a ciertos sistemas o aplicaciones habituales. Tales escenarios (por ejemplo, alojamiento web, ejecutar un sistema de recursos humanos con x número de usuarios, etc.) pueden incluir variables como:

- La velocidad de despliegue y el alcance de los recursos requeridos
- Tiempos de respuesta
- Escalabilidad (por ejemplo, identificar cuantas conexiones simultaneas deba poder soportar un sistema determinado)
- Características específicas por tipo de almacenamiento (durabilidad de los datos, disponibilidad, tiempo necesario para acceder a datos en cada tipo de almacenamiento)
- Cuantas copias redundantes del objeto estarán disponibles en caso de fallo de uno de los sistemas
- Requisitos específicos de seguridad o cumplimiento.

Los escenarios deben estar bien definidos para incluir la gama de servicios que el cliente probablemente usará durante el proyecto. De esta manera, el cliente puede comparar el coste total estimado del proyecto.

3.3.4 Es necesario analizar todas las características que el CSP pone a disposición del cliente

Algunos de los servicios o características que ofrecen los proveedores de la nube pueden no tener un coste específico, pero sí proporcionar valor al cliente. Este tipo de servicios o características también pueden ser parte evaluable dentro de los pliegos del sector público. Ejemplos de tales características podrían ser:

- Herramientas de análisis y control de servicios desplegados en la nube que proporcionan consejos automáticos sobre cómo reducir los costes y mejorar el rendimiento y la seguridad.
- Servicios de "infraestructura como código" que permita utilizar un archivo de texto simple para modelar y poner a disposición, de manera automatizada y segura, todos los recursos necesarios para sus aplicaciones en todas las regiones y cuentas.
- Visualización de los recursos y aplicaciones en la nube
- Servicios de protección contra DDoS (ataques de denegación de servicio) administrados que protegen las aplicaciones que se ejecutan en la nube.
- Gestión de Identidades y Acceso (IAM) que permite controlar de forma segura el acceso a los servicios y recursos de la nube.

Los criterios de evaluación pueden redactarse para permitir que los CSP indiquen las funciones incluidas de manera predeterminada y cómo estos servicios tienen un impacto en el coste total.

3.3.5 El abanico de servicios y modelos de precio de CSP debe posibilitar la optimización de las aplicaciones

Se podrán incluir criterios de evaluación que midan la capacidad de optimizar la aplicación final con métodos de optimización como descuentos basados en un compromiso de uso e instancias reservadas. Por ejemplo:

1. x% de ahorro si los clientes compran instancias reservadas (1 año, 3 años, etc.).
2. y% de reducción sobre la factura por un compromiso de volumen determinado.
3. z% de ahorro en promedio basado en revisiones de optimización de arquitectura e infraestructura.

Hay que tener en cuenta el coste durante la duración total de la propiedad y cómo los métodos de optimización pueden reducir estos costes (por ejemplo, el uso creciente de las funciones sin servidor de un CSP puede reducir los costes en un x%, al convertir servicios a arquitecturas "serverless").

4 Contratación

4.1 Los términos y condiciones de los proveedores de la nube suelen ser estándar

Los servicios y operaciones de los CSP están estandarizados por naturaleza, por lo tanto, las condiciones contractuales también lo son. Sin embargo, existe la capacidad de ajustar estos contratos levemente para adaptarse a los contextos legislativos y reglamentarios locales.

Se recomienda que se evalúen y se adopten las condiciones de servicios estándar de los proveedores CSP en la primera licitación del Acuerdo Marco. También es importante que, en sucesivas licitaciones, no se incluyan términos que no son compatibles con la nube pública.

5 Glosario

CSP (Cloud Solution Provider): Proveedores de Servicios en la Nube
DDoS (Denial of Service): ataque de denegación de servicios,
ENS Esquema Nacional de Seguridad
IAM (Identity and Access Management). Gestión de Identidades y Acceso
MSP (Managed Service Provider): Proveedor de Servicios gestionados
SLA (service level agreement): Nivel de servicio
TCO (Total Cost of Ownership): Coste total de propiedad

Anexo 1 – Criterios de evaluación

Criterios administrativos

Criterios de calificación propuestos	*Motivo*
Detalles organizativos; por ejemplo: Nombre, Forma jurídica, Número de identificación fiscal, etc.	
Tamaño de la empresa, situación económica y financiera[1]	*El cliente puede determinar si el CSP podrá cumplir el contrato.*
Motivos de exclusión; p. ej., actividades delictivas o fraudulentas, etc.	
Casos prácticos y referencias del cliente (especifique el número o el tipo de requisito)	*El cliente puede medir la experiencia del CSP para ofrecer los servicios solicitados.*
Compromisos y prácticas de sostenibilidad disponibles públicamente.	*El cliente puede ver si un CSP está comprometido con dirigir su negocio de la forma más respetuosa con el medio ambiente.*
El CSP debe demostrar una trayectoria probada en innovación y lanzamiento de nuevos servicios y funciones útiles a lo largo de los últimos 5 años	*Demuestra que el CSP trabaja para poner nuevos productos a disposición de los clientes con rapidez, y que a continuación itera rápidamente y mejora los productos. Ayuda a los clientes a mantener una infraestructura de TI de vanguardia sin tener que realizar inversiones de recapitalización.*

