Aquisição de soluções em nuvem: melhores práticas para clientes do setor público

Março de 2015

Sumário

Objetivo:

A aquisição de serviços em nuvem é diferente da maioria das aquisições de tecnologia tradicionais. Entidades do setor público estão habituadas a comprar infraestruturas de TI usando as regras de aquisição concebidas para compras tradicionais, como hardware ou software de datacenter. No entanto, essas abordagens de compras tradicionais incluem práticas de compra e cláusulas contratuais que podem dificultar a adoção da escalabilidade, dos custos mais baixos e do caráter inovador da tecnologia de nuvem.

A aquisição de serviços de nuvem apresenta uma oportunidade de reavaliar as estratégias de aquisição já existentes a fim de criar um processo rápido e flexível de aquisição que possibilite que as organizações aproveitem toda a escala e a flexibilidade da nuvem. Este whitepaper disponibiliza orientações para líderes dos setores de negócios, de tecnologia e de aquisição do setor público na construção de uma estratégia de aquisição de nuvem bem-sucedida para a aquisição de serviços relacionados à Infraestrutura como serviço (IaaS) e à Plataforma como serviço (PaaS)[1]. As melhores práticas desse documento se baseiam em muitos anos de experiência da Amazon Web Services, Inc. (AWS) no fornecimento de infraestrutura global de grande escala de forma confiável e segura.

Por que a computação em nuvem é diferente?

A diferença fundamental entre a computação em nuvem e a TI tradicional é que, em um modelo de nuvem, os clientes não compram ativos físicos.
A computação, o armazenamento e outros serviços de infraestrutura poderosos são executados em datacenters de provedores de serviços em nuvem (CSP), com clientes que pagam para utilizar esses serviços de forma semelhante a um modelo do tipo de serviços de utilidade pública, pagando apenas pelos recursos utilizados.
A natureza do tipo de serviços de utilidade pública desse modelo se estende a outras características da computação em nuvem, como o fato de que a computação em nuvem funciona da mesma forma para todos os clientes. Esse fato é essencial, pois permite que os CSPs operem em uma escala realmente grande e, como resultado, proporcionem economias significativas. Os clientes podem usar os serviços em nuvem como elementos fundamentais, personalizando para si próprios uma infraestrutura para basear seus aplicativos. Além disso, como outros prestadores de serviços de utilidade pública, os CSPs não determinam como os clientes devem usar seus serviços, e não veem ou acessam os conteúdos do cliente.

O que é a computação em nuvem?

O Instituto Nacional de Padrões e Tecnologia (NIST) dos Estados Unidos define a computação em nuvem como um modelo para permitir um acesso à rede conveniente, onipresente e sob demanda a um pool compartilhado de recursos de computação configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente fornecidos e liberados com uma interação com o provedor de serviços ou esforço de gerenciamento mínimo.
http://www.nist.gov/itl/cloud/

Pode ser interessante comparar o modelo de serviço em nuvem com o de uma empresa de energia elétrica. Uma empresa de energia elétrica fornece eletricidade para todos os clientes da mesma maneira, cobrando de acordo com o uso e permitindo

[1] Consulte a página 33 para ver as definições do NIST de tipos de serviços em nuvem. A AWS hospeda soluções SaaS. No entanto, as aquisições de SaaS são realizadas entre o provedor de SaaS e o comprador e têm seus próprios termos e condições únicos.

que os clientes usem essa eletricidade para suas necessidades particulares. A empresa de energia elétrica não pergunta nem sabe se os clientes estão utilizando uma máquina de lavar louça ou uma televisão e não adapta o fornecimento de eletricidade a clientes individuais. O pagamento é feito de acordo com a eletricidade consumida em um dado ciclo de faturamento. Da mesma forma, os CSPs permitem que os clientes paguem somente pelo que utilizam e oferecem os mesmos serviços para todos os clientes.

O entendimento de que a computação em nuvem oferece um modelo de entrega diferente ajuda a estabelecer as expectativas sobre as responsabilidades do CSP e dos clientes. Como os clientes não possuem ativos físicos, é natural que eles não abordem as aquisições de nuvem como se fossem uma compra de um ativo físico. Entidades do setor público devem ponderar sobre como os serviços de utilidade pública são adquiridos, orçados e utilizados, e construir uma estratégia de aquisição de nuvem que seja feita para ser diferente da estratégia de TI tradicional, projetada para aproveitar os benefícios do modelo de fornecimento em nuvem.

Modelos de nuvem "X" como serviço (XaaS)

Os ambientes de computação em nuvem tendem a ser uma combinação de serviços relacionados de IaaS, PaaS e Software como serviço (SaaS). Esses modelos de nuvem diferentes são utilizados em conjunto de uma maneira que é semelhante a um ambiente de TI tradicional, com plataformas e serviços de infraestrutura de suporte subjacente. Cada modelo de nuvem requer uma abordagem diferente para aquisição, gestão, definição de preços, termos e condições e segurança. Como representado na **Figura 1**, os diversos modelos de implementação e utilização da nuvem têm diferentes níveis de CSP e de responsabilidades do cliente.

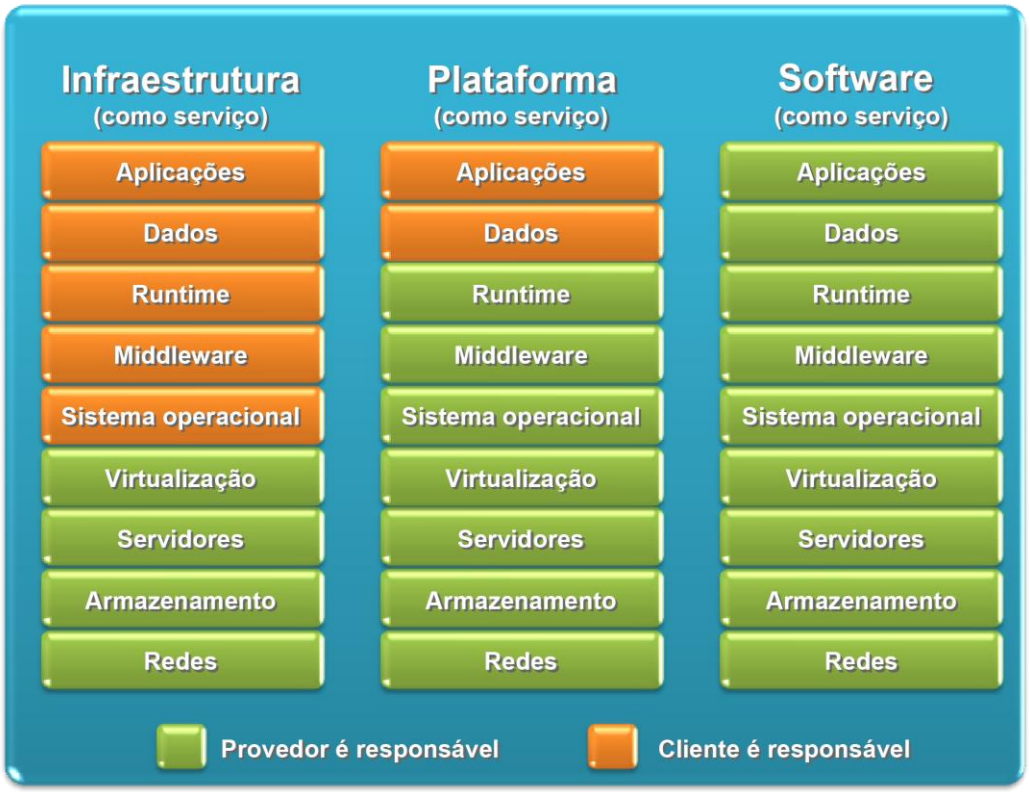

Figura 1 - Funções e responsabilidades de XaaS

Qualquer tentativa de utilizar um único conjunto de termos e requisitos comuns que abranja os três modelos de XaaS em um modelo de aquisição único provavelmente será problemática. Para estratégias de aquisição de IaaS e PaaS, recomendamos que as organizações do setor público tenham em mente as seguintes considerações-chave:

- **Requisitos baseados em desempenho –** escolha uma abordagem ou veículo de contrato que permita focar nas necessidades e soluções voltadas para o desempenho, e não nos requisitos de aquisição tradicionais "prescritivos" que dificultam o aproveitamento de todos os benefícios e valores da nuvem.
- **Definição de preços –** adote uma definição de preços de nuvem sob demanda, do tipo de serviços de utilidade pública, que seja impulsionada pela concorrência comercial.
- **Segurança e garantia/auditoria –** entenda que as responsabilidades de segurança e conformidade são compartilhadas entre os clientes da nuvem e o CSP. Aproveite as melhores práticas do setor sobre segurança e auditoria, que oferecem a garantia de que os CSPs têm controles de segurança físicos e lógicos eficazes em ordem.
- **Termos e condições –** perceba que os serviços em nuvem são comprados como um item comercial e verifique quais termos e condições são apropriados (ou não) para a compra de um item comercial, como os serviços em nuvem. Os termos e condições do CSP são projetados para refletir como funciona um modelo de serviço de nuvem. Assim, é fundamental que os termos e condições únicos de um CSP sejam incorporados e utilizados o mais amplamente possível.
- **Considerações adicionais –** separe a compra de infraestrutura de nuvem da compra de serviços gerenciados e mão de obra para planejamento, desenvolvimento, execução e manutenção de migrações e cargas de trabalho da nuvem. A infraestrutura de nuvem e os serviços gerenciados podem ser fornecidos como uma solução abrangente; no entanto, eles devem ser considerados como serviços separados com termos e condições e SLAs distintos.

Essas considerações-chave de aquisição são discutidas nas seções a seguir. A tabela de melhores práticas da página 14 disponibiliza orientações sobre as melhores práticas de aquisição de nuvem, juntamente com exemplos de linguagem de solicitação focada na nuvem retirados diretamente de solicitações do setor público.

Requisitos baseados no desempenho

As estratégias de aquisição de nuvem bem-sucedidas focam em requisitos de nível de aplicativo e baseados no desempenho, ao invés de ditar métodos específicos, infraestrutura ou hardware utilizados para atingir os requisitos de desempenho. Em um modelo de nuvem, um CSP possui e mantém o hardware conectado à rede necessário para os serviços de nuvem. Com este fardo de infraestrutura a menos para os clientes, é necessário incluir prescrições normativas que especifiquem o que a pilha de infraestrutura subjacente deve ser.

Os clientes podem aproveitar as melhores práticas industriais e comerciais estabelecidas de um CSP para operações de datacenter, ao invés de ditar o uso de procedimentos ou equipamentos específicos (por exemplo, racks, tipos de servidores, etc). Ao aproveitarem os padrões comerciais

do setor da nuvem, os clientes evitam a imposição de restrições desnecessárias sobre os serviços que podem utilizar e aproveitam o acesso às soluções mais inovadoras e de baixo custo de infraestrutura de nuvem.

Veículos de contrato

Quando as organizações do setor público decidem o modelo de nuvem de que precisam (consulte os modelos de nuvem XaaS na página 4), elas devem determinar se é melhor obter serviços de nuvem diretamente com um CSP ou usar um modelo indireto em que os serviços de nuvem sejam adquiridos através de um parceiro CSP ou revendedor de nuvem. As considerações a seguir sobre termos e condições devem ser levadas em consideração:

- **Compra direta de um CSP** – use termos projetados para um serviço disponível comercialmente. Comprado como um serviço de item comercial que é oferecido sem horas de trabalho.
- **Compra indireta de um CSP parceiro** – comprado de um parceiro/revendedor CSP, negociando um acordo com essa organização.

Muitos CSPs oferecem um acordo clickthrough on-line que disponibiliza uma maneira rápida e fácil de começar a usar os serviços em nuvem. Alguns clientes do setor público preferem ter uma relação direta com um CSP e simplesmente usam um acordo clickthrough de CSP para começar a usar a infraestrutura de nuvem como um serviço do tipo de serviço utilidade pública. Ao considerar esse modelo de aquisição direta, os clientes devem analisar a tabela de melhores práticas na página 14.

Também é importante perceber a diferença entre a compra de infraestrutura de nuvem e serviços gerenciados. As organizações do setor público devem considerar o tamanho da função que pretendem assumir no fornecimento de serviços de nuvem e o quanto eles pretendem terceirizar a um provedor de serviços gerenciados.

- **Serviços em nuvem "não gerenciados" –** serviços de infraestrutura e plataforma de nuvem comprados como um serviço de item comercial de um CSP.
- **Serviços "gerenciados" –** empresas que ajudam os clientes a projetar, desenhar, migrar e gerenciar suas cargas de trabalho e aplicações na nuvem.

Novamente, é útil pensar na computação em nuvem como sendo como um serviço de utilidade pública, como um provedor de energia elétrica. Uma empresa de energia elétrica não fornece mão de obra para auxiliar os clientes com o uso de sua compra. Em vez disso, a empresa fornece os serviços fundamentais com os quais os clientes (muitas vezes assistidos por empresas de consultoria) criam suas soluções personalizadas.

Ter o veículo de contrato certo e implementado é a chave para tirar partido de uma entrega rápida sob demanda da nuvem. **A tabela 1** descreve quatro opções de veículo de contrato.

