Aquisição de Serviços de Cloud no setor público

Manual - Inclusão de exemplos de linguagem do RFP para um Contrato de fornecimento de Cloud

Avisos

Este documento é fornecido apenas para fins informativos. Ele não foi desenvolvido em conformidade com as exigências legais para os processos de aquisição pública dentro de uma determinada região. Os clientes de Serviços de Cloud são responsáveis por fazer sua própria avaliação independente das informações presentes neste documento e de qualquer uso dos produtos ou serviços do fornecedor de Cloud. Este documento não cria garantias, representações, compromissos contratuais, condições ou seguros.

Os documentos e a linguagem de exemplo não devem ser considerados aconselhamento jurídico, orientação ou recomendação. Os clientes de Serviços de Cloud devem consultar os seus advogados para avaliar as suas responsabilidades perante a lei aplicável no país em que operam. O CISPE (Fornecedores de serviços de infraestrutura de Cloud da Europa) declara expressamente a sua isenção de garantias, responsabilidades ou danos associados a ou provenientes das informações presentes neste documento.

Sobre o CISPE

CISPE (*Fornecedores e serviços de infraestrutura de Cloud da Europa*, https://cispe.cloud) é um grupo independente sem fins lucrativos. Representamos fornecedores de serviços de infraestrutura de Cloud na Europa e trabalhamos com os setores e os legisladores para fornecer orientação e informação sobre os Serviços de Cloud e a função que desempenham no setor, na vida pública e na sociedade em geral.

A nossa crescente associação inclui empresas que operam em todos os países da União Europeia, com sedes globais em 16 deles. A associação está aberta às empresas, contanto que confirmem que ao menos um de seus serviços atende aos requisitos do Código de Conduta de Proteção dos Dados do CISPE. Nós:

- Defendemos os benefícios de politicas de aquisição Cloud-first dentro da União Europeia (UE) e seus estados-membro
- Promovemos requisitos de segurança e padrões técnicos coerentes em toda a União Europeia
- Sustentamos requisitos de privacidade abrangentes com um Código de Conduta
- Trabalhamos para manter o mercado de infraestrutura de Cloud da União Europeia aberto, competitivo e livre de impedimentos
- Prevenimos obrigações de monitoramento de conteúdo injustificáveis na estrutura jurídica da União Europeia

Os nossos associados fornecem e mantêm os "blocos de construção de TI" essenciais, que permitem que o governo, as autoridades públicas e as empresas construam os seus próprios sistemas e forneçam serviços importantes para bilhões de cidadãos. A cargo desta função, ajudamos a possibilitar o desenvolvimento de tecnologias e serviços de última geração que incorporam Inteligência Artificial (IA), Objetos Conectados, veículos autónomos de 5G, e a próxima geração de tecnologia de conectividade celular.

Código de conduta para serviços de infraestrutura de Cloud

O código do CISPE estabeleceu previamente a data do RGPD (Regulamento Geral de Proteção de Dados da União Europeia). Ele está alinhado com os requisitos estritos do RGPD para ajudar os fornecedores de infraestrutura de Cloud a respeitar e oferecer uma estrutura sólida com a qual os clientes consigam selecionar fornecedores de Cloud e tenham confiança em seus serviços. O Código de Conduta do CISPE declara mais de 100 serviços, oferecidos por mais de 30 empresas de Cloud sediadas em mais de 16 estados-membro da União Europeia, e é usado por milhões de utilizadores finais e clientes. https://cispe.cloud/code-of-conduct/

CISPE e o setor público

O CISPE contribui com o debate de políticas públicas europeias e trabalha para garantir um melhor conhecimento sobre a função, a contribuição e o potencial do setor de infraestrutura de Cloud da Europa.

Embora o modelo de compra pública deva condicionar o processo de adotar e usar a computação em Cloud, a aquisição de Serviços de Cloud é diferente das aquisições de tecnologia mais tradicionais que o setor público conhece. As abordagens de aquisição precisam ser repensadas: o CISPE vem incentivando os legisladores da União Europeia a desenvolver uma abordagem mais ambiciosa e prospectiva com base em iniciativas de políticas do tipo "primeiro a Cloud" (Cloud-first), o que ajuda a fomentar o crescimento do mercado de infraestrutura de Cloud única na Europa e a sustentar as metas de crescimento do Mercado Somente Digital (Digital Single Market - DSM).

Este manual tem como objetivo fornecer orientações e suporte úteis para autoridades públicas que pretendam adquirir Serviços de Cloud.

Mais informações
Membros do CISPE: https://cispe.cloud/members
Direção executiva: https://cispe.cloud/board-of-directors
Serviços de computação em Cloud declarados no Código de Conduta do CISPE: https://cispe.cloud/publicregister

Sumário

Resumo e objetivo deste Manual

Este **Manual de Aquisição de Serviços de Cloud** tem como objetivo fornecer orientações aos clientes de Cloud que pretendem comprar Serviços de Cloud por meio de um processo de aquisição competitivo (**Solicitação de Proposta para Serviços de Cloud - RFP**), mas que não têm conhecimentos para elaborar um Contrato Quadro de Cloud.

Este documento é fornecido apenas para fins informativos. Ele não foi desenvolvido em conformidade com as exigências legais para os processos de aquisição pública dentro de um determinado país ou região.

O manual também conta com uma linguagem adicional de critérios de seleção para **Planos de fornecimento programado (call-offs)** ou **Miniconcorrências** na aquisição de um Contrato Quadro de Cloud. As seções do manual são organizadas como um RFP de TI genérico. A linguagem genérica de exemplos do RFP e dos critérios de seleção é acompanhada por comentários com o intuito de explicar melhor por que um RFP de Cloud é diferente de um RFP de TI tradicional.

> ***'Serviços de Cloud'*** *é um termo que se refere a todas as tecnologias de Cloud e serviços relacionados que o utilizador final pode precisar aceder. Ele inclui a necessidade de serviços de consultoria ou profissionais/geridos para auxiliar e executar a migração para a Cloud e sustentar as cargas de trabalho na Cloud, além da própria infraestrutura de Cloud, e serviços de marketplace de Cloud, como produtos de Software como Serviço (SaaS).*

A necessidade emergente da computação em Cloud como escolha padrão para as TI do setor público demonstra uma oportunidade de modernizar as estratégias de aquisição existentes. Os processos de aquisição centralizados na Cloud podem possibilitar que as entidades do setor público extraiam todos os benefícios da Cloud, como o acesso a inovação, mais velocidade e agilidade, melhor governação, maior conformidade e segurança, além de mais eficiência e economia de custos.

