

10 consideraciones sobre la adquisición en un entorno de nube

Marzo de 2017



© 2017, Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

Avisos

Este documento se suministra únicamente con fines informativos. Representa la oferta actual de productos y prácticas de AWS a partir de la fecha de publicación de este documento. Dichas prácticas y productos pueden modificarse sin previo aviso. Los clientes son responsables de realizar sus propias evaluaciones independientes de la información contenida en este documento y de cualquier uso de los productos o servicios de AWS, cada uno de los cuales se ofrece “tal cual”, sin garantía de ningún tipo, ya sea explícita o implícita. Este documento no genera ninguna garantía, declaración, compromiso contractual, condición ni certeza por parte de AWS, sus filiales, proveedores o licenciantes. Las responsabilidades y obligaciones de AWS con respecto a sus clientes se controlan mediante los acuerdos de AWS y este documento no forma parte ni modifica ningún acuerdo entre AWS y sus clientes.

Contenido

Finalidad	2
Diez consideraciones sobre la adquisición	2
1. Comprender por qué la informática en la nube es diferente	2
2. Planificación temprana para el máximo aprovechamiento de todo el beneficio de la nube	3
3. Evite demasiados requisitos normativos	3
4. Separe la infraestructura en la nube (servicios sin administrar) de los servicios administrados	4
5. Incluir un modelo de precios de servicios	4
6. Aprovechar las acreditaciones de terceros relativas a la seguridad, la privacidad y la auditoría	5
7. Entender que la seguridad es una responsabilidad compartida	7
8. Diseño e implementación del modelo de gobernanza de los datos en la nube	7
9. Especificar términos de un artículo comercial	8
10. Definir los criterios de evaluación de la nube	8
Conclusión	8

Finalidad

Amazon Web Services (AWS) ofrece servicios en la nube escalables y rentables que los clientes del sector público pueden utilizar para cumplir mandatos, reducir costos, impulsar eficiencias y acelerar la innovación.

El proceso de adquisición de servicios en la nube diseñados para prestarse en modo de infraestructura como servicio (IaaS) difiere del proceso de compra de tecnología tradicional. Los enfoques tradicionales de contratación y adquisición del sector público, diseñados para comprar productos como el hardware y el software relacionado, pueden resultar incompatibles con los servicios en la nube (como IaaS). La incapacidad de modernizar los enfoques de contratación y adquisición puede reducir el conjunto de competidores y dificultar la capacidad del cliente para adoptar y aprovechar la tecnología de nube.

Diez consideraciones sobre la adquisición

La adquisición de servicios en la nube constituye una oportunidad excelente para replantearse las estrategias de adquisición existentes, de manera que pueda crear un proceso de adquisición flexible que permita a su organización pública aprovechar al máximo todos los beneficios que brinda la nube. Las siguientes consideraciones de adquisición son componentes clave que pueden constituir la base de una estrategia de adquisición más amplia de la nube en el sector público.

1. Comprender por qué la informática en la nube es diferente

Los proveedores de servicios en la nube (CSP) a gran escala ofrecen servicios comerciales en la nube a una escala enorme y de la misma forma a todos los clientes. Los clientes aprovechan servicios comerciales estandarizados bajo demanda. Pagan únicamente lo que utilizan.

El modelo de prestación de servicios comerciales estandarizados de la informática en la nube difiere radicalmente del modelo tradicional para compras de TI en las instalaciones (que tiene un alto nivel de personalización y podría no corresponder

a un artículo comercial). Comprender esta diferencia puede ayudarle a estructurar un modelo de adquisición más eficaz. Los servicios en la nube de IaaS eliminan la necesidad de que el cliente posea recursos físicos. Hay una tendencia continuada a alejarse de la idea de propiedad de los activos físicos y acercarse hacia servicios de infraestructura bajo demanda que imitan a los servicios públicos. Las entidades públicas deben entender la manera en que se presupuestan, adquieren y utilizan este tipo de servicios estandarizados, similares a los servicios públicos, y crear una estrategia para la adquisición de servicios en la nube a todas luces diferente de la de una infraestructura de TI tradicional, ya que ha de estar diseñada para aprovechar al máximo los beneficios que ofrece el modelo de suministro de la nube.