Tabela 1 – Opções de veículo de contrato

1. Criação de um catálogo de nuvem (Compra direta ou indireta) Catálogos de nuvem podem assumir diferentes formas e podem ser conhecidos também como agendas, estruturas, contratos com prazo definido, contratos de aquisição em âmbito governamental (GWACs), planos de tecnologia e comunicação de informação (TCI) ou veículos de entrega/ quantidade indefinida (ID/IQ). O estabelecimento de um veículo de catálogo de nuvem para uso por múltiplos compradores pode simplificar o processo de aquisição, ao mesmo tempo em que otimiza as economias de escala. O veículo de contrato, uma vez estabelecido, permite à empresa adquirir os serviços de nuvem específicos necessários, quando e como precisar, a partir de um catálogo pré-aprovado, em vez de realizar aquisições distintas. Essa abordagem reduz os requisitos administrativos e diminui significativamente o tempo de ciclo e a complexidade da aquisição.	**2. Aproveitamento de um contrato de fornecedor existente (compra indireta)** Muitos clientes acreditam que o aproveitamento de um contrato de fornecedor existente é ideal para um veículo de aquisição de nuvem. Há muitas opções para clientes do setor público adquirirem serviços em nuvem usando um contrato existente. Por exemplo, uma opção para os clientes do Governo Federal dos EUA é trabalhar com parceiros da AWS para aproveitar o Schedule 70 da Administração de Serviços Gerais (GSA) do governo dos EUA (http://www.gsa.gov/portal/content/104506) e acessar os serviços em nuvem como um Outro Custo Direto (OCD). Um exemplo de uma opção de cliente do governo estadual e local dos EUA é trabalhar com parceiros da AWS para aproveitar os contratos existentes, tais como um contrato de cooperação de organização de compras cooperativas Western States Contracting Alliance – National Association of State Procurement Officials (WSCA-NASPO) para serviços públicos de hospedagem de nuvem (http://www.aboutwsca.org/contract.cfm/contract/w37). Os veículos de contrato de parceiros da AWS que permitem compras da AWS estão listados no centro de contrato do setor de parceiros da AWS: http://aws.amazon.com/contract-center/
3. Compra de um revendedor CSP (compra indireta) Os parceiros CSP normalmente têm relacionamentos com clientes ou veículos de contrato existentes. Por exemplo, o programa global de revendedores de canal da AWS (http://aws.amazon.com/partners/channel-reseller/) permite que parceiros qualificados revendam serviços da AWS para clientes finais dos setores público e comercial. O programa foi projetado para parceiros de consultoria da AWS Partner Network (APN) (http://aws.amazon.com/partners/consulting/) que tenham criado suas práticas do AWS para incluir serviços profissionais e gerenciamento de implementações da AWS, como: System Integrators (SIs – Integradores de sistema), Managed Service Providers (MSPs – Prestadores de serviços gerenciados), agências digitais e Value-Added Resellers (VARs – Revendedores de valor agregado).	**4. Emissão de uma aquisição de solução (compra indireta)** Neste modelo, os órgãos do setor público emitem uma solicitação a um SI ou empresa de serviços/ consultoria gerenciada e solicitam que eles proponham uma solução abrangente (por exemplo, software, serviços de implementação *e* infraestrutura da nuvem). É comum que os clientes tenham requisitos para uma aquisição de TI em que a nuvem é apenas um dos muitos componentes. Reconhecendo que a nuvem é fornecida como item comercial, a autoridade da aquisição solicitará aos licitantes de SI/empresas de consultoria que documentem suas arquiteturas de solução propostas, expliquem como pretendem utilizar a infraestrutura da nuvem e qual será o projeto para atender aos requisitos e SLAs. Essa abordagem encoraja os licitantes de aquisição de solução a utilizarem os serviços da nuvem da forma mais econômica e apropriada.

Definição de preços

Para se contratar um serviço em nuvem de modo que seja considerada a demanda flutuante, os clientes precisam de um contrato que os permita pagar pelos serviços conforme são consumidos. **A tabela 2** contém quatro elementos de definição de preços para serem levados em consideração quando organizações do setor público criam requisitos de solicitação de nuvem.

Tabela 2 – Considerações sobre definição de preços de nuvem

1. Transparência	**2. Preços de variáveis**
A definição de preços do CSP deve estar publicamente disponível e transparente. A definição de preços neste formato demonstra a verdadeira natureza comercial da nuvem. As informações sobre a definição de preços do AWS estão publicamente disponíveis em: http://aws.amazon.com/pricing/.	Um modelo de aquisição de nuvem deve ser flexível para permitir que os preços da nuvem flutuem com base nas definições de preços do mercado. Essa abordagem aproveita a natureza dinâmica e competitiva da definição de preços da nuvem, além de apoiar inovações e reduções de preços (na data da publicação, a AWS havia baixado preços 48 vezes: http://aws.amazon.com/pricing/).
3. Vários modelos para definição de preços Permitir que o CSP ofereça diferentes modelos de definição de preços possibilita às organizações avaliar cada modelo de definição de preços do CSP em relação aos seus requisitos de TI exclusivos, ao invés de uma comparação específica de definição de preços de unidades de computação e de armazenamento arbitrárias. As solicitações de catálogo da nuvem devem permitir que os CSPs ofereçam seus próprios modelos de definição de preços, permitindo que os clientes selecionem um modelo que melhor atenda às suas necessidades específicas. Além disso, as solicitações de aquisição de soluções devem desafiar licitantes de SI/empresas de consultoria a utilizarem o modelo de definição de preços de um CSP de uma forma otimizada, uma vez que apresentam uma definição de preços em sua resposta de solicitação.	**4. Modelo de serviços de utilidade pública em que se paga pelo que se usa** A incorporação de um modelo de pagamento conforme o uso dos serviços de utilidade pública, em que, no final de cada mês, o valor pago corresponde ao que foi usado, é ideal para a utilização de recursos e métricas e permite que os clientes olhem para serviços de TI como uma despesa operacional (OpEx), em oposição a um modelo tradicional de despesas de capital (CapEx). Pensar no valor em longo prazo dos ativos é fundamental para organizações do setor público e, em datacenters típicos do setor público, as grandes despesas de capital iniciais dependem de melhorias contínuas na tecnologia (ou seja, os mais novos servidores, roteadores ou load balancers) geralmente caras, resultando, em última análise, em insatisfação do usuário final e uma desaceleração da inovação e da adoção de TI. Ao longo do tempo, os custos permanecem fixos, mas o mesmo ocorre com os recursos. As economias de escala disponíveis com a nuvem permitem que CSPs como a AWS comprem e atualizem grandes volumes de infraestrutura constantemente a custos muito baixos. Consequentemente, os clientes colhem os benefícios da redução dos custos da nuvem, do desempenho crescente com uma infraestrutura melhorada e da funcionalidade aprimorada com ampla inovação de sistema.

Orçamento para nuvem

Um dos grandes benefícios da computação em nuvem é a possibilidade de financiar a TI como uma despesa operacional. A principal vantagem reside no fato de ser possível pagar apenas pelos recursos de computação consumidos, sem ter que investir demasiadamente em datacenters e servidores, o que inevitavelmente leva a capacidade limitada ou recursos ociosos.

A aquisição de TI tradicional é construída em torno do modelo CapEx de compras e possui um ativo físico, no qual se paga adiantado por um ativo que deprecia com o tempo. No entanto, fazer o orçamento para um ambiente de TI como OpEx pode ser uma transição relativamente sem dificuldades para os clientes do setor público quando se leva em consideração que essa não é uma abordagem inflexível do tipo "tudo ou nada". Tende a haver um meio termo entre CapEx e OpEx, e as aquisições bem-sucedidas de nuvem procuram soluções orçamentais de curto prazo, ao mesmo tempo em que planejam uma mudança, em longo prazo, para um modelo do tipo de serviços de utilidade pública.

No curto prazo, os clientes podem explorar a possibilidade de fazer layers de despesas operacionais em um orçamento CapEx durante a sua transição para a nuvem, dado que, com a computação em nuvem, a despesa de capital tradicional não é mais necessária, gerando disponibilidade de fundos de capital. Em um modelo de nuvem, pode haver reduções significativas em custos CapEx *e* OpEx existentes. Além de não ter nenhum investimento inicial, os clientes devem considerar que os custos com OpEx envolvidos na gestão e manutenção de datacenter que hospedam servidores (energia, segurança, redes, HVAC, etc.) não são mais necessários, já que o CSP gerencia toda a infraestrutura de TI. Isso também libera orçamento para investir, de forma rápida, em iniciativas inovadoras que não podem ser feitas facilmente quando se gerenciam CapEx.

Os pontos-chave a serem considerados quando se faz um orçamento para um modelo de nuvem incluem:

- Separe a aquisição de infraestrutura de nuvem a partir de serviços gerenciados. Considere contratos de curto prazo para serviços gerenciados e calcule os custos previstos de futuros projetos de TI como opções de CapEx e OpEx, pois isso ajudará a determinar qual orçamento é apropriado para o escopo de projetos de serviços gerenciados.
- Utilize ferramentas do CSP que automatizam o provisionamento. Isso permite a utilização otimizada dos recursos, reduzindo os recursos quando eles não estão sendo usados.
- Construa mecanismos de governança para monitorar e prever custos e cargas de trabalho de nuvem e reduzir o risco. Utilize ferramentas do CSP que automatizem o provisionamento, o acesso de controle e forneçam recursos de monitoramento/apresentação de relatórios da nuvem.
- Utilize uma definição de preços associada do CSP para orçar a utilização estimada e reduzir despesas.

Como um exemplo do Governo Federal dos Estados Unidos promovendo uma abordagem flexível para fazer o orçamento, no orçamento do presidente para o ano fiscal de 2015 foi afirmado que: "O orçamento inclui investimentos para transformar o portfólio de TI do governo por meio da computação em nuvem, dando às agências a capacidade de comprar serviços de TI em um modelo baseado em serviços de utilidade pública, em que se paga apenas pelos serviços consumidos".

Estrutura de item de linha única

O uso de uma estrutura de item de linha única para serviços em nuvem é uma abordagem simples e baseada em serviços de utilidade pública para aproveitar o modelo da nuvem de pagamento por utilização. Pense na aquisição de serviços em nuvem como a compra de uma conta de CSP, que consiste em um menu completo de serviços em nuvem de CSP. Os usuários podem simplesmente selecionar os serviços de que necessitam neste menu de itens de linha do CSP.

Uma abordagem de item de linha única fornece a flexibilidade de oferecer novas ofertas e serviços de CSP para os usuários em tempo real e disponibiliza aos usuários o acesso rápido aos recursos de que necessitam. Uma estrutura de item de linha única também acomoda a demanda flutuante, assegurando plena utilização e custos baixos. Abaixo está um exemplo de uma abordagem de estrutura de item de linha única:

Nº ITEM	FORNECIMENTOS/SERVIÇOS	QUANTIDADE	UNIDADE	PREÇO UNITÁRIO	VALOR
1001	Serviços em nuvem do CSP	1,000	Cada	$1	$1,000

Itens de linha adicionais podem ser adicionados a serviços como suporte do CSP, treinamento do CSP, serviços profissionais ou gerenciados e software de terceiros, como os produtos disponíveis no AWS Marketplace (https://aws.amazon.com/marketplace).

Na estrutura de item de linha acima, cada unidade equivale a US$ 1,00 dos Serviços em nuvem do CSP. Para demonstrar a entrega e utilização de cada unidade nesta amostra de estrutura, o CSP deverá permitir que os clientes gerem relatórios detalhados de faturamento que mostrem os custos por hora, dia ou mês, por cada conta em uma organização, por produto ou recurso do produto ou por tags definidas pelo cliente.

Por exemplo, os clientes da AWS podem ver as informações de faturamento tanto nos níveis granulares quanto nos de resumo. Usando o Explorador de custos da AWS para visualizar padrões de gastos com recursos AWS ao longo do tempo, os clientes podem filtrar a visão de utilização/faturamento por serviços, por conta vinculada ou por tags personalizadas aplicadas a recursos. Além disso, o recurso de Faturamento consolidado da AWS permite aos clientes consolidarem o pagamento de várias contas da AWS dentro de uma organização, designando uma delas para ser a conta do pagante. Os clientes podem visualizar uma apresentação combinada das cobranças feitas pela AWS ocorridas em todas as contas, assim como obter um relatório de custos detalhado para cada uma das contas da AWS individuais associadas à conta do pagante.

Segurança e garantia

Conforme os clientes de computação em nuvem vão construindo sistemas em cima da infraestrutura de nuvem, as responsabilidades de conformidade e segurança são compartilhadas entre o CSP e os clientes da nuvem. Em um modelo de IaaS, os clientes controlam como vão arquitetar e proteger seus aplicativos e dados colocados na infraestrutura, enquanto os CSP são responsáveis por fornecer serviços em uma plataforma controlada e altamente segura, fornecendo um amplo conjunto de recursos de segurança. O nível de responsabilidades do CSP e dos clientes neste modelo de responsabilidade compartilhada depende do modelo de implementação de nuvem (consulte os modelos de nuvem XaaS discutidos na página 4), e os clientes devem ser claros quanto a quais responsabilidades estão no escopo das obrigações deles em cada modelo. O modelo de responsabilidade compartilhada IaaS da AWS é retratado na **figura 2**.