Os métodos tradicionais de aquisição de TI para a compra de *hardware, software e data centers* não refletem a aquisição de Serviços de Cloud. As abordagens com relação a preços, governação de contratos, termos e condições, segurança, requisitos técnicos, SLAs e tudo o resto mudam em um modelo de Cloud, daí que usar os métodos existentes de aquisição acaba reduzindo ou eliminando os benefícios que a Cloud oferece.

Um dos melhores meios da aquisição eficiente de Serviços de Cloud para o setor público é um **Contrato Quadro de Cloud** – um programa multiorganizacional com diversas opções, por onde compradores qualificados, afiliados à organização compradora, podem adquirir as tecnologias de Cloud e os serviços associados que atendem às suas necessidades. Como um veículo de contratos de Cloud, esses contratos quadro viabilizam a aquisição de Serviços de Cloud de maneira eficiente. Assim, tanto as organizações compradoras como as entidades de utilizadiores finais têm acesso a uma ampla escolha de Serviços de Cloud e aproveitam todos os benefícios que ela oferece: agilidade, economia de escala massiva, escalabilidade para atingir melhor disponibilidade por um custo menor, gama de funcionalidades, ritmo de inovação e capacidade para endereçar novas geografias.

Note-se que **este documento tem como foco a compra de tecnologias de Cloud de Infraestrutura como Serviço (IaaS) e Plataforma como Serviço (PaaS), conforme fornecido por um *Fornecedor de Serviço de***

Infraestrutura de Cloud (CISP). Essas tecnologias de Cloud podem ser compradas diretamente de um CISP ou Revendedor do CISP. *Outras considerações de RFP são necessárias para distribuidores de serviços de marketplace de Cloud (PaaS e SaaS) e serviços de consultoria de Cloud.*

Além disso, este artigo não cobre todos os aspectos da criação de uma estrutura de aquisição de Cloud completa. Há outros documentos do setor e dos analistas que abrangem questões como práticas recomendadas de aquisição de Cloud, como fazer o orçamento de um serviço em Cloud, governação da Cloud, etc. Recomendamos que essas orientações e documentos sejam levados em consideração durante o desenvolvimento de uma estratégia geral de aquisição de Cloud.

A **Tabela 1** abaixo descreve o Manual de RFP de Serviços de Cloud e onde a linguagem do RFP de exemplo aparece para cada componente de um RFP de Serviços de Cloud.

Tabela 1 – Resumo das seções do Manual de RFP de Serviços de Cloud

Seção	Visão geral e linguagem de amostra do RFP
1.0 Visão geral de um Contrato Quadro de	Uma visão detalhada do modelo de contrato Quadro de Cloud (Lotes, como concorrer, e contratação)
2.0 Visão geral de um RFP para	Linguagem genérica de exemplo do RFP que abrange as seções abaixo, com comentários que explicam a lógica por detrás da estrutura de RFP dos Serviços de Cloud e a linguagem usada.
2.1 Disposição do RFP para	2.1.1 Introdução e objetivos estratégicos 2.1.2 Cronograma de resposta 2.1.3 Definições 2.1.4 Descrição detalhada do modelo de compra e concorrência dentro do Contrato Quadro 2.1.5 Requisitos mínimos do licitante - Administrativos
2.2 Técnico	2.2.1 Requisitos mínimos 2.2.2 Comparação entre fornecedores 2.2.3 Contratação
2.3 Segurança	2.3.1 Requisitos mínimos 2.3.2. Comparação entre fornecedores 2.3.3 Contratação
2.4 Definição de preço	2.4.1 Requisitos mínimos 2.4.2 Comparação entre fornecedores
2.5 Configuração de execução do contrato/Termos e condições	2.5.1 Termos e condições 2.5.2 Como fazer a seleção entre outorgados por projeto 2.5.3 Entrada e saída
3.0 Melhores práticas/lições aprendidas	3.1 Governação da Cloud 3.2 Orçamento para 3.3 Sobre o modelo empresarial do parceiro **Error! Reference source not found. Error! Reference source not found.** 3.5 Fornecimento antes do RFP/pesquisa de mercado

Seção	Visão geral e linguagem de amostra do RFP
Apêndice A - Requisitos técnicos de comparação entre os licitantes	Uma lista de requisitos genéricos de tecnologia de Cloud para planos de fornecimento programado (call off)ou mini concorrências
Apêndice B - Demo	Script exemplo de um produto de tecnologia em Cloud que demonstra a pontuação (demonstrações de Cloud como parte de um plano de fornecimento programado ou mini concorrência)

1.0 Visão geral de um Contrato Quadro de Cloud

Um contrato Quadro de Cloud bem formulado pode permitir a aquisição de Serviços de Cloud de forma que beneficie tanto as organizações do setor público como os fornecedores de Cloud participantes. Entre os benefícios de um contrato Quadro de Cloud bem formulado estão:

- Cooperativo por natureza:
    - Diversas organizações que se unem para inserir pedidos de requisitos semelhantes significam conveniência, eficiência, redução de custos e um processo de pedidos simplificado. Isso estabelece uma forma eficaz de agregar a procura que diversas organizações do setor público têm de tecnologias de Cloud comuns e Serviços de Cloud associados, como soluções de marketplace e consultoria.
- Linha completa de Serviços de Cloud:
    - Pode incluir no âmbito todos os serviços de consultoria/profissionais/geridos necessários para auxiliar e executar totalmente a migração para a Cloud e cargas de trabalho, além de tecnologias de Cloud e serviços de marketplace fornecidos pelo CISP.
    - As tecnologias de Cloud podem ser compradas diretamente de um CISP ou através de um revendedor atribuído.
- Governação do contrato:
    - Alinha organizações/compradores diferentes em um conjunto comum de termos e condições e uma única adjudicação de contrato principal, em vez de termos e contratos diferentes para cada organização.
    - Também é benéfico para os fornecedores, pois proporciona um processo de aquisição padrão, termos e condições e um mecanismo de pedido para navegar, em vez de termos e mecanismos diferentes para cada organização do setor público.
    - Oferece flexibilidade. Criar, aprovar e executar um contrato de Cloud eficiente dentro de políticas/regulamentações governamentais exige experimentação e capacidade de ajustar-se rapidamente. É muito mais vantajoso criar um contrato Quadro que possibilite ao setor público e aos fornecedores de Cloud trabalhar em equipe para aprimorar o contrato - de forma geral, mecânica e eficiente. Um contrato de vários anos que não funciona e não pode ser ajustado gera uma experiência negativa para utilizadores finais do setor público, organizações de aquisição e fornecedores de Cloud.