2. Planificación temprana para el máximo aprovechamiento de todo el beneficio de la nube

Un aspecto fundamental para el éxito de una estrategia de nube es la participación de las principales partes interesadas (adquisiciones, legal, presupuestos y finanzas, seguridad, TI y directiva empresarial) desde el principio. Esta participación garantiza que las partes interesadas puedan entender cómo afectará a las prácticas existentes la adopción de la nube. Brinda una oportunidad de restablecer las expectativas para la elaboración de presupuestos de TI, la administración de riesgos, los controles de seguridad y la conformidad. El fomento de una cultura de innovación y la formación del personal sobre los beneficios de la nube y sobre cómo utilizar la tecnología de nube ayuda a quienes tienen conocimientos institucionales a comprender este entorno. También ayuda a acelerar la aceptación durante la transición a la adopción de la nube.

3. Evite demasiados requisitos normativos

Las partes interesadas del sector público implicadas en la adquisición de la nube deberían plantear las preguntas adecuadas para solicitar las mejores soluciones. En un modelo de nube, no se adquieren los recursos físicos, por lo que los requisitos tradicionales de adquisición de centros de datos dejan de ser pertinentes. Si se siguen planteando las mismas preguntas que con los centros de datos, las soluciones que se podrían obtener estarán inevitablemente relacionadas con los centros de datos, por lo que los CSP no podrán ofertar o, lo que es peor, se generarán contratos mal diseñados que impedirán que los

clientes del sector público puedan aprovechar todas las funcionalidades y beneficios de la nube.

En una estrategia adecuada para la adquisición de servicios en la nube, los requisitos deben centrarse en el desempeño de las aplicaciones y dar prioridad a las cargas de trabajo y a los resultados en lugar de establecer qué hardware, infraestructura o métodos subyacentes deben emplearse para conseguir esos requisitos de desempeño. Los clientes pueden aprovechar las prácticas recomendadas establecidas por un CSP para las operaciones de centros de datos, ya que el CSP tiene el nivel de conocimientos y experiencia necesario para ofrecer servicios en la nube de IaaS seguros y a gran escala. No es necesario dictar especificaciones personalizadas para los equipos, operaciones y procedimientos (por ejemplo, bastidores, tipos de servidor y distancias entre centros de datos). Aprovechando las normas del sector de la nube comercial y las prácticas recomendadas (incluidas las certificaciones y acreditaciones reconocidas en el sector), los clientes evitan restricciones innecesarias sobre los servicios que pueden utilizar y garantizar el acceso a soluciones en la nube innovadoras y rentables.

4. Separe la infraestructura en la nube (servicios sin administrar) de los servicios administrados

Existe una diferencia entre la adquisición de infraestructura en la nube (IaaS) y la adquisición de mano de obra para utilizar la infraestructura en la nube o servicios administrados, tales como la nube de software como servicio (SaaS). Las adquisiciones de nube adecuadas separan la infraestructura de la nube de los servicios y mano de obra informática u otras compras de servicios administrados. Los servicios y la infraestructura en la nube, como la mano de obra para planificación, desarrollo, ejecución y mantenimiento de migraciones y cargas de trabajo en la nube, pueden ser suministrados por socios de CSP (u otros terceros) como solución global. Sin embargo, la infraestructura en la nube se debe considerar un "servicio" independiente con diferentes funciones y responsabilidades, acuerdos de nivel de servicios (SLA) y términos y condiciones específicos.