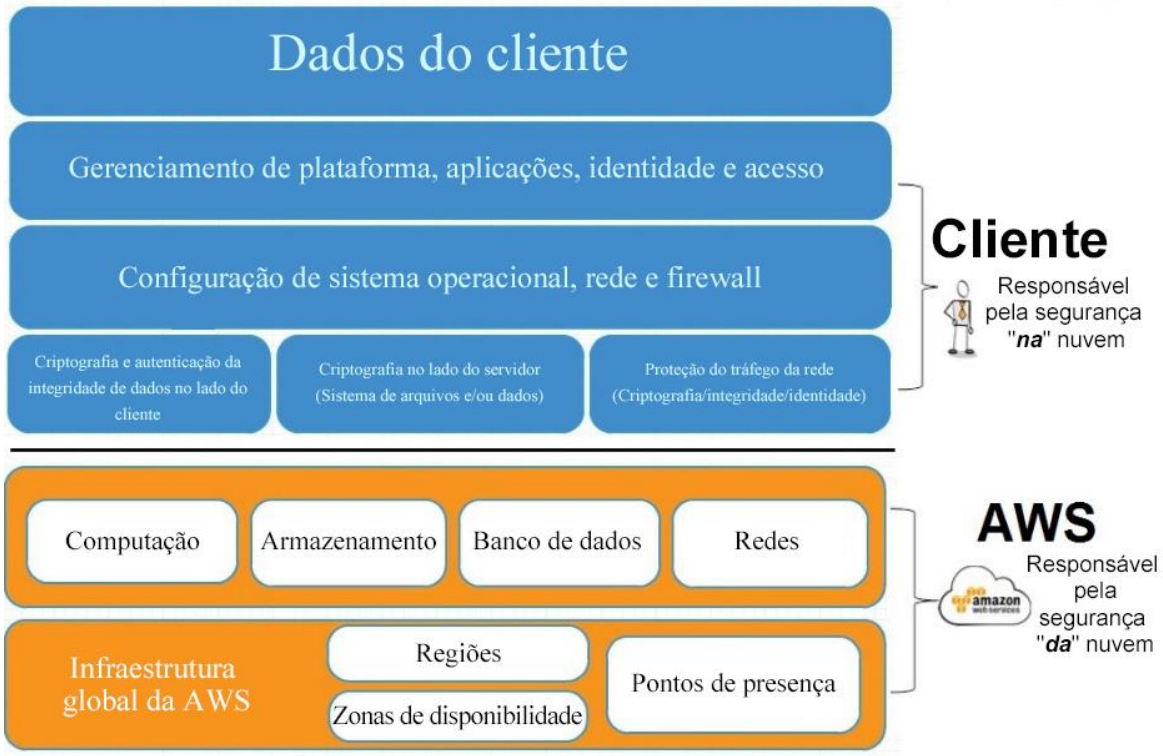

Figura 2 – Modelo de responsabilidade compartilhada da AWS

- **Responsabilidade da AWS –** a AWS opera, gerencia e controla os componentes de infraestrutura, desde o sistema operacional de hospedagem e a layer de virtualização até a segurança física das instalações em que os serviços operam.
- **Responsabilidade do cliente/parceiro –** o cliente/parceiro assume a responsabilidade e o gerenciamento do sistema operacional convidado (incluindo atualizações e patches de segurança), de outro software de aplicação associado e da configuração dos firewalls do grupo de segurança e outros recursos de segurança, gerenciamento de mudanças e registros fornecidos pela AWS.

Padrões de segurança/auditoria e credenciamento de terceiros

Certificações e avaliações de terceiros fornecem garantias de que controles efetivos de segurança físicos e lógicos estão em vigor. Quando as organizações do setor público utilizam esses relatórios, elas evitam sujeitar-se a processos excessivamente onerosos ou fluxos de trabalho de aprovação que podem não ser justificados pelas necessidades reais de conformidade e risco. Existem diversas estruturas de segurança, melhores práticas, padrões de auditoria e controles padronizados que as solicitações de nuvem podem citar, como: o Programa federal de gerenciamento de risco e autorização (FedRAMP), os Controles de empresas de serviços (Service Organization Controls, SOC) 1/Declaração sobre normas para comprovação de contratos (Statement on Standards for Attestation Engagements, SSAE) 16/ Normas internacionais para contratos de garantia (ISAE) 3402 (anteriormente conhecida como Declaração sobre normas de auditoria [SAS] nº 70), SOC 2, SOC 3, Padrão de segurança de dados (DSS) da Indústria de cartões de pagamento (PCI), Organização internacional para padronização (International Organization for Standard - ISO) 27001, ISO 9001, Estrutura de gerenciamento de riscos do Departamento de defesa (RMF do DoD, Modelo de segurança de nuvem), Lei federal de gestão de segurança da informação (FISMA), Regulamentos do tráfego internacional de armas (ITAR) e Norma de processamento de informações federais (FIPS) 140-2.[2]

Ao criarem uma estratégia de aquisição de nuvem, as organizações do setor público devem aproveitar essas melhores práticas do setor sobre segurança e auditoria em vez de incluir seus próprios protocolos de segurança exclusivos. Se os CSPs precisassem disponibilizar personalizações de segurança individuais, isso diminuiria a capacidade deles de redimensionar e transmitir os benefícios de inovação e economia para os clientes. A AWS e outros CSPs oferecem seus serviços da mesma maneira para todos os usuários, e seria quase impossível ter que levar em consideração as políticas de segurança, conformidade e auditoria únicas de cada cliente, se adequar a elas, incorporá-las a um modelo de negócios do CSP e ainda ser capaz de oferecer serviços de nuvem com o mesmo nível de agilidade, tamanho e preço.

Privacidade de dados

Os clientes do setor público devem reter o controle total e a propriedade de seus dados e ter a capacidade de escolher as localizações geográficas nas quais seus dados serão armazenados, com os controles de acesso e identidade do CSP disponíveis para restringir o acesso à infraestrutura e aos dados do cliente. Os CSPs devem disponibilizar aos clientes a escolha de como armazenar, gerenciar e proteger seus dados e não exigir um contrato de longo prazo ou de exclusividade.

Os CSPs também devem fornecer a documentação detalhando como clientes do setor público podem usar serviços de nuvem para atender aos requisitos específicos de privacidade/proteção de dados e conformidade. Por exemplo, a AWS fornece whitepapers e arquiteturas de referência para atender às exigências regulamentares e de conformidade específicas, como a Health Insurance Portability e Accountability Act (Lei da Portabilidade e Prestação de Contas em Seguro Saúde, HIPAA) dos EUA, os requisitos de proteção de dados da UE, e as considerações sobre privacidade de dados da Austrália, Nova Zelândia e Cingapura, para citar algumas. Todos os whitepapers de privacidade de dados da AWS podem ser encontrados no site da AWS: http://aws.amazon.com/compliance/.

[2] Consulte a página 33 para obter informações sobre a postura de conformidade e segurança da AWS.

Termos e condições

A computação em nuvem deve ser adquirida como um item comercial. De forma geral, itens comerciais são reconhecidos como itens de um tipo que foram vendidos, locados, licenciados ou oferecidos de outra forma ao público em geral. As aquisições de nuvem bem-sucedidas reconhecem que os CSP não estão fornecendo resultados construídos de forma personalizada e que os benefícios da nuvem se originam do funcionamento em grande escala.

A relevância é a consideração primordial quando se decide sobre os termos e condições a serem incluídos em uma solicitação de nuvem. Quando é feita a aquisição de serviços de nuvem, os termos ou requisitos que se sobrepõem ou são duplicações de padrões abrangentes do setor existentes (por exemplo, credenciamento de FedRAMP focado na nuvem do Governo Federal dos EUA) devem ser removidos; caso contrário, eles podem agir como obstáculos desnecessários ao processo de aquisição e, mais importante, reduzirão o benefício e o valor de fazer a mudança para a nuvem.

As políticas e os procedimentos existentes podem ser usados como orientações, e não como estruturas rígidas que impeçam as organizações de aproveitarem os benefícios de escala que a computação em nuvem oferece. As solicitações de nuvem devem reconhecer as diferenças entre adquirir serviços em nuvem e adquirir a infraestrutura de TI tradicional e remover requisitos que não são mais adequados para um modelo de serviços comercial em nuvem.

Novos serviços e recursos

Os termos e condições únicos de um CSP são essenciais para perceber os benefícios da computação em nuvem. Os clientes de serviços em nuvem devem permitir o desenvolvimento dos termos e condições a fim de se beneficiarem dos novos serviços e das melhorias do serviço dinâmico. Os termos de serviço estáticos que são encontrados em aquisições de TI tradicionais (ou seja, termos de uso para uma determinada peça de hardware adquirida) permanecem constantes porque o hardware não pertence mais ao fornecedor. Com a computação em nuvem, a infraestrutura evolui com os serviços de nuvem à medida que eles são desenvolvidos.

A grande escala de serviços de nuvem do tipo de serviços de utilidade pública impulsiona a inovação e eficiência de custos. Novamente, considere um serviço de utilidade pública operando em uma grande escala semelhante à AWS, como um grande fornecedor de telecomunicações. Com um serviço de item comercial como este, não é viável pedir o consentimento de cada um dos clientes para atualizar ou melhorar os serviços. As despesas administrativas resultantes acabariam por aumentar o preço do serviço, além de atrasar desnecessariamente o lançamento de melhorias e novos serviços inovadores. No caso da AWS, iteramos produtos continuamente para garantir o mais alto nível de funcionalidade, proteção e durabilidade e, até o momento desta publicação, havíamos lançado mais de 1.260 novos serviços e recursos desde a criação em 2006.

Um benefício adicional de computação em nuvem sobre a infraestrutura de TI tradicional é que os clientes têm a flexibilidade para evitar ficarem presos a um fornecedor, o que ocorre no modo tradicional. As entidades do setor público devem aproveitar a ausência de necessidade de fidelidade a um fornecedor propiciada pela nuvem, ao não exigirem que os CSPs e os parceiros do CSP assinem contratos de longo prazo ou concedam exclusividade contratual.

Considerações adicionais

As organizações devem educar a equipe existente sobre os benefícios e as oportunidades da utilização de serviços de nuvem, a fim de diminuir quaisquer preocupações com relação ao emprego, explicando como a adoção da nuvem influenciará as práticas existentes e como a equipe vai ganhar um novo conjunto de habilidades de ponta. Além disso, os CSPs devem oferecer uma ampla gama de opções de treinamento para permitir que os clientes adquiram as habilidades, os conhecimentos e a experiência para projetarem, implementarem e gerenciarem aplicativos em sua plataforma de nuvem escolhida.

Não é aconselhado adicionar requisitos para as solicitações de nuvem que possam vir a ser encargos administrativos desnecessários tanto para o cliente quanto para o CSP. Os CSPs disponibilizam serviços de itens comerciais que dependem de escala e, portanto, não podem assumir pedidos personalizados, como participar de reuniões regulares de clientes, fornecer avisos personalizados, relatórios personalizados sobre o uso, faturas personalizadas ou consulta fora dos serviços normais. A fim de oferecer um serviço sem interação pessoal e de baixa administração em grande escala, ao mesmo tempo em que os custos baixos são mantidos, o CSP mantém os custos de administração baixos sempre que possível. Os parceiros do CSP muitas vezes desempenham um papel de serviços de gestão tradicional e fornecem a mão de obra necessária para implementar e gerenciar aplicativos em nuvem e cargas de trabalho.

Tabela de melhores práticas:

A tabela de melhores práticas a seguir acrescenta informações sobre considerações de aquisição de nuvem discutidas acima, e fornece orientações sobre as melhores práticas de solicitação de nuvem. A tabela também contém exemplos reais de linguagem de solicitação de nuvem tirados diretamente de solicitações de nuvem do setor público.

Tabela 3 – Aquisição de soluções em nuvem: Melhores práticas

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
Requisitos baseados no desempenho: Melhores práticas			
1. Requisitos de hardware/equipamento ou software específicos **Problema potencial** Exigência que os CSPs mantenham sistema operacional/ software, medidas antivírus e hardwares específicos ou atualizem equipamentos específicos.	**Os CSPs devem** – fornecer um ambiente virtual personalizável que é independente do programa e sistema operacional. Além disso, os CSPs devem detalhar seu provisionamento de hardware, manutenção, atualização e processo de descomissionamento. **Clientes do setor público devem evitar** – especificar o hardware e o software subjacentes usados por um CSP para operar seu serviço. Os clientes devem tratar especificações de equipamentos como referência ou fatores de avaliação, não como requisitos rígidos.	A computação em nuvem deve aliviar a carga de infraestrutura dos clientes. A especificação em demasia sobre a infraestrutura não é relevante em um modelo de nuvem, já que a infraestrutura e os equipamentos são de posse e administração do CSP. Isso permite que os clientes mudem o foco dos requisitos de hardware para o desempenho do aplicativo. O CSP deve fornecer uma plataforma altamente segura e independente de linguagem e sistema operacional. No caso da AWS, os clientes recebem um ambiente virtual que lhes permite escolher o sistema operacional, a linguagem de programação, a plataforma de aplicação Web, o banco de dados e outros serviços de que necessitam.	**GSA, Escritório de serviços do cidadão e tecnologias inovadoras (OCSIT) RFQ** • "(O CSP deve...) oferecer recursos para o consumidor para fornecimento, processamento, armazenamento, rede e outros recursos computacionais fundamentais em que ***o consumidor é capaz de implantar e executar softwares arbitrários, que podem incluir sistemas operacionais e aplicações. Não se espera que o consumidor gerencie ou controle a infraestrutura de nuvem subjacente***, mas ele deve ter controle sobre os sistemas operacionais, o armazenamento e as aplicações de implantação."