- Escolha:
    - Permite que os compradores escolham entre diversos CISPs qualificados e define um elevado padrão para todos os Serviços de Cloud e serviços associados, como marketplace de PaaS/SaaS e consultoria de Cloud.
    - Permite o controle sobre a quantidade de fornecedores no acordo pela garantia de que o padrão de cada outorgado seja adequadamente aprovado.

Um contrato Quadro para comprar Serviços de Cloud funciona melhor quando inclui tecnologias cerne de IaaS/PaaS fornecidas pelos CISP, e serviços de consultoria que os utilizadores finais do setor público possam aceder, quando necessário, para conseguirem planear, migrar, utilizar e manter uma carga de trabalho em execução na Cloud. Portanto, sugerimos que um RFP de Serviços de Cloud que elabore um Contrato Quadro de Cloud que seja dividido em 3 lotes, conforme disposto abaixo:

- LOTE 1 - TECNOLOGIAS DE CLOUD
  As tecnologias de Cloud podem ser compradas diretamente de um CISP ou de um revendedor CISP atribuído.

- LOTE 2 – MARKETPLACE
  Acesso a um marketplace de serviços de PaaS e SaaS.

- LOTE 3 - CONSULTORIA DE CLOUD
  Serviços de consultoria relacionados com a Cloud (formação, serviços profissionais, serviços geridos, etc.) e suporte técnico.

*Conforme observado anteriormente, este artigo tem como foco a compra de tecnologias de Cloud IaaS e PaaS (**LOTE 1**) conforme fornecidas por um CISP (compradas diretamente de um CISP ou través de um Revendedor CISP). Requisitos separados de qualificação são necessários para fornecedores nos LOTES 2 e 3 de um RFP de serviços de Cloud.*

A **Figura 1,** abaixo, exibe uma visão detalhada de como um RFP de Serviços de Cloud bem-estruturado e de alto nível, dividido nesses três lotes, pode levar a um Contrato Quadro de Cloud que ofereça às entidades do setor público agilidade (tanto técnica quanto contratual), visibilidade e controle de despesas e uso da Cloud, além da capacidade de ter todos os Serviços de Cloud necessários para desenvolver e manter as soluções de que elas precisam.

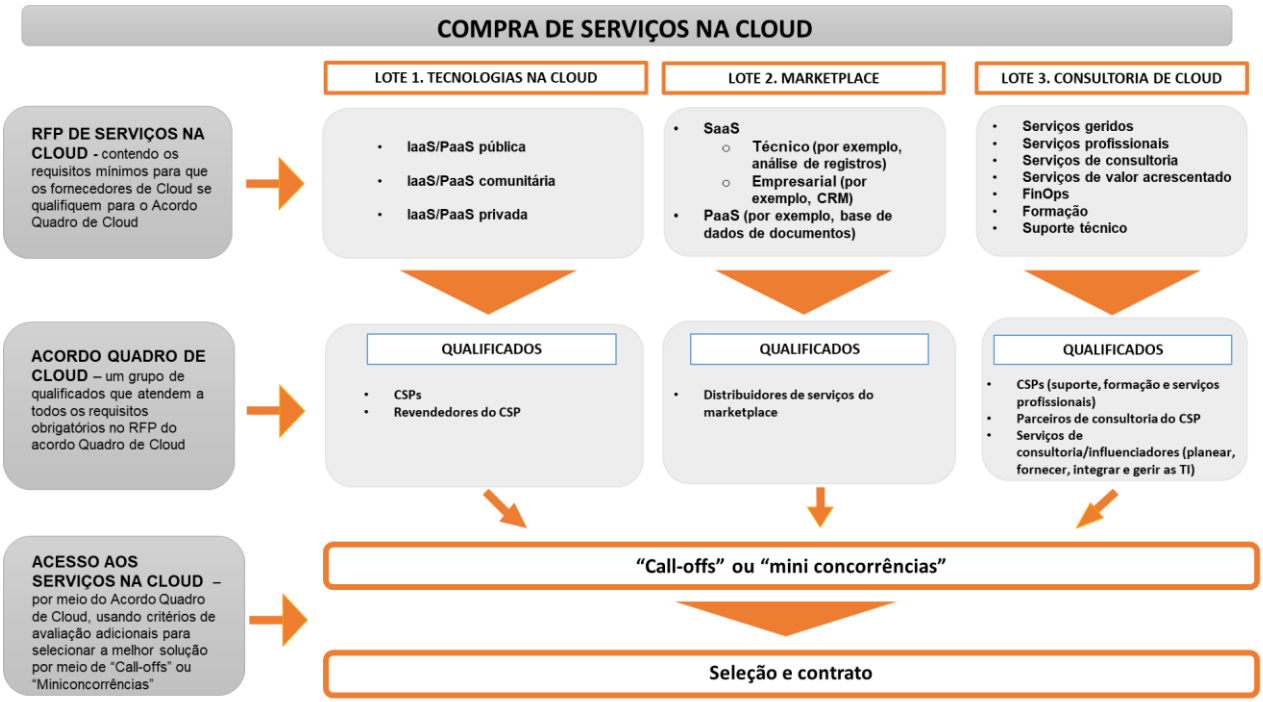

Figura 1 – Um RFP de serviços de Cloud bem elaborado será separado em 3 lotesServiços de Cloud. Cada lote contém Categorias ou "tipos de ofertas" para que a adequação técnica e contratual atenda aos requisitos do utilizador final durante a compra com Contrato de Estrutura de Cloud.

Observe o seguinte:

- Cada lote apresenta várias outorga (Awards).
- O LOTE 3 pode ser outorgado por outro RFP, ou, possivelmente, por um contrato existente de serviços de consultoria.