5. Incluir un modelo de precios de servicios

Para darse cuenta de los beneficios de la informática en la nube debe pensar más allá del enfoque comúnmente aceptado de una contratación a precio fijo.

Para suscribir un contrato de nube que tenga en cuenta una demanda fluctuante, necesita un contrato que le permita pagar por los servicios a medida que se consuman.

Los precios del CSP deben tener las características siguientes:

- Se ofrecen mediante un modelo de servicio de pago según el uso por el cual al final de cada mes los clientes pagan por lo que han consumido.
- Pueden fluctuar según los precios de mercado, de forma que los clientes puedan beneficiarse de la naturaleza dinámica y competitiva de los precios de la nube.

Permitir al proveedor de servicios en la nube ofrecer precios flexibles de pago por uso brinda a los clientes la oportunidad de evaluar cuál será el costo del uso, en lugar de tener que adivinar sus necesidades futuras y hacer una adquisición por encima de las necesidades. Los proveedores de servicios en la nube proporcionan precios actualizados y herramientas disponibles públicamente que permiten a los clientes evaluar sus precios, como la Calculadora de costo mensual AWS: <http://aws.amazon.com/calculator>. Además, los CSP deben ofrecer a los clientes las herramientas necesarias para generar informes de facturación detallada y personalizable que cumplan sus necesidades operativas y de conformidad.

Los proveedores de servicios en la nube también deben ofrecer características que permitan a los clientes analizar el uso de la nube y el gasto, de modo que los clientes puedan crear alertas que les avisen al acercarse a los umbrales de uso y gasto proyectado/presupuestado. Gracias a este tipo de alertas, las organizaciones pueden determinar si desean reducir el uso para evitar gastos excesivos o conseguir financiación adicional para hacer frente a los costos que sobrepasan el presupuesto previsto.

6. Aprovechar las acreditaciones de terceros relativas a la seguridad, la privacidad y la auditoría

Aprovechar las prácticas recomendadas del sector con respecto a la seguridad, la privacidad y la auditoría garantiza que estén en vigor los controles de seguridad física y lógica eficaces. Esto evita procesos de aprobación excesivamente costosos y duplicaciones de flujos de trabajo que a menudo no se justifican en virtud de los riesgos reales y las necesidades de conformidad.

En los pliegos de condiciones de la nube se pueden citar numerosos marcos de seguridad, prácticas recomendadas, normas de auditoría y controles estandarizados; por ejemplo, los siguientes:

- Federal Risk and Authorization Management Program (FedRAMP)
- Controles de organizaciones de servicios (SOC, Service Organization Controls) 1/Instituto estadounidense de contables públicos certificados (AICPA, American Institute of Certified Public Accountants): AT 801 (anteriormente, Statement on Standards for Attestation Engagements [SSAE] N.º 16)/International Standard on Assurance Engagements (ISAE) 3402 (anteriormente, Statement on Auditing Standards [SAS] N.º 70), SOC 2, SOC 3
- Estándar de seguridad de datos (Data Security Standard, DSS) del sector de tarjetas de pago (Payment Card Industry, PCI)
- Organización Internacional de Normalización (ISO, por sus siglas en inglés), ISO 27001, ISO 27017, ISO 27108, ISO 9001
- Departamento de Defensa (DoD, por sus siglas en inglés) de EE. UU. Guía de requisitos de seguridad (SRG)
- Ley sobre la administración de la seguridad de la información (FISMA, Federal Information Security Management Act)
- Reglamento estadounidense sobre el tráfico internacional de armas (ITAR, International Traffic in Arms Regulations)
- Ley de derechos educativos de la familia y privacidad (Family Educational Rights and Privacy Act, FERPA)
- Programa de evaluadores registrados de seguridad de la información (IRAP) (Australia)
- IT-Grundschutz (Alemania)
- Estándar de procesamiento de la información federal (FIPS, Federal Information Processing Standard) 140-2