Criterios técnicos

Criterios de calificación propuestos para el CSP	*Motivo*
Infraestructura	
La infraestructura del CSP debe ofrecer al menos 2 clústeres de centros de datos en una región geográfica determinada. Cada clúster debe estar formado por al menos 2 centros de datos conectados mediante un enlace de baja latencia que permita realizar implementaciones en modo activo/activo de alta disponibilidad y de escenarios DR-BC (Disaster Recovery/Business Continuity). Los centros de datos que conforman cada clúster deben estar aislados físicamente y ser independientes en caso de fallo entre sí.	*El CSP debe poder ofrecer una infraestructura adecuada para crear aplicaciones de alta disponibilidad en las que se pueden evitar puntos únicos de error.*

[1] La licitación de servicios en la nube se centra en la información empresarial de alto nivel, sin entrar en detalles específicos del número de empleados de la empresa y la estructura de equipos de los empleados internos. Con la tecnología basada en la nube no existe ninguna correlación entre el rendimiento del servicio y el número de empleados. En su lugar, las licitaciones de nube se centran en el tamaño global de la empresa para satisfacer los requisitos (la escala adecuada), así como en una experiencia eficiencia probada.

Criterios de calificación propuestos para el CSP	*Motivo*
El CSP deberá informar sobre los países donde los datos del cliente serán alojados y procesados.	*El cliente debe tener visibilidad sobre la ubicación de los datos, las opciones técnicas de las que dispone para controlar dicha ubicación, y en su caso, de los mecanismos de transferencias internacionales que pone a disposición del cliente de conformidad con la normativa vigente sobre protección de datos. En función del caso de uso concreto, el cliente deberá poder valorar qué tipo de soluciones y controles debe desplegar para cada proyecto en función de sus necesidades.*
El CSP debe tener la capacidad de ofrecer una conectividad directa, dedicada y privada entre los centros de datos del CSP.	*La conectividad privada es un requisito fundamental para poder crear una infraestructura híbrida y segura.*
El CSP debe proporcionar los mecanismos suficientes, que incluyen el cifrado de los datos en tránsito.	*El cliente puede exigir que haya una capacidad por la que ningún dato pueda transitar sin cifrar.*
Certificaciones mínimas del CSP	
El CSP debe contar con la certificación ISO 27001, 27017, 27018 y ENS (Esquema nacional de seguridad) nivel alto	*La realización de una auditoría y la obtención de una certificación y una acreditación de terceros garantiza que los clientes puedan realizar análisis comparativos de los servicios (y en concreto de la plataforma) en cuanto a calidad, seguridad y fiabilidad. Es imprescindible que se cumplan un mínimo de certificaciones.*
El CSP debe ofrecer servicios que cumplan con la normativa vigente sobre protección de datos	*El cliente debe poder crear o ejecutar aplicaciones compatibles con el RGPD, por lo que la oferta de servicios y herramientas compatibles con el RGPD debe ser un requisito previo.*
El CSP debe facilitar informes auditados de terceros, como los informes SOC 1 y 2 (que cubren las ubicaciones y los servicios que utiliza la Comisión Europea) que permitan conocer sus controles y procedimientos.	*El CSP debe ser transparente en lo referente al funcionamiento y la administración de la aplicación. Los informes SOC son un medio para garantizar la confianza y la transparencia.*
Características del servicio	
La infraestructura del CSP debe estar accesible a través de las interfaces programáticas (las API) y la consola de administración basada en Web.	*El acceso de autoservicio y las interfaces programáticas son un estándar necesario de los proveedores del CSP para dejar de mediar tanto como sea posible en el acceso de usuario y del propio proveedor.*
El CSP debe ofrecer un conjunto de servicios de base que incluyan: almacenamiento de objetos, base de datos relacional administrada, base de datos no relacional administrada, balanceadores de carga administrados, monitorización y escalado automático integrado.	*Una simple oferta de máquinas virtuales no es suficiente para que un proveedor pueda cualificarse como proveedor de nube. Los proveedores de nube deben ofrecer un conjunto de servicios PAAS e IAAS para acelerar y mejorar las aplicaciones del cliente.*
El CSP debe permitir al cliente cambiar libremente el uso y la configuración de sus servicios o mover los datos dentro y fuera del CSP (oferta de autoservicio).	*El acceso de autoservicio a los servicios y los datos es un requisito estricto que permite al consumidor ser completamente independiente.*

Criterios de calificación propuestos para el CSP	*Motivo*
El CSP debe permitir una facturación de "pago según el uso" de sus servicios.	*El pago según el uso permite al cliente optimizar los costes de sus cargas de trabajo, minimizar los riesgos y utilizar el CSP para aplicaciones y pruebas de concepto (PdC) de corta duración.*
Seguridad de los datos y el sistema	
Las características del CSP deben proporcionar al cliente un control de sus políticas de seguridad, que incluyen la confidencialidad, la integridad y la disponibilidad de los datos y el sistema del cliente.	*El cliente debe estar habilitado para definir e implementar sus estándares de seguridad en sus cargas de trabajo. Confiar en que el proveedor "hará lo correcto" con los datos del cliente no es suficiente.*
Control de costes	
El CSP debe contar con mecanismos y herramientas que permitan al cliente monitorizar el gasto a lo largo del tiempo. Las herramientas deben hacer posible la segmentación básica de los costes según la carga de trabajo, el servicio y la cuenta.	
El CSP debe ofrecer herramientas para alertar al cliente siempre que se supere el umbral de coste.	
El CSP debe entregar facturas detalladas al cliente. Debe existir la posibilidad de estructurar la factura para dividir los costes por carga de trabajo, entorno y cuenta.	