Categorias do LOTE 1

Um bom Contrato Quadro de Cloud solicita que os CISPs descrevam o modelo de Cloud que oferecem, separado por Categorias abaixo de cada lote. Recomendamos o uso do padrão industrial de computação em Cloud (as Características Básicas de Cloud do NIST (National Institute of Standards and Technology)) – para as definições de Cloud **Pública**, Cloud **Comunitária** e Cloud **Privada**. Estruturar um contrato de Cloud dessa forma possibilita à agência compradora e às entidades públicas usar a estrutura para escolher entre diversos modelos que atendam às suas necessidades.

Consulte a *Seção 2.1.3 Definições* para ver a definição do NIST de cada modelo de Cloud abaixo do LOTE 1 (IaaS/PaaS público, IaaS/PaaS comunitário e IaaS/PaaS privado).

Como competir – Planos de fornecimento programado (call-offs) ou Miniconcorrências?

Os critérios de qualificação para um RFP de Serviços de Cloud devem abranger elementos importantes e standards mínimos, não devendo incluir standards do tipo "é bom ter". Adicionar outros standards acima do necessário para fornecedores que se qualificam para o acordo Quadro pode fazer com que alguns fornecedores não consigam competir, acabando por ser uma opção a menos para os compradores.

Depois do RFP e da elaboração subsequente do Contrato Quadro de Cloud, os órgãos do setor público que compõem o acordo, podem solicitar ou "programar o fornecimento" de Serviços de Cloud quando necessário. Com um contrato de fornecimento programado dentro do acordo, os compradores podem refinar os requisitos com especificações funcionais adicionais, ainda retendo os benefícios oferecidos no acordo quadro.

Se houver necessidade, é possível estabelecer uma miniconcorrência para identificar o melhor fornecedor para determinada carga de trabalho ou projeto. Miniconcorrência é quando o cliente entra na concorrência conforme o acordo quadro, convidando todos os fornecedores dentro de um lote a responder a alguns requisitos. O cliente convida todos os fornecedores em potencial de um mesmo lote a licitar e, por isso, a importância dos requisitos mínimos para os outorgados em um RFP de Serviços de Cloud, já que isso garante um alto padrão de opções dentro de cada lote.

Observe que é importante que haja **conjuntos distintos de termos e condições** *do contrato para cada um dos lotes, conforme listado na Figura 1, acima. Uma "abordagem de tamanho único" no contrato para todos os lotes gera problemas de viabilidade e compatibilidade técnicas.*

2.0 Visão geral de um RFP para serviços de Cloud

Esta seção descreve o modelo e o âmbito do RFP para serviços de Cloud, como: objetivos estratégicos, participantes, definições, cronograma e requisitos mínimos administrativos. Mais uma vez, enfatizamos que o foco deste manual é LOTE 1 - TECNOLOGIAS DE CLOUD.

2.1 Disposição do RFP para serviços de Cloud

Recomendamos enfaticamente que as entidades do setor público tenham clareza quanto aos seus objetivos e requisitos mais importantes na Introdução de um RFP para Serviços de Cloud.

2.1.1 Introdução e objetivos estratégicos

Para fins de clareza quando o assunto são os objetivos estratégicos, uma boa prática é argumentar sobre a Introdução de um RFP para serviços de Cloud; **(1)** os objetivos de negócio e os benefícios que a organização pretende conseguir com o uso da Cloud; **(2)** a estrutura do contrato: quem compra, quem opera, quem faz o orçamento, etc.; **(3)** um bom conhecimento do modelo de responsabilidade compartilhada entre o setor público e os fornecedores de Cloud, algo que está no cerne da compra e uso bem-sucedidos da Cloud, e **(4)** o tipo de relacionamento criado entre Fornecedores de Serviços de Cloud (CISPs), distribuidores de serviços de marketplace, parceiros de consultoria, agências de aquisição/contratação do governo e utilizadores finais do governo. Mencionar esses quatro pontos ajuda as organizações a desenvolver um RFP que atenda melhor às suas necessidades, além de garantir que clientes e fornecedores conheçam bem os resultados do RFP.

É propositado que o RFP de Cloud seja diferente dos RFPs de TI tradicionais. A tecnologia de Cloud não é simplesmente uma substituição igual de métodos tradicionais de computação, mas sim a introdução de uma forma totalmente nova de consumir a tecnologia. RFPs bem elaboradas para serviços de Cloud podem ajudar as entidades públicas a agir rapidamente para tirar proveito da Cloud.

De todos os aspectos de compra de Cloud que mencionamos como prática recomendada, o bom conhecimento do modelo de responsabilidade compartilhada é, possivelmente, o melhor ponto de partida. O modelo de responsabilidade compartilhada[1] é usado principalmente quando se fala de segurança e conformidade na Cloud, mas essa delimitação de responsabilidades aplica-se a todos os aspectos das tecnologias de Cloud. Um RFP de Serviços de Cloud deve ajudar a esclarecer qual é a abrangência de um CISP em um ambiente de Cloud e o que continua sendo uma responsabilidade do cliente. Por exemplo, um CISP possibilita monitorar recursos e aplicações que são executados na Cloud, ***mas*** é da responsabilidade do cliente realmente usar esses recursos, pois um CISP que opera em escala massiva não tem como fazer isso para milhões de clientes.

Além disso, clientes de Cloud devem entender como uma Rede de Parceiros do CISP ajudam os clientes a utilizar a Cloud e gerir as suas responsabilidades. Por exemplo, um Fornecedor de Serviços Geridos (Managed Services Provider - MSP) pode ajudar um cliente a configurar e usar os recursos de monitorização do CISP para atender aos seus requisitos exclusivos de conformidade e auditoria.