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
2. Acordos de nível de serviço **Problema potencial** Obrigatoriedade de SLAs específicos em vez de SLAs comerciais do CSP, ou seja, tempo de atividade, durabilidade, confiabilidade ou outros SLAs.	**Os CSPs devem** – oferecer compromissos de serviços por meio de SLAs comerciais, ou seja, tempo de atividade, durabilidade, confiabilidade ou outros SLAs. **Os clientes do setor público devem** – manter os CSPs nos mesmos padrões altos esperados de qualquer fornecedor de hardware ou software. No entanto, aconselhamos que as organizações evitem a obrigatoriedade de SLAs específicos fora dos SLAs comerciais disponíveis.	No caso da AWS, a nossa plataforma de nuvem funciona da mesma forma para todos os clientes. Não podemos administrar SLAs personalizados para clientes individuais, já que a AWS é um serviço sem interação pessoal e de baixa administração que opera em grande escala. Com relação à escrita, a AWS oferece os seguintes SLAs, que estão publicados no site da AWS: • SLA do Amazon EC2: http://aws.amazon.com/ec2-sla/ • SLA do Amazon S3: http://aws.amazon.com/s3-sla/ • SLA do Amazon CloudFront: http://aws.amazon.com/cloudfront/sla/ • SLA do Amazon Route 53: http://aws.amazon.com/route53/sla/ • SLA do Amazon RDS: http://aws.amazon.com/rds-sla/	**GSA, Escritório de serviços do cidadão e tecnologias inovadoras (OCSIT) RFQ** • "Como contratado, você é obrigado a ***enviar o seu padrão corporativo de SLA***. O SLA deve ser realista, mensurável, transparente e agressivo." **Declaração de trabalho (SOW) de computação em nuvem da agência NASA** • "A NASA vai ***estar ciente dos SLAs do CSP*** e implantar cargas de trabalho e aplicações importantes de tal forma que ela continue a operar no caso de um SLA não ser cumprido. ***A NASA será responsável pela manutenção de SLAs apropriados associados a qualquer equipamento de propriedade da NASA ou serviços operados pela NASA usados com o CSP***."

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
3. Serviços novos e modificados **<u>Problema potencial</u>** Inclusão de restrições ou exigências de consentimento sobre a capacidade do CSP de mudar e melhorar os serviços e recursos que estão disponíveis durante o período de vigência do contrato.	**Os CSPs devem** – fornecer um serviço do tipo de serviço de utilidade pública que tem valor por operar em grande escala. Essa escala impulsiona a inovação, e o CSP deve transmitir a inovação para os clientes sob a forma de novos e avançados serviços e recursos. **Os clientes do setor público devem** – aproveitar novos serviços e recursos durante a vigência do contrato.	A AWS evolui e aprimora continuamente os serviços existentes e adiciona novos serviços com frequência (a AWS lançou 516 novos serviços e recursos em 2014). A adoção da inovação e a capacidade de se ajustar aos serviços permite que os clientes do setor público se beneficiem de melhorias dinâmicas de serviços. Não é aconselhado acrescentar quaisquer restrições desnecessárias em uma solicitação de nuvem, como mudar os requisitos de consentimento, uma vez que eles podem limitar a capacidade de um CSP de se redimensionar, além de limitar a capacidade de um cliente de aproveitar as mudanças frequentes de serviços com inovações.	**New South Wales, Austrália – Aquisição de uma estrutura de TI** • "O cliente reconhece e concorda que o Como serviço pode ser disponibilizado ao cliente e outros clientes do contratado em uma forma de serviço compartilhado de uma base de código em comum e/ou ambiente em comum e ***<u>o contratado pode periodicamente: alterar, adicionar ou excluir funções, recursos, desempenho ou outras características do Como serviço e, se tal alteração, adição ou exclusão for feita, as especificações do Como serviço devem ser atualizadas de acordo</u>***." **RFI da Administração de segurança e benefícios a funcionários (EBSA) do Departamento do trabalho (DOL) dos EUA** • "Descreva a configuração proposta para cumprir as exigências do primeiro dia ***<u>com o entendimento explícito de que, durante a vigência do contrato, esses requisitos nominais do perfil mudarão</u>***. O fornecedor deve continuar a desenvolver e aprimorar a infraestrutura em conformidade com os requisitos emergentes e especificações de tecnologia em desenvolvimento, conforme exigido."
Definição de preço: Melhores práticas			

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
4. Modelos para definição de preços diferentes **<u>Problema potencial</u>** Inclusão de requisitos para descontos para todos, notificações personalizadas de mudança de definição de preço e qualquer outro requisito de definição de preços que não esteja incluído nos modelos de definição de preços públicos normais de um CSP**.**	**Os CSPs devem** – fornecer definições de preços transparentes e atualizadas e ferramentas que permitam aos clientes avaliar a definição de preços do CSP. **Os clientes do setor público devem** – avaliar diferentes modelos de definição de preços do CSP e selecionar o modelo que melhor atenda às suas necessidades específicas.	É desaconselhado incluir restrições de modelo de definição de preços em solicitações de nuvem. Permitir que os CSPs ofereçam diferentes modelos de definição de preços permite que os clientes do setor público avaliem cada modelo em relação aos seus próprios requisitos específicos. É importante evitar uma comparação de definição de preços específica feita através de unidades de computação ou armazenamento arbitrárias. As organizações do setor público devem usar definições de preço do CSP disponíveis publicamente no seu processo de avaliação. A AWS fornece uma calculadora simples mensal para discriminação dos custos e custo mensal total estimado, com base no uso estimado de cada serviço em nuvem da AWS: http://calculator.s3.amazonaws.com/index.html.	**Iniciativa de consolidação de datacenter federal, Aquisição de serviços em nuvem pública da agência civil (Draft RFP)** • "***<u>(O governo) solicita que as respostas do CSP incluam o seu método e o modelo de definição de preços proposto</u>*** para fornecer cada um desses sistemas aos usuários finais (do governo) como uma capacidade de nuvem pública. ***<u>(O governo) utilizará esta informação para avaliar as propostas recebidas</u>***."

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
5. Definição de preços variável **Problema potencial** Inclusão de requisitos para definição de preços fixos por um período.	**A definição de preços do CSP deve** – ser transparente e permitir a flutuação para refletir a natureza dinâmica e competitiva da computação em nuvem. **Os clientes do setor público devem** – adotar modelos de definição de preços variáveis, a fim de se beneficiar das quedas de preços dinâmicas.	Aconselhamos que as solicitações de nuvem incluam disposições que aproveitem a natureza elástica da computação em nuvem. Elas devem solicitar que os CSPs ofereçam um modelo de pagamento de acordo com uso como dos serviços de utilidade pública, em que, no final de cada mês, o pagamento seja feito de acordo com o uso durante esse mês. Uma abordagem flexível de definição de preços reflete a natureza dinâmica e competitiva de definição de preços da nuvem e apoia a inovação e a redução dos preços. No momento que esse documento foi escrito, a AWS havia baixado os preços 48 vezes: https://aws.amazon.com/pricing/).	**Declaração de trabalho (SOW) de computação em nuvem da agência NASA** • "Transparência de definição de preços e ***Passagem de redução de preços para*** a NASA. ***Devido à tendência constante à diminuição de preços na definição de preços em serviços em nuvem comercial, impulsionada por novas tecnologias e pela competição***, juntamente com o nível mínimo absoluto de serviços de valor agregado solicitados do revendedor nesta SOW, ***o custo unitário de serviço do CSP calculado pago pela NASA sob esta ordem de entrega nunca poderá ultrapassar a definição de preços por unidade do CSP publicada no site do CSP, que é válida no momento em que a unidade de serviço é consumida pela NASA***." **GSA, Escritório de serviços do cidadão e tecnologias inovadoras (OCSIT) RFQ** • Requisitos básicos: a. Fornecer uma solução inovadora, escalonável e econômica que atenda requisitos de curto prazo e tempo de execução rápido para infraestrutura de nuvem da GSA, reduzindo os custos e riscos e ganhando eficiência. b. ***Fornecer serviços em nuvem com um modelo de definição de preços dinâmico que oferece flexibilidade máxima de negócios e permite a escalabilidade e o crescimento.***

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
6. Faturamento **Problema potencial** Solicitação que o CSP forneça faturamento adaptado e personalizado.	**Os CSPs devem** – fornecer aos clientes as ferramentas necessárias para gerar relatórios detalhados de faturamento. **Os clientes do setor público devem** – utilizar ferramentas de faturamento do CSP para gerar relatórios detalhados de faturamento para satisfazer as suas necessidades de negócios e de conformidade. Os clientes podem trabalhar em conjunto com os parceiros de consultoria para aproveitar a experiência deles na gestão de aplicativos de nuvem e cargas de trabalho.	Os clientes da AWS podem gerar relatórios detalhados de faturamento que detalhem seus custos por hora, dia ou mês, por cada conta em sua organização, por produto ou recurso do produto ou por tags que os clientes definem. Os clientes podem criar tags para seus recursos da AWS para adicionar seus próprios rótulos a quase todos os itens de linha em seus relatórios. Informações completas sobre o faturamento da AWS estão disponíveis no site da AWS: http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/DetailedBillingReports.html A rede de parceiros da AWS (APN) http://aws.amazon.com/partners/ pode ajudar clientes do setor público que procuram auxílio para personalizar relatórios de faturamento e gerenciar cargas de trabalho na nuvem.	**Declaração de trabalho (SOW) de computação em nuvem da agência NASA** • "A NASA planeja ***usar tags de uso e alocação de custos para custo granular e outros relatórios dentro de todas as contas vinculadas do CSP***."

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
7. Calendário de itens comerciais – "Em contrato" ou "Atualização de tecnologia" **Problema potencial** Exigência que um CSP forneça uma lista de preços e produtos/serviços que não leve em consideração as mudanças nos preços. Esboço de um processo rígido em que o contrato é modificado (ou "atualizado") para incluir novos preços, que é, então, contratualmente aceito pelo cliente.	**Os clientes do setor público devem** – adotar modelos de definição de preços variáveis, além de simplificar os processos de aquisição existentes, a fim de aproveitar a rápida escalabilidade da nuvem e entrega sob demanda.	Não é aconselhado acrescentar quaisquer processos desnecessários em uma solicitação de nuvem que limitem a capacidade de redimensionar e aproveitar as reduções de preços e as mudanças de serviços inovadores frequentes. Os clientes do setor público não conseguirão perceber todos os benefícios da nuvem se exigirem que as alterações nos preços sigam um processo tradicional de alteração contratual, como no caso de um GWAC ser modificado (ou "atualizado") para incluir novos preços uma vez que o governo os aceite contratualmente.	**GSA, Escritório de serviços do cidadão e tecnologias inovadoras (OCSIT) RFQ** • "O Contratado deverá fornecer uma solução com bom custo-benefício que utilize tecnologias de virtualização comprovadas e estáveis e ***tecnologias de ponta em constante atualização***."
8. Taxas contratuais e encargos administrativos **Problema potencial** Exigência que os CSPs se apresentem e paguem uma taxa para a agência governamental que administra o contrato**.**	**Os clientes do setor público devem** – levar em consideração como o acesso ao contrato e as taxas administrativas podem ser reestruturadas para melhor utilização de um modelo de computação em nuvem.	Como a computação em nuvem é um item comercial e um serviço não gerenciado, as taxas dos contratos não são escaláveis em um modelo de nuvem, e os processos administrativamente onerosos, como este, podem dificultar a capacidade dos clientes do setor público de aproveitar a rápida escalabilidade da nuvem e a entrega sob demanda.	
Segurança e garantia: Melhores práticas			

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
9. Padrões de segurança/credenciamentos de terceiros **<u>Problema potencial</u>** Exigência de práticas de segurança específicas que são redundantes ou incompatíveis com os padrões do setor.	**Os CSPs devem** – fornecer documentação que detalhe normas de segurança e credenciamentos de terceiros relativos às práticas atuais. **Os clientes do setor público devem** – aproveitar as certificações de terceiros para evitar sujeitar-se a fluxos de trabalho de aprovação ou processos excessivamente onerosos que podem não ser justificados pelo risco real e pelas necessidades de conformidade.	Os CSPs devem oferecer instalações de alta segurança e infraestrutura de nuvem para proteger os aplicativos e dados dos clientes, além de uma extensa rede de sistemas de monitoramento de segurança. A infraestrutura de nuvem deve fornecer diversos recursos de segurança incorporados para que os clientes possam se concentrar apenas na segurança do sistema operacional e aplicativos de convidados. O atendimento às ofertas de segurança personalizadas para cada cliente eliminaria a capacidade de um CSP de escalonar e transmitiria inovação e benefícios de redução de custos para os clientes corretamente. No caso da AWS, estamos em conformidade com os mesmos padrões de segurança altos para todos os clientes e não nos comprometemos a disponibilizar segurança personalizada para os nossos clientes, grandes ou pequenos. Um exemplo importante de um credenciamento de terceiro é o programa FedRAMP do Governo Federal dos Estados Unidos. O FedRAMP é projetado para fornecer uma abordagem padronizada de avaliação, autorização e monitoramento contínuo da segurança para produtos e serviços de nuvem. Para muitos clientes (de dentro e fora os EUA), o FedRAMP é usado como um padrão do ponto de vista de segurança, além dos termos e condições padrão de um CSP relacionados à segurança. Outros governos e entidades do setor público têm suas próprias políticas de segurança respeitadas por eles. Aconselhamos que as	**Serviços de computação em nuvem de Oklahoma** • "O Ofertante deve ***<u>observar os seguintes padrões ou requisitos de controle de segurança, operações e ambiente e enviar relatórios anuais: checklist SAS 70 type II Data Center e FedRAMP</u>***." **Serviços de apoio e hospedagem na nuvem da agência civil através do ECSIII** • "O contratado ***<u>deverá ser um provedor de serviços em nuvem (CSP) compatível com FedRAMP</u>***." **DC2.0 – Plataforma (europeia) de serviços de infraestrutura (do governo)** • "Os candidatos selecionados poderão, posteriormente, demonstrar na sua proposta ***<u>que eles satisfazem as condições de conformidade por meio de relatórios de terceiros</u>*** levando, de forma independente, a garantia independente sobre a eficácia do seguinte processo mínimo: http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf"