7. Entender que la seguridad es una responsabilidad compartida

Dado que los clientes de informática en la nube crean sistemas sobre la infraestructura de nube, los proveedores de servicios y los consumidores de servicios en la nube comparten las responsabilidades en materia de seguridad y conformidad. En un modelo IaaS, los clientes controlan tanto el diseño y la protección de las aplicaciones y los datos que ponen en la infraestructura. Los proveedores de servicios en la nube son responsables de prestar servicios a través de una infraestructura controlada y segura, así como de proporcionar una amplia gama de características de seguridad adicionales. Las responsabilidades respectivas del CSP y del cliente dependen del modelo de implementación en la nube que se utiliza, ya sea IaaS, SaaS o Plataforma como servicio (PaaS). Los clientes deben entender claramente sus responsabilidades en materia de seguridad en cada modelo de nube.

8. Diseño e implementación del modelo de gobernanza de los datos en la nube

Las organizaciones deben mantener un control absoluto sobre los datos, así como su titularidad. Además, deben poder elegir las ubicaciones geográficas en las que desean almacenar los datos, donde el CSP debe haber aplicado controles de identidad y acceso que restrinjan el acceso a la infraestructura y los datos de los clientes. Los clientes deben entender claramente sus responsabilidades con respecto a la forma de almacenar, administrar, proteger y cifrar sus datos. Un beneficio importante de la informática en la nube en comparación con la infraestructura de TI tradicional es que los clientes tienen flexibilidad para evitar la dependencia de proveedores tradicionales. Los clientes en la nube no compran recursos físicos y los proveedores de servicios en la nube ofrecen la capacidad de aumentar y reducir la pila de TI según sea necesario, con mayor portabilidad e interoperabilidad que con el antiguo paradigma de TI. Las entidades del sector público deben requerir que los proveedores de servicios en la nube: 1) proporcionan acceso a herramientas y servicios de portabilidad en la nube que permitan a los clientes trasladar datos dentro y fuera de la infraestructura de la nube según sea necesario, y 2) no exigir compromisos mínimos ni contratos a largo plazo.

9. Especificar términos de un artículo comercial

La informática en la nube se debe adquirir como artículo comercial y las organizaciones deben tener en cuenta qué términos y condiciones son adecuados (y no adecuados) en este contexto. Un artículo comercial se reconoce como un artículo de tal tipo que se haya vendido, alquilado, concedido bajo licencia o puesto a la venta de otra manera al público en general y, por lo general, funciona del mismo modo para todos los usuarios/clientes, tanto comerciales como de la administración. Los términos y condiciones de los CSP sobre IaaS están diseñados para reflejar el funcionamiento de un modelo de servicios en la nube (es decir, no se compran recursos físicos y los proveedores de servicios en la nube operan a escala masiva para ofrecer servicios comerciales estandarizados). Es fundamental que los términos y condiciones de un CSP se incorporen y utilicen todo lo posible.

10. Definir los criterios de evaluación de la nube

Los criterios de evaluación en la nube deben centrarse en los requisitos de desempeño del sistema. Seleccione el CSP adecuado entre un grupo de recursos establecido para aprovechar la elasticidad, las eficiencias de costos y la rápida escalabilidad que ofrece la nube. Este enfoque garantiza que obtenga los mejores servicios en la nube para satisfacer sus necesidades, el máximo valor en estos servicios y la capacidad de aprovechar la innovación impulsada por el mercado. Las definiciones de los beneficios de la nube del Instituto Nacional de Normalización y Tecnología (NIST) son un excelente punto de partida para determinar los criterios de evaluación de la nube:

<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf>.

Conclusión

Miles de clientes del sector público utilizan AWS para lanzar rápidamente servicios a través de un proceso de adquisición eficiente centrado en la nube. Tener en cuenta estos diez pasos ayudará a las organizaciones a proporcionar unos resultados aún más centrados en los ciudadanos, en los estudiantes y en la misión.