[1] Consulte a Seção 5 do Código de Conduta do CISPE para Fornecedores de Serviços de Infraestrutura de Cloud: https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf

Simplificando, as responsabilidades no modelo de Cloud são:

Um **CISP** fornece tecnologia de Cloud

Um **Cliente** utiliza a tecnologia de Cloud

Empresas de consultoria (se necessário) ajudam o cliente a aceder e usar a tecnologia de Cloud

> ***"Empresas de consultoria"*** *são empresas que prestam serviços de consultoria, serviços geridos/profissionais para ajudar os clientes a criar, arquitetar, desenvolver, migrar e gestionar as suas cargas de trabalho e aplicações na Cloud. Essas empresas contam com Integradores de sistemas, Consultoras estratégicas, Agências, Fornecedores de serviços geridos e Revendas de valor acrescentado.*

Pense no termo "compra" de Serviços de Cloud como comprar em uma loja de equipamentos. Nessa loja, você encontra muitos materiais e ferramentas para construir o que precisa. Pode construir um armário ou uma piscina, ou uma casa inteira, a escolha é sua. Quando compra materiais e ferramentas, a loja de equipamentos pode oferecer orientação e conhecimento, mas não vai até sua casa fazer algo para si. Então, tem algumas opções:

1. Comprar os materiais e as ferramentas por conta própria para construir sozinho.
2. Comprar os materiais e as ferramentas e contratar alguém que construa e/ou opere algo para si.
3. Contratar alguém para construir/operar algo para si e pedir que a pessoa forneça os materiais e as ferramentas como parte do serviço.

Quando uma organização tem as capacidades internas para criar e gerir o seu ambiente de Cloud e as soluções por conta própria, ela realmente só precisa de ter acesso a tecnologias e ferramentas de Cloud padronizadas do CISP (diretamente do CISP ou por um Revendedor CISP – consulte o **LOTE 1).** Os softwares SaaS e PaaS necessários precisam estar disponíveis em um marketplace de Cloud (**LOTE 2**). Se houver necessidade de mais consultoria, migração, implementação e/ou gestão, a Rede de Parceiros do CISP entra em ação (**LOTE 3**).

Linguagem de exemplo do RFP: Introdução e objetivos estratégicos

A computação em Cloud oferece às organizações do setor público um acesso rápido a diversos recursos de TI flexíveis e de baixo custo, que se pagam conforme se usam. As organizações podem oferecer o tipo e o tamanho certos de recursos necessários para estimular as suas inovadoras ideias ou operar seus departamentos de TI, eliminando a necessidade de grandes investimentos em hardware e/ou contratos de licenciamento de software de longo prazo.

*A **<ORGANIZAÇÃO>** tem um requisito de acesso a esses tipos de Tecnologias de Cloud Comercialmente Disponíveis para atender às suas necessidades organizacionais num amplo espectro de organizações afiliadas.*

*O principal objetivo deste RFP é outorgar um **<CONTRATO QUADRO>** paralelo e não exclusivo com até **<x>** fornecedores, que representam diferentes tecnologias de Cloud e serviços relacionados.*

1. ***LOTE 1**. Fornecedores de Serviços de Cloud (CISPs) ou Revendedores CISP para a compra de tecnologias de Cloud*

2. ***LOTE 2.** Fornecedores de serviços de marketplace.*

3. ***LOTE 3.** Fornecedores de serviços de Consultoria para oferecer um conhecimento adicional na migração e utilização dessas ofertas do CISP*

*Em relação ao **LOTE 1**, as organizações concorrentes (CISPs ou revendedores CISP) devem demonstrar como suas ofertas cumprem com os objetivos:*

- ***Agilidade –** Disponibilizar recursos de TI para utilizadores finais em questão de minutos em vez dos períodos tradicionais de semanas ou meses.*
- ***Inovação –** Ter acesso instantâneo às mais novas e inovadoras tecnologias no mercado.*
- ***Custo –** Trocar despesas de capital por despesas variáveis (por exemplo, CapEx para OpEx). Pagar somente pelo que consome.*
- ***Orçamento –** Exibir informações de faturação e uso em níveis granulares e resumidos, visualizando padrões nos gastos ao longo do tempo, além de prever despesas futuras.*
- ***Elasticidade –** Conseguir custos variáveis mais baixos derivados da mais alta economia de escala que a Cloud fornece.*
- ***Capacidade –** Eliminar estimativas em relação às necessidades de capacidade de infraestrutura.*
- ***Parar de depender de data centres** - Concentrar-se nas necessidades dos cidadãos, e não no esforço para acoplar, manter e alimentar servidores.*
- ***Segurança –** Formalizar a criação de contas com maior visibilidade e capacidade de auditoria de recursos e eliminar o custo de proteger ambientes e o hardware físico.*
- ***Responsabilidade partilhada -** Aliviar a carga operacional pois o CISP opera, gestiona e controla os componentes desde o sistema operativo host e a camada de virtualização até à segurança física das instalações em que os serviços operam.*
- ***Automação –** Integrar a automação na arquitetura de Cloud para aprimorar a capacidade de dimensionar com segurança, rapidez e economia.*
- ***Governação na Cloud –** (1) começar com um inventário completo de todos os ativos de TI; (2) gerir todos esses ativos de forma centralizada, e (3) criar alertas referentes ao uso/faturação/segurança/etc. – tudo isso com recursos de acompanhamento de ativos, gestão de inventário, gestão de mudanças, gestão e análise de registros, visibilidade geral e governação na Cloud.*
- ***Controle –** Ter total visibilidade de como os serviços de TI são consumidos e onde podem ser ajustados para fins de segurança, fiabilidade, desempenho e custo.*
- ***Reversibilidade –** Ferramentas de portabilidade e serviços para ajudar a migrar de e para a infraestrutura do CISP, minimizando o aprisionamento tecnológico, e respeitar os Códigos de Conduta do setor*
- ***Proteção dos dados –** Capacidade de demonstrar conformidade com o Regulamento Geral de Proteção de Dados (RGPD) por meio de um código de conduta do mercado dedicado para serviços de Infraestrutura de Cloud: o Código de Conduta de Proteção de Dados do CISPE.*

- ***Transparência –*** *Os clientes devem ter o direito de conhecer o local das infraestruturas usadas para processar e armazenar os seus dados (ao nível da área da cidade).*

2.1.2 Cronograma de resposta do RFP

Uma prática recomendada é fornecer aos concorrentes um cronograma antecipado da atividade licitatória durante a criação de um contrato Quadro de Cloud e o RFP de Serviços de Cloud associado. Quanto mais interação com o setor, melhor, pois isso ajuda a garantir um entendimento claro de todas as partes quanto aos requisitos do RFP e, consequentemente, de como todos os serviços dos fornecedores se enquadram no modelo dos Serviços de Cloud.