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
		organizações do setor público investiguem os credenciamentos, termos e padrões de segurança de terceiros de um CSP e os avalie para garantir que eles satisfaçam as suas próprias necessidades de segurança. Para uma revisão abrangente das práticas de segurança da AWS, visite os links abaixo: • Centro de Segurança da AWS: http://aws.amazon.com/security/ • Conformidade com a AWS: http://aws.amazon.com/compliance/ • FedRAMP: http://aws.amazon.com/compliance/fedramp-faqs/ (consulte a página 34 para obter informações sobre a conformidade do FedRAMP da AWS)	

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
10. (a) Propriedade de dados **Problema potencial** Exigência que um CSP gerencie ou controle os dados dos clientes de uma forma prescritiva.	**Os CSPs devem** – permitir que os clientes coloquem e retirem dados da plataforma, conforme necessário, usando a Internet pública e/ou meios alternativos e não proibir clientes de remover seus dados. **Os clientes do setor público devem** – ter uma compreensão clara de suas funções e responsabilidades em relação à propriedade e à gestão de dados e colocar em prática medidas adequadas para armazenar e proteger dados.	Existem quatro princípios importantes em matéria de propriedade e gerenciamento de dados no modelo de responsabilidade compartilhada da AWS: • Os clientes continuam a ser donos dos seus dados. • Os clientes escolhem as localizações geográficas em que desejam armazenar seus dados; elas só são alteradas por decisão do cliente. • Os clientes podem fazer o download ou excluir seus dados sempre que quiserem. • Os clientes devem considerar a confidencialidade dos seus dados e decidir se e como criptografar os dados enquanto estiverem em trânsito e/ou parados. Os clientes podem, com base no modelo padrão amplamente aceito de computação em nuvem IaaS/PaaS, encerrar, a qualquer momento, e extrair/mover os dados do provedor de nuvem, de forma rápida e em um formato aceito, sem precisar se comunicar com o fornecedor. A AWS permite que clientes retirem ou coloquem dados, conforme necessário, no armazenamento da AWS usando a Internet pública ou serviços em nuvem da AWS, como AWS Direct Connect (http://aws.amazon.com/directconnect/) e AWS Import/Export (http://aws.amazon.com/importexport/).	**New South Wales, Austrália – Aquisição de uma estrutura de TI** • "***O cliente é o único responsável por todos os dados do cliente*** e ele e seus usuários permitidos são os únicos responsáveis pela inserção de dados de cliente no Como serviço, realizando manutenção de dados de clientes (incluindo backup e restauração de dados de clientes)." "Salvo disposição em contrário nos documentos de ordem, o cliente é o único responsável por: a. configurar, instalar, fazer manutenção e obter licenças para qualquer software, aplicativo ou outros materiais que possam ser instalados, localizados, hospedados ou armazenados de outra forma na Infraestrutura como serviço; b. garantir que todos os conteúdos e dados armazenados ou retidos de outra forma na Infraestrutura como serviço possuam um backup e que as mídias em que estão as cópias de backup estejam armazenadas de forma segura; c. restaurar dados ou conteúdos de mídias de backup; implementar e fazer manutenção das medidas de segurança para proteger os dados, softwares, aplicativos ou outros materiais que estão instalados, localizados, hospedados ou armazenados de outra forma na Infraestrutura como serviço; obter todas as autorizações de terceiros que são necessárias para permitir que o cliente armazene os dados e conteúdos relevantes na Infraestrutura como serviço; e ***todo o uso da infraestrutura como serviço por qualquer pessoa***."

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
			Iniciativa de consolidação de datacenter federal, Aquisição de serviços de nuvem pública da agência civil (Draft RFP) • "(O governo) está à procura de propostas que ***proporcionem uma estratégia de saída razoável e evitem a fidelização obrigatória a um CSP***. Uma estratégia de saída deve incluir custos de saída nulos (por exemplo, sem fidelização) para migrar para outros provedores ou governo, se necessário."
10. (b) Localização e soberania de dados **Problema potencial** Exigência que um CSP mantenha dados de clientes em locais específicos, ou proibição de colocação de dados em determinadas áreas geográficas (ou seja, fora dos EUA).	**Os CSPs devem** – permitir que os clientes mantenham o controle total sobre os seus dados, e escolham em quais localizações geográficas desejam armazenar os dados. **Os clientes do setor público devem** – ter uma compreensão clara de suas funções e responsabilidades em relação à propriedade e à gestão de dados e compreender que a escolha da localização geográfica para se armazenar os dados é uma responsabilidade do cliente.	As solicitações de nuvem não devem exigir que os fornecedores mantenham os dados em locais específicos, mas devem exigir que os fornecedores ofereçam algumas regiões globais em que os clientes possam armazenar seus dados. Sob o modelo de responsabilidade compartilhada da AWS, os clientes escolhem as localizações geográficas em que desejam armazenar seus dados, e eles não são movidos a menos que um cliente solicite. Informações sobre as 11 regiões da AWS estão disponíveis em: http://aws.amazon.com/about-aws/global-infrastructure/	**Comando de sistemas de guerra naval e espacial (SPAWAR), RFI de consolidação de datacenter** • "Onde a hospedagem de dados descrita está sendo realizada? ***É possível limitar a hospedagem para os EUA*** com seu modelo de serviço?" **Iniciativa de consolidação de datacenter federal, Aquisição de serviços de nuvem pública da agência civil (Draft RFP)** • "O CSP deve fornecer uma solução virtualizada ***com bom custo-benefício e com uma carga balanceada*** geograficamente (dentro do território continental dos EUA)."

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
10. (c) Gerenciamento de criptografia/caução de chave **<u>Problema potencial</u>** Exigência que um CSP tome medidas em relação a chaves de criptografia que são responsabilidade do cliente (ou seja, fazer caução de chaves).	**Os CSP devem** – fornecer uma ampla gama de recursos de segurança que os clientes possam usar para proteger suas instâncias e dados. **Os clientes do setor público devem** – ter uma compreensão clara de suas funções e responsabilidades em relação à propriedade e ao gerenciamento de dados e entender que a criptografia de dados e as medidas de criptografia de segurança relacionadas (como fazer caução de chaves) são responsabilidades do cliente.	De acordo com o modelo de responsabilidade compartilhada da AWS, os clientes mantêm controle e posse dos seus dados. Todos os dados armazenados pela AWS em nome dos clientes têm recursos sólidos de segurança e controle de isolamento de locatários. Os clientes devem considerar a confidencialidade dos seus dados e decidir se e como criptografarão os dados enquanto estiverem em trânsito e/ou parados. No caso da AWS, os serviços são "independentes do conteúdo", o que significa que todo o conteúdo é tratado com o mesmo nível de cuidado alto, do conteúdo público ao conteúdo mais confidencial. Cabe ao cliente determinar o quão confidencial é o seu conteúdo e, para conteúdos mais confidenciais, colocar em prática layers adicionais de segurança conforme o modelo de responsabilidade compartilhada. É de responsabilidade do cliente armazenar chaves em caução ou tomar outras medidas necessárias de proteção de chaves de criptografia. O *Whitepaper de melhores práticas de segurança da AWS* disponibiliza detalhes sobre como proteger dados parados e em trânsito na nuvem da AWS: http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf	**GSA, Escritório de serviços do cidadão e tecnologias inovadoras (OCSIT) RFQ** • "Fornecer um método seguro de fator duplo de acesso remoto para dar à equipe designada da GSA a capacidade de desempenhar funções na infraestrutura hospedada. Esse acesso ***<u>deve permitir o acesso sem cliente (baseado na Web) que atenda à criptografia validada FIPS 140–2 e à autorização do FedRAMP</u>*** conforme detalhado nos Requisitos de segurança de rede." **Infraestrutura e hospedagem de nuvem da Plataforma geoespacial nacional (GSP) do Gabinete do secretário de informações geográficas (OGIO) do Departamento do Interior (DOI)** • "O Contratado deverá disponibilizar os seguintes serviços: ***<u>Disponibilizar capacidade de criptografia</u>*** para serviço de armazenamento de dados de nível de objeto. ***<u>Disponibilizar capacidade de criptografia</u>*** para serviço de armazenamento de dados em nível de objeto com chaves gerenciadas e baseadas no cliente."

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
11. Apagamento seguro **Problema potencial** Exigência que um CSP tome certas medidas quando os dados são apagados fora do processo de desativação de armazenamento documentado de um CSP.	**Os CSPs devem** – disponibilizar aos clientes a capacidade de apagar dados, além de informações sobre o processo de desativação de armazenamento do CSP. **Os clientes do setor público devem** – compreender as suas funções e responsabilidades com relação à eliminação segura de dados.	Os CSP devem disponibilizar aos clientes a capacidade de apagar seus dados e devem documentar como desativar os dispositivos com segurança. De acordo com o modelo de responsabilidade compartilhada da AWS, os clientes retêm controle e propriedade de seus dados, portanto, é responsabilidade do cliente gerenciar os dados. Como parte do processo de desativação de armazenamento da AWS, quando um dispositivo de armazenamento atinge o final da sua vida útil, os procedimentos da AWS incluem um processo de desativação que é projetado para impedir que os dados do cliente sejam expostos a pessoas não autorizadas. A AWS usa as técnicas detalhadas no DoD 5220.22-M ("Manual operacional do programa de segurança industrial nacional") ou NIST 800-88 ("Orientações para o tratamento de mídia") para destruir dados como parte do processo de desativação. Todos os dispositivos de armazenamento magnético desativados são desmagnetizados e fisicamente destruídos conforme as práticas padrão do setor.	**Declaração de trabalho (SOW) de computação em nuvem da agência NASA** • "Os proprietários de dados e sistema da NASA são responsáveis por aderir às políticas de retenção de dados da NASA. Com relação aos dados produzidos e/ou gerenciados pelo CSP por meio da atividade de prestação de serviços em nuvem, a ***NASA vai rever periodicamente, utilizando o processo de Monitoramento contínuo FedRAMP, se o CSP está mantendo adequadamente sua retenção e destruição de dados***."

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
12. Limpezas de segurança de equipe, Treinamento de privacidade ou Acordos de confidencialidade (NDAs) **<u>Problema potencial</u>** Exigência que os funcionários do CSP façam limpezas de segurança, participem de ações de treinamento exigidas pelo cliente ou assinem NDAs.	**Os clientes do setor público devem** – evitar incluir requisitos de funcionários em solicitações de nuvem.	Os fornecedores de itens comerciais normalmente não vão negociar a força de trabalho, fornecer currículos ou fazer com que os indivíduos se dediquem a pedidos personalizados. As limpezas de segurança, os pedidos de treinamentos únicos e os NDAs podem minar, de forma significativa, a capacidade de um CSP escalonar seus serviços e não são relevantes quando se compra um serviço de item comercial. No caso da AWS, não temos quaisquer direitos de acesso às instâncias, aos dados ou ao sistema operacional convidado dos clientes. Os controles estão em conformidade para garantir que o acesso a locais de datacenter, aplicativos, programas ou código-fonte do objeto da AWS seja restrito apenas ao pessoal autorizado. Em alinhamento com os padrões da ISO 27001, a AWS estabeleceu procedimentos e políticas formais para delinear os padrões mínimos para acesso lógico aos recursos da AWS. O relatório SOC 1 tipo II da AWS descreve os controles vigentes para gerenciar o provisionamento de acesso aos recursos da AWS. No que diz respeito aos requisitos de verificação de antecedentes no que se refere a controles de segurança, a documentação da AWS desses controles pode ser vista como uma parte da submissão de FedRAMP da AWS, que está disponível mediante solicitação para AWS ou FedRAMP. Se necessário, a APN inclui parceiros que mantêm as credenciais de limpeza de segurança necessárias para obter acesso a instalações do governo: http://aws.amazon.com/partners/.	

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
13. Análise forense (incluindo varredura de vulnerabilidades e testes de penetração) **Problema potencial** Exigência que um CSP permita que clientes ou designatários de clientes realizem investigações forenses de rede, instalações, dados, registros de logs ou outros bens do CSP como parte de uma investigação.	**Os CSPs devem** – permitir que os clientes realizem procedimentos forenses, como testes de penetração e varredura de vulnerabilidades das instâncias virtuais dos clientes. Os CSPs devem fornecer documentação detalhando as medidas de monitoramento de infraestrutura de nuvem e os procedimentos de varredura de vulnerabilidade. **Os clientes do setor público devem** – aproveitar os recursos de segurança disponibilizados pelos CSPs para proteger suas instâncias e dados.	De acordo com o modelo de responsabilidade compartilhado pela AWS, os clientes detêm o controle de seus próprios softwares, aplicativos e sistemas operacionais convidados e são responsáveis por realizar varreduras de vulnerabilidade e correções de seus próprios sistemas. Os clientes da AWS podem solicitar permissão para executar varreduras em sua infraestrutura em nuvem, desde que se limitem a instâncias do cliente e não violem a política de uso aceitável da AWS. A prévia aprovação para esses tipos de verificações pode ser iniciada enviando-se uma solicitação por meio do formulário AWS Vulnerability/Penetration Testing Request (Solicitação de teste de penetração/ vulnerabilidade da AWS): http://aws.amazon.com/security/penetration-testing/. A segurança da AWS examina regularmente todos os endereços IP de endpoint de serviço voltado à Internet quanto à existência de vulnerabilidades (essas verificações não incluem instâncias de clientes). A segurança da AWS notificará as partes adequadas para solucionar quaisquer vulnerabilidades identificadas. Além disso, avaliações de ameaça de vulnerabilidade externa são realizadas regularmente por empresas de segurança independentes.	**Declaração de trabalho (SOW) de computação em nuvem da agência NASA** • "Definir ***parâmetros claros para o desempenho de varreduras de vulnerabilidades em andamento da NASA e testes de penetração de recursos gerenciados pela NASA dentro da plataforma do CSP***." **GSA, Escritório de serviços do cidadão e tecnologias inovadoras (OCSIT) RFQ** • "A pedido do governo, o ***contratado que está hospedando deve fornecer as seguintes informações de segurança de rede e documentação para fins de análise e auditoria***: ○ Configuração dos Sistemas de detecção de intrusão (IDS), ○ Configuração do firewall da rede, ○ Agendamento e conformidade das correções de dispositivos de rede e servidor, ○ Servidores, dispositivos de rede, logs de segurança e ○ Inventário de hardware detalhado incluindo servidores, dispositivos de rede e armazenamento. ○ E qualquer informação relacionada ao Processo de certificação e o credenciamento (C&A) feito pela GSA ou outras agências federais ou identificar a FedRAMP ATO que está no arquivo no FedRAMP Project Management Office."

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
14. Mecanismo de auditorias (Cláusulas de auditoria do governo) **Problema potencial** Exigência que um CSP permita que um cliente ou designatário de cliente faça auditoria das instalações do CSP, ou outros direitos de auditoria, como sistemas de faturamento.	**Os CSPs devem** – fornecer aos clientes acesso a relatórios de auditoria independentes que detalhem se os controles efetivos de segurança física estão em funcionamento. **Os clientes do setor público devem** – evitar incluir cláusulas de auditoria que possam não ser relevantes em solicitações de itens comerciais.	Os clientes devem utilizar as melhores práticas do setor sobre auditoria e segurança. A utilização desses credenciamentos de terceiros e padrões já estabelecidos simplifica o processo de aquisição e fornece aos clientes garantias de segurança. Existem estruturas de segurança, melhores práticas, padrões de auditoria e controles padronizados que as solicitações podem citar, como: FedRAMP, SOC 1/SSAE 16/ISAE 3402 (anteriormente SAS70), SOC 2, SOC 3, PCI DSS, ISO 27001, ISO 9001, DoD RMF (Modelo de segurança na nuvem), FISMA, ITAR e FIPS 140-2. No caso da AWS, não permitimos o acesso a datacenters para clientes, uma vez que isso expõe um vasto número de clientes ao acesso físico de terceiros. Em vez de permitir que clientes realizem auditorias físicas, a AWS pede que um terceiro independente realize auditorias de seus datacenters. Essas auditorias são realizadas de acordo com FedRAMP, a declaração sobre normas para comprovação de contratos nº 16 (SSAE 16) e as Normas internacionais para contratos de garantia nº 3402 (ISAE3402), normas profissionais. Os auditores produzem um relatório de controles de empresas de serviços 1 (SOC 1), tipo 2 junto com a auditoria. Análises independentes da segurança física do datacenter também fazem parte de uma auditoria ISO 27001, de uma avaliação do PCI e de uma auditoria dos ITAR. Algumas práticas governamentais tradicionais de aquisição exigem o acesso a instalações e o direito de examiná-las, ou exigem outros direitos de auditoria, como sistemas de faturamento. No entanto, esses requisitos não são adequados quando se compram serviços de nuvem de itens comerciais.	**GSA, Escritório de serviços do cidadão e tecnologias inovadoras (OCSIT) RFQ** • "A infraestrutura de hospedagem em nuvem precisa ser autorizada ***pelo FedRAMP e conseguir atender todos os requisitos*** de monitoramento contínuo no prazo de 180 dias a contar da atribuição deste BPA. Veja os controles de segurança do FedRAMP em cio.gov." **DC2.0 – Plataforma (europeia) de serviços de infraestrutura (do governo)** • "***A modificação da certeza de gerenciamento pode ser fornecida sob a forma de um relatório*** de conformidade SOC2 tipo 2 (ISAE3000) ou PCI DSS 2.0, um ISO 27001 ou ISO 27002 e/ou um relatório de auditoria externa semelhante." "O provedor de nuvem pode ***fornecer relatórios demonstrando que terceiros independentes respeitam, de forma completa, os procedimentos*** de segurança e SOC2 operacional como ISO 27002, PCI DSS 2.0, ISO 27001 tipo 2, etc."

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
15. Serviço de monitoramento e Gerenciamento de incidentes **<u>Problema comum</u>** Exigência de processos de monitoramento e gerenciamento de incidentes personalizados, como a exigência de parâmetros adaptados junto com notificações de incidentes/violações de segurança.	**Os CSPs devem** – fornecer aos clientes as ferramentas de monitoramento necessárias para controlar, de forma eficaz, seus serviços, além de detalhar os controles em vigor para monitorar a infraestrutura de nuvem do CSP. **Os clientes do setor público devem** – compreender as suas funções e responsabilidades em matéria de monitoramento de serviço e gerenciamento de incidentes.	De acordo com o modelo de responsabilidade compartilhada da AWS, os clientes têm a responsabilidade de monitorar suas próprias instâncias virtuais quanto a violações de privacidade. Os clientes da AWS podem aproveitar uma série de ferramentas de monitoramento de plataforma da AWS como Amazon CloudWatch, AWS CloudTrail, AWS Trusted Advisor, Verificação de saúde da AWS e ferramentas de monitoramento de terceiros para monitorar suas instâncias e extrair métricas e análise de sistema. O relatório SOC 1 tipo II da AWS fornece uma visão geral dos controles vigentes para monitorar o ambiente gerenciado da AWS. Os detalhes de monitoramento e gerenciamento de incidentes da AWS estão contidos no whitepaper de Visão geral de processos de segurança da AWS: https://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf Detalhes adicionais sobre monitoramento e gerenciamento de incidentes da AWS estão contidos no whitepaper de Risco e conformidade da AWS: http://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf	**GSA, Escritório de serviços do cidadão e tecnologias inovadoras (OCSIT) RFQ** • "O ***<u>contratado deverá trabalhar com o Gabinete de gerenciamento do programa FedRAMP de acordo com seu FedRAMP Provisional ATO</u>***, e com o ISSM ou ISSO designado pelo governo para oferecer suporte a requisitos de informação em desenvolvimento no prazo de 2 horas após o incidente. A documentação desenvolvida no âmbito do presente BPA deve ser entregue conforme especificado para entrega ao Representante do gabinete de contratação (COR) e FedRAMP. ***<u>O Contratado que está hospedando deverá ter um processo interno de resposta a incidentes</u>***. O governo federal definirá com o Contratado que está hospedando o que será incluído em um relatório de incidente." **Declaração de trabalho (SOW) de computação em nuvem da agência NASA** • "A NASA entende que ela mantém o controle dos seus próprios softwares, aplicativos e sistemas operacionais convidados e é responsável pelo desenvolvimento de um processo de resposta a incidentes para atender as suas exigências organizacionais para aqueles incidentes que não tenham sido causados pelo CSP nem requerem o envolvimento do CSP na sua resolução. ***<u>Para incidentes que exijam a notificação do CSP ou seu envolvimento na resolução, a NASA, por meio de um Plano de ações e marcos da NASA (POAM) para resposta a incidentes ocorridos na plataforma do CSP, tentará fazer um acordo com o CSP sobre as práticas de resposta a incidentes que serão aplicadas a utilização, pela NASA, dos serviços do CSP nessas circunstâncias.</u>***"
Termos e condições: Melhores práticas			

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
16. Nação mais favorecida **<u>Problema comum</u>** Exigência que os CSPs disponibilizem a menor definição de preço ou os termos mais favoráveis para o cliente.	**Os clientes do setor público devem** – adotar modelos de definição de preço variáveis a fim de aproveitar a rápida escalabilidade da nuvem, a entrega sob demanda e se beneficiar das quedas de preço dinâmicas. A inclusão de requisitos para oferecer uma definição de preço com menor preço ou termos mais favoráveis para o cliente não é apropriada em uma solicitação de nuvem de item comercial.	Deve-se evitar incluir nas solicitações de nuvem requisitos para oferecer aos clientes uma definição de preço com menor preço ou termos mais favoráveis. Uma abordagem flexível de definição de preços reflete a natureza dinâmica e competitiva de definição de preços da nuvem e apoia a inovação e a redução dos preços.	**Declaração de trabalho (SOW) de computação em nuvem da agência NASA** • "Devido à tendência constante à diminuição de preços na definição de preços em serviços em nuvem comercial, impulsionada por novas tecnologias e pela competição, juntamente com o nível mínimo absoluto de serviços de valor agregado solicitados do revendedor nesta SOW, ***<u>o custo unitário de serviço do CSP calculado pago pela NASA sob esta ordem de entrega nunca poderá ultrapassar a definição de preços por unidade do CSP publicada no site do CSP, que é válida no momento em que a unidade de serviço é consumida pela NASA</u>***. O mesmo requisito existe para os serviços do CSP não calculados consumidos pela NASA, como suporte a negócios e empresarial. Como ***<u>os usuários de tecnologia da informação da NASA são extremamente conscientes da definição de preço publicada e prezam que a NASA tenha a garantia de receber a melhor definição de preço</u>*** possível, o pedido do revendedor por descontos apropriados apresenta a melhor oportunidade para esta ordem de entrega ser vista como respondendo, de forma continua, às necessidades da agência e com uma utilização cada vez maior. Além disso, CSSO avaliará, constantemente, a dinâmica de loja de serviços de nuvem, em nome da base de usuários da NASA, para garantir que essa ordem de entrega continue a ser o melhor veículo possível para que os serviços do CSP adquiridos atendam às diversas necessidades da agência, com relação a custos e outras questões."

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
17. Capacidade para encerrar a prestação de serviços **<u>Problema comum</u>** Exigência de uma data de fim de contrato especificada, ou não inclusão de direito de rescisão, tanto para o CSP quanto para o cliente.	**Os CSPs devem** – permitir que os clientes rescindam o contrato a qualquer momento que lhes convir. **Os clientes do setor público devem** – garantir que são capazes de encerrar a prestação de serviços com um CSP a qualquer momento.	No caso da AWS, é possível encerrar a prestação de serviços a qualquer momento. A AWS não celebra acordos com um prazo que termina em uma data especificada. Se a prestação de serviços fosse encerrada em uma data especificada, a AWS seria forçada a encerrar uma conta do cliente naquela data, o que poderia causar a um cliente a perda de dados e de trabalho valioso. No entanto, um cliente pode colocar em prática um processo interno para controlar e monitorar uma data final e encerrar a prestação de serviços na data desejada.	**Instituto nacional de normas e tecnologia (NIST), Escritório de gerenciamento de sistemas de informação (OISM) - Pedido de cotação (RFQ)** • "Que métodos devem ser considerados para proteger e devolver os dados de um cliente quando requisitado ou em caso de rescisão do contrato?" **Serviços de nuvem da NASA Enterprise** • "Os dados armazenados em um provedor de serviço podem ser exportados por solicitação do cliente. O CSP permite que os clientes movam os dados no armazenamento da AWS ou os retirem do armazenamento conforme necessário. Além disso, ao utilizar infraestrutura virtual, o CSP permite que imagens de máquina virtual sejam baixadas e postadas em um novo provedor de nuvem. Os clientes podem exportar suas AMIs e usá-las localmente ou em outro provedor (sujeito a restrições de licenciamento de software)."

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
18. Encargos administrativos/gerenciamento de contrato **<u>Problema comum</u>** Exigência que o CSP participe de reuniões, forneça avisos personalizados, relatórios sobre o uso e faturas personalizadas ou ofereça suporte ou consulta fora dos serviços normais.	**Os clientes do setor público devem** – incluir requisitos relevantes para serviços de itens comerciais que não incluam horas de trabalho.	Os CSPs disponibilizam serviços de itens comerciais que dependem de escala e, portanto, não podem assumir pedidos personalizados, como a participação de reuniões regulares de clientes, o fornecimento de avisos personalizados, relatórios personalizados sobre o uso, faturas personalizadas ou o fornecimento de consulta fora dos serviços normais. A AWS não fornece ou oferece horas de trabalho; no entanto, a rede de parceiros da AWS (APN) pode fornecer serviços de trabalho intensivo adicionais.	**Instituto nacional de normas e tecnologia (NIST), Escritório de gerenciamento de sistemas de informação (OISM) - Pedido de cotação (RFQ):** • "Quais são as vantagens e desvantagens financeiras, legais e operacionais de um modelo de nuvem? Existem questões específicas sobre as quais o Estado deva estar ciente? ***<u>Que considerações de escalabilidade foram avaliadas com a expansão da prestação de serviços</u>***?" **Serviços de nuvem da NASA Enterprise** • "A NASA planeja usar tags de uso e alocação de custos para custo granular e outros relatórios dentro de todas as contas vinculadas do CSP. Para isso, a NASA disponibilizará, regularmente, ao revendedor uma lista de tags de uso e alocação de custos novas e que não são mais requeridas para que o revendedor possa indicar quais serão incluídas ou excluídas nos relatórios de faturamento acima exigidos pela NASA. • O revendedor deve permitir a geração de "relatórios de faturamento detalhados" para cada conta da NASA vinculada ao CSP selecionando a opção "receber relatórios de faturamento" na seção Preferências de cada Conta de faturamento consolidado usada para fornecer à NASA serviços de Faturamento consolidado para suas contas vinculadas ao CSP. • A NASA requer acesso a esses Relatórios detalhados de faturamento para gerir com responsabilidade os custos da Agência, de modo que o acesso irrestrito via ação do revendedor nos termos da presente ordem de entrega seja exigido como indicado a seguir para cada relatório de faturamento detalhado. - Relatório mensal - Relatório de faturamento detalhado - Relatório de alocação de custos mensal - Relatório de faturamento detalhado com recursos e tags"