Observe que o cronograma do RFP está sujeito à legislação e às obrigações jurídicas locais, e a lista abaixo serve como um guia de práticas recomendadas em comparação com uma lista prescritiva de atividades e cronogramas.

Linguagem de exemplo do RFP: Cronograma de resposta

Veja o cronograma do RFP abaixo referente ao RFP de Serviços de Cloud:

Cronograma do RFP para Serviços de Cloud
• *Emissão da solicitação de informações (RFI):* • *Resposta do RFI:* • *Emissão do rascunho de uma solicitação de proposta (RFP):* • *Prazo do rascunho da resposta do RFP:* • *Fase de consulta ao mercado: <timelines>* • *Emissão do RFP pré-qualificação:* • *Resposta do RFP pré-qualificação:* • *Emissão do RFP:* • *Prazo para perguntas da Ronda 1:* • *Respostas da Ronda1:* • *Prazo para perguntas da Ronda 2:* • *Respostas da Ronda 2:* • *Prazo para resposta do RFP:* • *Período de esclarecimento da proposta:* • *Período de negociação:* • *Data de intenção da outorga:* • *Outorga do contrato:* • *Duração do contrato (opções de extensão):*

Observe que o cronograma do RFP está sujeito à legislação e às obrigações jurídicas locais, e a lista abaixo serve como um guia de práticas recomendadas em comparação com uma lista prescritiva de atividades e cronogramas.

2.1.3 Definições

Um RFP de Serviços de Cloud deve incluir uma lista detalhada de definições. Esta lista inclui funções do fornecedor (por exemplo, fornecedor do serviço de Cloud, revendedor de Cloud, parceiro de Cloud), conceitos gerais de tecnologia (computação, armazenamento, IaaS/PaaS, SaaS) e outras partes importantes do contrato. Segue aqui uma amostra de lista de definições:

Linguagem de exemplo do RFP: Definições

As definições abaixo de computação em Cloud são do National Institute of Standards and Technology (NIST).[2]

- ***Infraestrutura como serviço (IaaS).*** *A capacidade oferecida ao consumidor é de provisionar processamento, armazenamento, redes e outros recursos de computação fundamentais em que o consumidor consegue implementar e executar softwares arbitrários, que podem incluir sistemas operativos e aplicações. O consumidor não gestiona nem controla a infraestrutura de Cloud subjacente, mas tem controle sobre sistemas operativos, armazenamento e aplicações implementados e, possivelmente, um controle limitado de alguns componentes de rede (por exemplo, firewalls de host).*

- ***Plataforma como um serviço (PaaS).*** *A capacidade fornecida ao consumidor é de implementar na infraestrutura de Cloud aplicações adquiridas ou criadas pelo consumidor com o uso de linguagem de programação, bibliotecas, serviços e ferramentas aceites pelo fornecedor. O consumidor não gestiona nem controla a infraestrutura de Cloud subjacente, que inclui rede, servidores, sistemas operativos ou armazenamento, mas tem controle sobre as aplicações implementadas e, possivelmente, configurações do ambiente de hospedagem da aplicação.*

- ***Software como serviço (SaaS).*** *A capacidade fornecida ao consumidor é de usar as aplicações do fornecedor executadas numa infraestrutura de Cloud. As aplicações são acessíveis por vários dispositivos clientes, tanto por uma interface thin client como um navegador da Web (por exemplo, e-mail pela Web), ou uma interface de programa. O consumidor não gestiona nem controla a infraestrutura de Cloud subjacente, que inclui rede, servidores, sistemas operativos, armazenamento ou mesmo recursos de aplicações individuais, com a possível exceção de configurações de aplicações específicas limitadas do utilizador.*

- ***Cloud pública.*** *A infraestrutura de Cloud é provisionada para o uso aberto do público em geral. Ela pode ser detida, gerida e operada por uma empresa, instituição de ensino ou organização governamental ou uma combinação delas. Ela existe no local do fornecedor de Cloud.*

- ***Cloud comunitária.*** *A infraestrutura de Cloud é provisionada para uso exclusivo de uma comunidade específica de consumidores de organizações que têm as mesmas preocupações (por exemplo, missão, requisitos de segurança, política e considerações de conformidade). Ela pode ser detida, gerida e operada por uma ou mais organizações na comunidade, um terceiro ou uma combinação deles, e pode existir local ou externamente.*

- ***Cloud híbrida.*** *A infraestrutura de Cloud é uma composição de duas ou mais infraestruturas distintas (privada, comunitária ou pública) que permanecem como entidades exclusivas, mas são enquadradas por tecnologias padronizadas ou proprietárias que possibilitam a portabilidade de dados e aplicações (por exemplo, cloud bursting para balanceamento de carga entre as Clouds).*

- ***Cloud privada.*** *A infraestrutura de Cloud é provisionada para uso exclusivo de uma única organização com diversos consumidores (por exemplo, unidades de negócios). Ela pode ser detida, gerida e operada pela organização, um terceiro ou uma combinação deles, e pode existir local ou externamente.*

[2] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

2.1.4 Descrição detalhada do modelo de compra e concorrência dentro do Contrato Quadro

Conforme mencionado anteriormente, as organizações do setor público devem identificar o modelo de como um contrato Quadro irá operar como um mecanismo de compra para tecnologias de Cloud, e os serviços relacionados de implementação e gestão. Isso deve ser esclarecido no RFP de Serviços de Cloud para que fornecedores de tecnologia de Cloud, organizações de serviços de consultoria relacionadas, distribuidores de marketplace e entidades de compra, entendam suas respectivas funções.

Quando o assunto é o âmbito do contrato Quadro, além dos planos de fornecimento programado (call-offs) e miniconcorrências subsequentes, as organizações devem levar em conta:

- Quem será responsável pela integração e serviços geridos que envolvem o uso das tecnologias de Cloud presentes no contrato.
- Existe algum requisito para que um Revendedor/Parceiro CISP forneça serviços de valor acrescentado diferentes de manter uma relação contratual com o CISP, oferecer serviços de faturação consolidados e acesso adequado e direto aos dados de uso e faturação associados à utilização dos serviços do fornecedor de Cloud?
- Existe algum requisito para um revendedor de valor acrescentado de serviço completo, integrador de sistemas ou fornecedor de serviços geridos, ou qualquer forma de serviço de mão de obra de TI?