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
19. Termos inaplicáveis e Requisitos de conformidade estatutária **Problema comum** Inclusão de referências aos estatutos que não pareçam aplicáveis às solicitações de nuvem – por exemplo, estatutos que lidem com a assistência a furacão, florestas tropicais, sinalização das embarcações de transporte, etc.	**Os clientes do setor público devem** – excluir referências a estatutos que não sejam aplicáveis.	Termos padrões e requisitos legais de compras de TI tradicionais podem não ser relevantes para ofertas do CSP de itens comerciais. Uma série de termos e estatutos tradicionais é independente e não aplicável à forma como um CSP fornece serviços – por exemplo, os estatutos que lidam com assistência a locais atingidos por furacão, sinalização das embarcações de navegação, conformidades com Energy Star, etc.	**Instituto nacional de normas e tecnologia (NIST), Escritório de gerenciamento de sistemas de informação (OISM) - Pedido de cotação (RFQ)** • "Esta é uma sinopse/solicitação combinada para itens comerciais preparada de acordo com o formato de procedimentos simplificados do Far subparte 12.6 para avaliação e solicitação de itens comerciais, complementada com informações adicionais incluídas no presente aviso. Esse anúncio constitui a única solicitação; cotações estão sendo solicitadas e um documento de solicitação escrito separado não será emitido. ***A solicitação está sendo emitida por meio de procedimentos simplificados de aquisição sob a autoridade do programa de teste Far 13.5 para determinados itens comerciais***."
20. Termos e estatutos em nível de pedidos (ou seja, nível de ordem de tarefas) **Problema comum** Inclusão de todos os termos e estatutos em nível de contrato mestre.	**Os clientes do setor público devem** – garantir que haja flexibilidade para fazer com que os termos e estatutos estejam no nível de pedido (ou seja, o nível de "ordem de tarefas"), em vez de incluir o espectro completo de termos e estatutos em nível de contrato mestre.	Em contratos de tipo "baseados em uma lista oficial de preços" como contratos de aquisição em âmbito governamental (GWACs), painéis, tecnologias e comunicação da informação (TIC) ou regimes de veículos de Entrega indefinida/quantidade indefinida (ID/IQ), recomendamos colocar a maior parte de termos e estatutos no pedido ou aproveitamento de ordem de tarefas, em comparação com nível de contrato mestre (por exemplo, Memorando de Entendimentos). Isso permitirá que usuários e agências individuais do setor público entrem em contato diretamente com um CSP, sem um amplo conjunto de termos e estatutos que podem não ser aplicáveis às necessidades de negócios do cliente.	**Projeto de trabalho de termos e condições e fator de avaliação para SIN de serviços de computação em nuvem Schedule 70 de TI** • "Responsabilidades da atividade de encomenda. **A atividade de encomenda é responsável por indicar requisitos de serviços de computação em nuvem exclusivos para a atividade de encomenda.** Os requisitos adicionais devem ser melhorias, esclarecimentos ou especificações de requisitos SIN existentes, mas não devem contradizer termos e condições de SIN e Schedule 70 de TI existentes. **As atividades de encomenda devem incluir (se aplicável) termos e condições para abordar definição de preço, segurança, propriedade de dados, restrições geográficas, privacidade, SLAs, etc.**"

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
21. Indenização **<u>Problema comum</u>** Exigência que um CSP defenda, ressarça ou cubra os cliente por quaisquer perdas ou danos que eles sofrerem, ou "reclamações de terceiros" contra um cliente.	**Os clientes do setor público devem** – entender por que os termos e condições do CSP são parte integrante do serviço e valor que eles oferecem.	Os preços fixos do CSP para os serviços têm por base a suposição de que o CSP está assumindo uma certa quantidade de risco ao oferecer os serviços. Este modelo de risco não assume que, se o cliente utilizar os serviços de forma não autorizada, o CSP sofrerá qualquer perda por essa atividade. Se um CSP fosse inserir esse risco em seu modelo de risco, provavelmente teria que cobrar um preço muito mais elevado por seus serviços.	
22. Indenização de patentes **<u>Problema comum</u>** Exigência que um CSP forneça indenização não nivelada.	**Os clientes do setor público devem** – entender por que os termos e condições do CSP são parte integrante do serviço e valor que eles oferecem.	No caso das patentes, um CSP é um provedor, o que significa que os serviços de CSP são usados como fundamentos nas soluções finais do cliente. Como um exemplo de por que uma indenização de patente não é aplicável em um contrato com um CSP, um cliente pode estar pagando a um CSP US$ 10.000 por mês para serviços de nuvem, mas ganhando US$ 50 milhões por mês para a solução que os serviços de nuvem estão sustentando. Se um CSP tivesse que indenizar o cliente, e um cliente fosse processado por violação de IP, as perdas que o CSP teria que cobrir seriam baseadas em uma porcentagem dos ganhos do cliente (US$ 50 milhões) em vez de uma porcentagem dos lucros do CSP (neste exemplo, US$ 10.000). O CSP poderia acabar perdendo desproporcionalmente mais do que recebeu, o que não é um modelo de negócio válido. Além disso, os CSPs não têm meios para precificar esse risco de indenização, já que não têm visibilidade ou influência quanto ao que os clientes carregam ou utilizam na conta deles. Esse tipo de risco normalmente não faz parte de como os CSPs precificam os serviços e, portanto, é improvável que seja a cobertura que os CSPs podem oferecer aos clientes.	
23. Propriedade intelectual (IP)	A relação entre o cliente e o CSP deve ser não exclusiva.	Um CSP e o cliente são independentes um do outro. Uma relação não exclusiva significa que cada uma das partes pode desenvolver produtos e serviços que competem com produtos e serviços da outra parte e trabalhar com terceiros que oferecem produtos ou serviços que competem com produtos e serviços da outra parte. CSPs e clientes contratam serviços em nuvem de forma comercial. Não há nenhuma troca de IP entre os CSPs e os clientes que não seja uma licença não exclusiva concedida ao cliente que utilizará os serviços do CSP.	
Práticas recomendadas adicionais			

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
24. Requisito de acessibilidade **<u>Problema comum</u>** Exigir que os produtos estejam em conformidade com os requisitos de acessibilidade que não se aplicam aos serviços de infraestrutura de nuvem comercial.	**Os clientes do setor público devem** – considerar se os requisitos de acessibilidade são aplicáveis à aquisição de serviços de itens comerciais, como IaaS e PaaS.	Não há nenhuma certificação formal para muitos requisitos de acessibilidade. Os serviços de infraestrutura de nuvem, como a AWS, são baseados em API, e as interfaces de gerenciamento normalmente são invisíveis aos usuários finais de aplicativos dos clientes. Por exemplo, um cliente de um serviço de vídeo streaming criado na AWS não precisa usar o AWS Management Console para aproveitar os serviços da AWS. Portanto, muitos requisitos de acessibilidade não são aplicáveis à infraestrutura de nuvem, já que ela não é acessada diretamente. A AWS oferece várias interfaces para seus serviços de computação em nuvem baseados em API, incluindo SDKs, kits de ferramentas IDE e ferramentas de linha de comando para desenvolvimento e gerenciamento de recursos da AWS. Além disso, a AWS oferece duas interfaces gráficas do usuário, o Console de Gerenciamento da AWS e o AWS ElasticWolf Client Console. O AWS ElasticWolf Client Console incorporou requisitos para a Seção 508 do Rehabilitation Act dos EUA, e a AWS preparou um modelo de acessibilidade de produto voluntário (VPAT, Voluntary Product Accessibility Template) para o Console, que descreve os recursos de acessibilidade do Console.	**RFP de serviços em nuvem da Universidade de Michigan** • "(23) Acesso para portadores de deficiência ***<u>Descreva brevemente os recursos atuais e roteiro para garantir que os serviços sejam acessíveis pela Web para portadores de deficiência.</u>*** Por exemplo: usuários (pesquisadores, estudantes), administradores de sistema, outros que exigem acesso a serviços de suporte, gerenciamento ou influência."

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
25. Privacidade de dados **<u>Problema comum</u>** Conformidade com requisitos de privacidade de dados como a Health Insurance Portability and Accountability Act (Lei da Portabilidade e Prestação de Contas em Seguro Saúde, HIPAA) dos EUA e outros requisitos de privacidade internacionais (por exemplo, Diretiva 95/46/CE do Parlamento Europeu sobre processamento e circulação de dados pessoais).	**Os CSPs devem** - fornecer aos clientes as informações necessárias para usar a AWS para armazenar conteúdos contendo dados pessoais. Se a conformidade com o HIPAA for um requisito do cliente, os CSPs devem poder oferecer um Acordo de Associados de Negócios (BAA, Business Associate Agreement) para o cliente aproveitar o cumprimento das responsabilidades do HIPAA de ambas as partes. **Os clientes do setor público devem** - aproveitar as certificações de conformidade dos CSPs, as informações de privacidade de dados e os BAAs para alcançar e manter a conformidade e a garantia de segurança enquanto estiverem usando os produtos e serviços dos CSPs.	Os ambientes dos CSPs devem ser projetados para oferecer aos clientes a capacidade de seguir uma ampla gama de padrões de proteção de dados e segurança internacional. Para aplicativos do cliente que utilizam informações de saúde protegidas (conforme definido no âmbito da HIPAA), a AWS pode oferecer um BAA e fornecer a infraestrutura técnica para permitir que os clientes atendam os requisitos de privacidade legais. O BAA da AWS leva em conta os serviços exclusivos que a AWS oferece e acomoda o modelo de responsabilidade compartilhada da AWS. Esse acordo permite que nossos clientes de saúde e ciências biológicas continuem a aproveitar a AWS para uma ampla gama de casos de uso do setor e tenham a capacidade para continuarem em conformidade com os regulamentos existentes e a regra finalizada recentemente emitida nos termos da HIPAA. Informações da AWS sobre proteção de dados e privacidade estão na nossa página de conformidade: http://aws.amazon.com/compliance/	**RFP de serviços em nuvem da Universidade de Michigan** (19a) Conformidade - HIPAA - Seus serviços estão em conformidade com a Health Insurance Portability and Accountability Act (Lei da Portabilidade e Prestação de Contas em Seguro Saúde, HIPAA)? Forneça mais explicações se necessário. - Sua empresa assinará um acordo de associados de negócios com a UMich conforme exigido pela HIPAA? - Em caso negativo, explique suas razões para podermos entender sua posição de negócios.

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
26. Solicitações de relatórios corporativos **Problema comum** Solicitar informações corporativas além das informações contidas nos relatórios anuais do CSP.	**Os clientes do setor público devem** – usar relatórios anuais do CSP para obter informações de fornecedores corporativos.	As solicitações de nuvem devem evitar a inclusão de requisitos para informações corporativas, como remuneração de membros do conselho ou executivos, que não são relevantes para a aquisição de um serviço de item comercial.	
27. Requisitos de seguro **Problema comum** Exigir que os CSPs mantenham tipos específicos de apólices de seguro e disposições para compensar o risco.	**Os clientes do setor público devem** - considerar o tipo de seguro que têm no momento e comparar com a quantidade de seguro adicional que é necessário de acordo com a responsabilidade compartilhada apropriada entre o CSP e o cliente. Adicionar requisitos adicionais de seguro pode afetar a capacidade de um CSP de dimensionar e repassar a economia de custos.	Além da responsabilidade dos CSPs de assegurar a infraestrutura, os serviços de itens comerciais que dependem de dimensionamento não podem assumir solicitações personalizadas de disposições e apólices de seguro adicionais. Clientes que buscam cobertura expandida para além de termos de contrato padrão de um CSP podem trabalhar com empresas de "seguro cibernético" de terceiros para cumprir as necessidades adicionais do seguro.	

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
28. Requisitos de subcontratação de pequenas empresas e empresas de minorias **<u>Problema comum</u>** Necessitar que o CSP utilize subcontratados, preferir certos subcontratados, entregar planos de subcontratação ou trabalhar com outras partes na entrega do contrato.	**Os clientes do setor público não devem** – incluir requisitos que não sejam aplicáveis aos serviços de itens comerciais, como o uso de certos subcontratados.	Normalmente, os CSPs não fornecerão ou apresentação propostas a empresas subcontratadas.	
29. Repasse obrigatório a subcontratados **<u>Problema comum</u>** Exigir que um CSP repasse certas cláusulas obrigatórias a todos os subcontratados.	**Os clientes do setor público não devem** – incluir requisitos que não sejam apropriados para serviços de itens comerciais, como cláusulas de repasse a subcontratados.	Em alguns tipos de contrato, existem cláusulas que exigem que o contratado principal repasse certas cláusulas obrigatórias a todos os parceiros/subcontratados. Normalmente, os CSPs não fornecerão ou farão proposta como parceiros formais de subcontratação, já que eles oferecem um serviço de item comercial e podem não ter uma estrutura de empresa configurada para administrar esses termos. Em um modelo de aquisição indireta (aquisição de serviços em nuvem por meio de um SI ou uma consultoria), um CSP pode rejeitar essas cláusulas oriundas de revendedores de valor agregado (VARs) e parceiros de SI como não aplicáveis a um fornecedor de serviços comerciais de "2ª camada". Em um modelo de aquisição direta (compra de serviços em nuvem diretamente de um CSP), um CSP normalmente rejeitaria essas cláusulas "obrigatórias" apropriadas para um subcontratado típico de commodities devido à natureza comercial dos serviços contratados e o fato de que a maioria dos CSP não exige que os subcontratados forneçam os serviços comerciais deles.	

Item	Melhores práticas	Considerações adicionais	Exemplo de linguagem de solicitações do setor público
30. Critérios de avaliação **<u>Problema comum</u>** Focar os requisitos em especificações sobre o desempenho da infraestrutura subjacente, como disponibilidade, tamanhos de máquina, tempos de resposta, etc.	**Os CSPs devem** - fornecer as ferramentas necessárias para permitir que os clientes avaliem os produtos e preços dos CSPs. **Os clientes do setor público devem** - determinar critérios de avaliação de solicitação com base em requisitos de desempenho da aplicação.	Os critérios de avaliação devem concentrar-se nos requisitos de desempenho do sistema em nível de aplicativo. Um CSP qualificado deve ser selecionado a partir de um pool de recursos estabelecido a fim de aproveitar das vantagens da elasticidade da nuvem, da eficiência em termos de custo e da rápida escalabilidade. Dessa forma, os clientes podem garantir que estão recebendo os melhores serviços de nuvem para atender às suas necessidades, o melhor valor (menor custo) e a capacidade de aproveitar a inovação impulsionada pelo mercado.	

Informações adicionais sobre aquisição de nuvem

As seções a seguir oferecem informações adicionais sobre aquisição de nuvem, com links para recursos sobre aquisição de nuvem.

Termos de itens comerciais

A fim de maximizar os benefícios da computação em nuvem, os termos comerciais devem reger o contrato. O governo federal dos EUA, por exemplo, tem uma política de aquisição publicada que favorece a compra de itens comerciais ao invés de itens desenvolvidos exclusivamente para o governo. Essa política é projetada para tirar vantagem total das inovações disponíveis e em desenvolvimento do setor comercial e permite que os itens comerciais sejam aceitos pelo governo sem preparações adicionais ou restrições contratuais. Consulte o regulamento de aquisição federal (FAR, Federal Acquisition Regulation) do governo federal dos EUA, subparte 12.3 – Provisionamento de solicitações e cláusulas de contratos para aquisição de itens comerciais (Solicitation Provisions and Contract Clauses for the Acquisition of Commercial Items) e a lei de otimização de aquisições federais (FASA, Federal Acquisition Streamlining Act) no link a seguir: http://www.acquisition.gov/far/html/FARTOCP12.html.

Governos estaduais, locais e internacionais devem utilizar suas próprias condições e políticas de compra de itens comerciais.

Definições do NIST para computação em nuvem

Para entender os requisitos relevantes em uma solicitação de nuvem, é importante compreender que a computação em nuvem tem vários modelos de utilização e implantação, incluindo nuvem privada, nuvem de comunidade, nuvem pública e nuvem híbrida, juntamente com IaaS, PaaS e SaaS. As informações e os padrões internacionalmente aceitos desses e de outros tipos de serviços em nuvem podem ser encontrados no site do NIST: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

Software como serviço (SaaS): O recurso fornecido ao cliente é usar aplicativos do provedor em execução em uma infraestrutura em nuvem. Os aplicativos são acessíveis de vários dispositivos do cliente por meio de uma interface simples com o cliente, como um navegador da web (p. ex., email com base na web) ou uma interface de programa. O cliente não gerencia ou controla a infraestrutura em nuvem subjacente que inclui rede, servidores, sistemas operacionais, armazenamento ou mesmo recursos de aplicativos individuais, com a possível exceção de limitadas definições de configurações do aplicativo, específicas do usuário.

Plataforma como serviço (PaaS) O recurso fornecido ao cliente é implantar aplicativos criados ou adquiridos pelo cliente na infraestrutura em nuvem criados por meio de linguagens de programação, bibliotecas, serviços e ferramentas suportadas pelo provedor. O cliente não gerencia ou controla a infraestrutura em nuvem subjacente que inclui rede, servidores, sistemas operacionais ou armazenamento, mas tem controle sobre os aplicativos implantados e possivelmente sobre definições de configurações para o ambiente de hospedagem do aplicativo.

Infraestrutura como serviço (IaaS): O recurso fornecido ao cliente é provisionar o processamento, o armazenamento, as redes e outros recursos fundamentais de computação, onde o cliente tem a capacidade de implantar e executar softwares arbitrários, que podem incluir sistemas operacionais e aplicativos. O cliente não gerencia ou controla a infraestrutura em nuvem subjacente, mas tem controle sobre os sistemas operacionais, o armazenamento e os aplicativos implantados e possivelmente controle limitado sobre determinados componentes de rede (p. ex., firewalls do host).

Segurança e conformidade

Existem diversas estruturas de segurança, melhores práticas, padrões de auditoria e controles padronizados que as solicitações de nuvem podem citar, como:

- Programa federal de gerenciamento de risco e autorização (Federal Risk and Authorization Management Program, FedRAMP)
- Controles de empresas de serviços (Service Organization Controls, SOC) 1/Declaração sobre normas para comprovação de contratos (Statement on Standards for Attestation Engagements, SSAE) 16/Normas internacionais para contratos de garantia (International Standard on Assurance Engagements, ISAE) 3402 (anteriormente conhecida como Declaração sobre normas de auditoria [SAS] Nº 70)
- SOC 2
- SOC 3
- Padrão de segurança de dados do setor de cartão de pagamento (Payment Card Industry Data Security Standard, PCI DSS)
- Organização internacional para padronização (International Organization for Standard, ISO) 27001
- ISO 9001
- ISO 27001
- Modelo de segurança de nuvem (Cloud Security Model, CSM) da Estrutura de gerenciamento de riscos do Departamento de defesa (Department of Defense Risk Management Framework, DoD RMF)
- Lei federal de gestão de segurança da informação (Federal Information Security Management Act, FISMA)
- Regulamentos sobre o tráfico internacional de armas (International Traffic in Arms Regulations, ITAR)
- Norma federal de processamento de informações (Federal Information Processing Standard, FIPS) 140-2

- Lei da privacidade e dos direitos educacionais da família (Family Educational Rights and Privacy Act, FERPA)
- IRAP (Austrália)

Para obter informações sobre todos os padrões e regulamentos de segurança com os quais a AWS tem conformidade, visite a página de conformidade da AWS: http://aws.amazon.com/compliance/.

O FedRAMP é um programa governamental federal dos EUA que fornece uma abordagem padronizada de avaliação, autorização e monitoramento contínuo da segurança para produtos e serviços em nuvem. O FedRAMP é obrigatório para implementações de agências federais na nuvem e para modelos de serviço com níveis de impacto de risco baixo e moderado. E a exigência da Secretaria de Gestão e Orçamento (Office of Management Budgets, OMB) define que as agências devem "utilizar o FedRAMP ao conduzir avaliações de risco, autorizações de segurança e ao conceder ATOs (Agency Authority to Operate) para agências a toda utilização de serviços em nuvem em qualquer departamento executivo ou por agências" (Memorando de política do FedRAMP, OMB). Um dos principais benefícios do FedRAMP é que ele permite às agências federais economizar significativamente tempo, custos e recursos ao avaliar a segurança dos provedores de nuvem. Informações adicionais sobre o FedRAMP, incluindo o Concept of Operations (CONOPS – Conceito de operações) do FedRAMP e o Guia de entendimento do FedRAMP, podem ser encontradas em http://www.fedramp.gov.

A AWS é um CSP em conformidade com o FedRAMP: http://aws.amazon.com/compliance/fedramp-faqs/. A AWS concluiu os testes executados por uma organização terceirizada de avaliação (Third Party Assessment Organization, 3PAO) credenciada pelo FedRAMP-e recebeu duas ATOs (Authority to Operate) por parte do Departamento de Saúde e Serviços Humanos dos EUA (HHS) depois de demonstrar conformidade com os requisitos do FedRAMP em nível de impacto moderado. Todas as agências do governo dos EUA podem aproveitar os pacotes de ATO para agências da AWS armazenados no repositório do FedRAMP para avaliar a AWS em relação às suas aplicações e cargas de trabalho, fornecer autorizações para usar a AWS e fazer a transição de cargas de trabalho dentro do ambiente da AWS.

A AWS também foi avaliada e aprovada como um CSP para os níveis 1-5 de impacto de segurança do Modelo de segurança de nuvem (Cloud Security Model, CSM) do Departamento de Defesa (DoD) dos EUA: http://aws.amazon.com/compliance/dod-csm-faqs/. O DoD CSM oferece uma avaliação formalizada e um processo de autorização para os CSPs obterem uma autorização provisória do DoD, que posteriormente pode ser aproveitada pelos clientes do DoD. Uma autorização provisória sob o CSM oferece uma certificação reutilizável que atesta nossa conformidade com as normas do DoD, reduzindo o tempo necessário para que um proprietário de missão do DoD avalie e autorize um dos seus sistemas para operação na AWS. A AWS atualmente está trabalhando para obter uma autorização no âmbito do recém-lançado Guia de requisitos de segurança (Security Requirements Guide, SRG) de computação em nuvem do DoD, versão 1, revisão 1 (12 de janeiro de 2015).

Informações sobre todos os recursos e produtos de segurança da AWS são encontradas na página de recursos de segurança da AWS: http://aws.amazon.com/security/security-resources/.

Relatórios de analistas

A pesquisa do Gartner (http://www.gartner.com/technology/research/cloud-computing/report/) posiciona a AWS no quadrante Líderes do novo Quadrante Mágico para infraestrutura como serviço da nuvem (maio de 2014). A infraestrutura como serviço (IaaS) em nuvem, no contexto do Quadrante Mágico, é definida como uma "oferta padronizada e altamente automatizada em que recursos de computação, complementados por recursos de armazenamento e rede, são propriedade de um provedor de serviços e oferecidos ao cliente sob demanda". A **Figura 3** mostra o Quadrante Mágico da Gartner 2014 para Infraestrutura em nuvem como serviço.

Figura 3 - Quadrante Mágico da Gartner para Infraestrutura em nuvem como serviço (maio de 2014)

Figura 4 - Quadrante Mágico da Gartner 2014 para serviços de armazenamento em nuvem pública (julho de 2014)

A pesquisa do Gartner também posiciona a AWS no quadrante Líderes do novo Quadrante Mágico para serviços de armazenamento em nuvem pública (**Figura 4** acima: http://www.gartner.com/technology/reprints.do?id=1-1WWKTQ3&ct=140709&st=sb). A Gartner define os líderes como aqueles que oferecem soluções de armazenamento inovadoras, criadas em uma plataforma protegida, com datacenters globais e credibilidade estabelecida como empresa.

O relatório da Forrester Wave: Public Cloud Platform Service Providers' Security, Q4 2014 (Segurança dos provedores de serviço de plataforma em nuvem pública, 4º trimestre de 2014) (**Figura 5** abaixo) (http://www.forrester.com/pimages/rws/reprints/document/113065/oid/1-SBOUWE) avaliou quatro das principais nuvens públicas em relação a 15 critérios-chave de segurança, detalhando as descobertas sobre a adequação de cada fornecedor em preencher os critérios e onde eles estão um em relação ao outro. A avaliação da Forrester afirma que a AWS lidera o grupo. "Além de demonstrar um amplo conjunto de recursos de segurança de datacenter, certificações e segurança de redes, a AWS teve uma avaliação excepcional em satisfação do cliente, parcerias de serviços de segurança e uma grande base instalada. A AWS liderou com o tamanho de seu desenvolvimento e também com a equipe de suporte técnico."

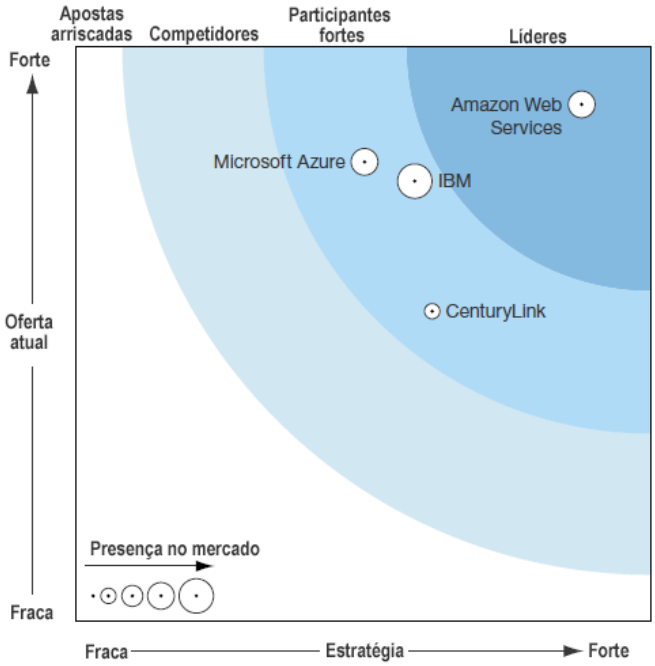

Figura 5 - Forrester Wave™: Segurança dos provedores de serviços em nuvem pública, 4º trimestre de 2014

O relatório da Forrester Wave: Enterprise Public Cloud Platforms, Q4 2014 (Plataformas corporativas de nuvem pública, 4º trimestre de 2014), de 29 de dezembro de 2014, identificou os 16 provedores de plataforma de nuvem pública mais significativos para grandes empresas. A AWS é líder em três dos quatro segmentos. Leia o relatório completo em:

http://d0.awsstatic.com/analyst-reports/The%20Forrester%20Wave%20Enterprise%20Public%20Cloud%20Platforms,%20Q4%202014.pdf

Mais relatórios de análise estão disponíveis em: http://aws.amazon.com/resources/analyst-reports/

Recursos de aquisição de nuvem

Recursos adicionais sobre aquisição de nuvem incluem:

- Webinar da AWS: How to Buy Cloud Computing Services for Your Agency: http://aws.amazon.com/webinars/buying-cloud-computing-services/
- Guia de soluções para governos estaduais e locais - Guia de melhores práticas para aquisição de soluções em nuvem e como serviço: http://www.govtech.com/library/papers/Best-Practice-Guide-for-Cloud-and-As-A-Service-Procurements.html?4