É importante observar que o CISP não é um Integrador de Sistemas (Systems Integrator - SI) nem um Fornecedor de Serviços Geridos (Managed Services Provider - MSP). Muitos clientes do setor público exigem um CISP para seu IaaS/PaaS, depois terceirizam a consultoria e o trabalho de planeamento, migração e gestão «prática» para um SI ou um MSP. A delineação das funções e responsabilidades de um modelo de Serviços de Cloud está ilustrada abaixo, na **Figura 2.**

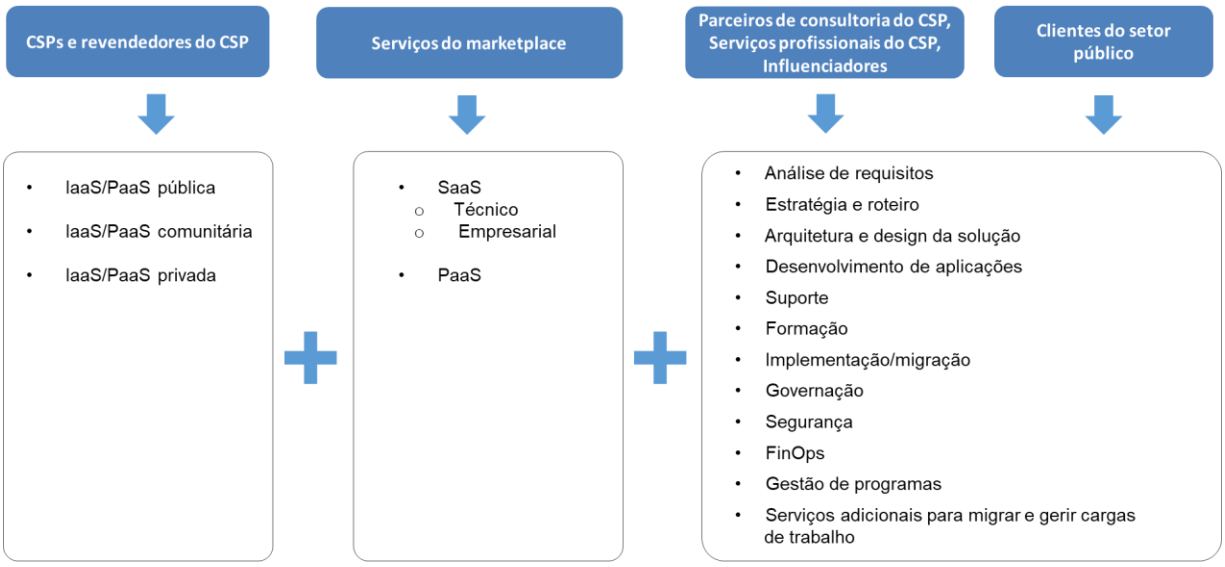

Figura 2 – Um RFP de serviços de Cloud deve fornecer aos utilizadores finais um menu contendo todos os serviços e produtos de Cloud de que eles precisam. Clientes do setor público precisam de um CISP para tecnologias de Cloud, um marketplace para produtos de PaaS e SaaS se necessário, depois o cliente pode determinar a importância da função que ele quer assumir na entrega dos serviços de Cloud e quanto pretende terceirizar para uma empresa de Consultoria/Integrador de sistemas/Fornecedor de serviços geridos/etc.

O exemplo de linguagem abaixo foi elaborado pelas funções e responsabilidades, conforme mostrado na **Figura 2**, acima. Um Contrato Quadro de Cloud, juntamente com o RFP de Serviços de Cloud, devem garantir que os compradores adquiram a capacidade de avaliar adequadamente as ofertas de cada fornecedor, com a possibilidade de optar entre os serviços necessários para a carga de trabalho/projeto. Para isso, o melhor é separar os serviços em lotes, conforme já mencionado, e esclarecer como os planos de fornecimento programado (call-offs) e as miniconcorrências são conduzidos mediante o contrato Quadro.

Exmplo de linguagem do RFP: Modelo de compra

Este contrato servirá como um modelo de compra ***Quadro****. Este Contrato Quadro inclui diversos* ***lotes*** *conforme definido pela <****ORGANIZAÇÃO>****, para Tecnologias de Cloud e serviços/produtos de marketplace relacionados, serviços de consultoria, serviço profissional/integração de sistemas/serviços geridos/serviços profissionais de migração, formação e suporte, como definido pela <****ORGANIZAÇÃO>,*** *e deve ser de uso de diversos compradores elegíveis afiliados à <****ORGANIZAÇÃO****>. Isso simplificará o processo de aquisição e também otimizará economias de escala.*

Uma vez estabelecido, esse contrato Quadro permite que uma organização compre as tecnologias de Cloud específicas e os Serviços de Cloud relacionados que desejam e quando precisarem, ao contrário da compra por aquisições individuais. Essa abordagem reduz os requisitos administrativos e diminui consideravelmente a complexidade da aquisição e o tempo do ciclo de compra.

A duração do Contrato Qudro será de, no máximo, ***<X>*** *anos, incluindo as renovações. O período máximo de um contrato de fornecimento programado (call-offs) de Quadro é geralmente* ***<x>*** *meses; esse período pode ser estendido por* ***<x>*** *meses, depois mais* ***<x>*** *meses, com as aprovações internas apropriadas, se necessário para uma extensão de contrato. Isso será especificado conforme o* ***Plano de fornecimento programado.***

A ESTRUTURA está dividida em ***três (3) lotes****.*

1. *LOTE 1: TECNOLOGIAS DE CLOUD - âmbito completo das tecnologias do fornecedor de Cloud (direto do CISP, do Revendedor ou do Revendedor com serviços/suporte de valor acrescentado):*
    i. ***Serviços de IaaS e PaaS*** *– um menu de tecnologias de Cloud, como computação, armazenamento, rede, base de dados, análises, serviços aplicacionais, implementação, gestão, programação, Internet das Coisas (IoT), etc.). Inclui pacotes de soluções de tecnologia de Cloud, como DR/COOP, Arquivo, Big Data & Analytics, DevOps, etc.*
2. *LOTE 2: MARKETPLACE – âmbito completo de serviços/produtos de PaaS e SaaS, como Contabilidade, CRM, Design, RH, GIS e Mapeamento, HPC, BI, Gestão de conteúdo, análise de registros, etc.*
3. *LOTE 3: CONSULTORIA DE CLOUD – âmbito total dos serviços de consultoria (serviços geridos, serviços profissionais, serviços de consultoria, serviços de valor acrescentado, FinOps, suporte técnico) relacionados com a migração e uso da Cloud. Esses serviços podem incluir: Planeamento, Design, Migração, Gestão, Suporte, QA, Segurança, Formação, etc.*

Os fornecedores podem enviar as suas ofertas para diversos lotes.

Os fornecedores enviarão as suas ofertas e preços relacionados no formato de sua preferência.

CONCORRÊNCIA DENTRO DO QUADRO E OUTORGA DE CONTRATOS

PLANOS DE FORNECIMENTO PROGRAMADO (CALL-OFFS)

Órgãos do setor público que fazem parte do contrato Quadro podem solicitar ou "programar o fornecimento" de serviços necessários quando precisam. Com um contrato Quadro de fornecimento programado, os compradores podem refinar os requisitos com especificações funcionais adicionais, ainda retendo os benefícios oferecidos no contrato Quadro.

Os contratos outorgados por meio do contrato Quadro conseguirão demonstrar um registo de auditoria claro em termos dos requisitos usados para selecionar o fornecedor dentro de cada lote. Compradores finais manterão os registros das comunicações com fornecedores, incluindo qualquer interação antecipada com o mercado, perguntas de esclarecimento, e-mails e conversas presenciais que tenham existido.

1. REDIGIR REQUISITOS DE FORNECIMENTO PROGRAMADO E BUSCAR APROVAÇÃO INTERNA PARA COMPRAR

Todos os compradores finais elegíveis para usar o Contrato Quadro criarão equipes conjuntas de utilizadores finais do negócio, especialistas em compras e especialistas técnicos para preparar uma lista de "itens essenciais" e "itens desejados". Esses requisitos ajudarão a decidir quais lotes que são aplicáveis e qual fornecedor está mais bem qualificado para atender aos requisitos. Ao elaborarem os requisitos, os compradores deverão considerar o seguinte:

- *fundos disponíveis para usar o serviço*
- *requisitos técnicos e de aquisição do projeto*
- *critérios em que a escolha será baseada*

2. PROCURAR SERVIÇOS

Os compradores presentes no Contrato Quadro usarão um Catálogo Quadro on-line (portal em que os Outorgados Qualificados do Contrato Quadro e seus serviços estarão listados) para encontrar produtos/serviços que atendam às suas necessidades identificadas. Eles escolherão os lotes apropriados, depois procurarão os serviços.

3. CONFERIR E AVALIAR OS SERVIÇOS

Os compradores presentes no Contrato Quadro deverão conferir as descrições dos serviços para localizar aqueles que atendem melhor às suas necessidades, com base nos requisitos e também no orçamento. Cada descrição de serviço incluirá:

- *Um documento da definição do serviço ou links para definições dos serviços*
- *Documento de termos e condições*
- *Documento de preços (links para preços públicos são aceitáveis com a suposição de que uma tabela de preços completa/documento de preços esteja disponível mediante solicitação)*

O preço será o custo da configuração mais comum do serviço. No entanto, o preço costuma ser baseado em volume, logo os compradores devem sempre analisar o documento de preços do fornecedor ou o preço público, para além das ferramentas da calculadora de preços, para saber o preço real do que está sendo comprado, e o valor geral fornecido ao comprador (por exemplo, serviços para otimização e redução de custo resultante).

Os compradores presentes no Contrato Quadro devem pedir que os fornecedores expliquem a descrição de seu serviço, os termos e condições, os preços ou os documentos/modelo de definição de serviços. Será mantido um registro de todas as conversas com os fornecedores.

4. ESCOLHER UM SERVIÇO E OUTORGAR UM CONTRATO

Fornecedor individual

Se apenas um fornecedor atender aos requisitos, o contrato poderá ser outorgado a ele.

Diversos fornecedores

Se houver vários serviços em uma lista, o comprador escolherá aquele com a MEAT (Most Economically Advantageous Tender, proposta economicamente mais vantajosa). Veja na tabela a seguir os critérios para a avaliação com base na MEAT. Os compradores podem decidir quais características detalhadas a usar e como ponderá-las.

Observe que o comprador pode precisar:

- *analisar combinações de diferentes fornecedores*
- *obter informações específicas sobre descontos por volume ou empresariais e serviços de otimização de custo do fornecedor*

A avaliação de fornecedores deve ser sempre justa e transparente. A escolha será baseada no melhor enquadramento, e os fornecedores/serviços não serão excluídos sem que os requisitos do projeto sejam consultados novamente.

Tabela 2 - Avaliação com base na MEAT

Critérios da outorga
Custo por todo o período: *eficiência de custo, preço e custos operacionais*
Mérito técnico e adequação funcional: *cobertura, capacidade da rede e desempenho, conforme especificado nos níveis de serviço relevantes*
Gestão de serviços pós-venda: *suporte técnico, documentação, função da gestão de contas e garantia de fornecimento de uma linha de serviços*
Características não funcionais

MINICONCORRÊNCIAS

Se houver necessidade, é possível estabelecer uma miniconcorrência para identificar o melhor fornecedor para determinada a carga de trabalho ou projeto. Miniconcorrência é quando o cliente entra na concorrência conforme o contrato Quadro, convidando todos os fornecedores dentro de um lote a responder a alguns requisitos. O cliente convidará todos os fornecedores potenciais dentro do lote para licitar. Consulte as informações comparativas adicionais nas seções abaixo a respeito de questões técnicas, segurança e preço/valor.

CONTRATO

O comprador e o fornecedor assinarão uma cópia do contrato antes que o serviço seja utilizado. O período máximo de um contrato Quadro é geralmente ***<x>*** *meses; esse período pode ser estendido por* ***<x>*** *meses, depois mais* ***<x>*** *meses, com as aprovações internas apropriadas, se necessário para uma extensão de contrato.*

Uma cópia do contrato deverá ser assinada por todas as partes interessadas (comprador e fornecedor) antes que o serviço seja utilizado.

2.1.5 Requisitos mínimos do licitante - Administrativos

Uma linguagem simples e clara para definir os critérios de qualificação do contrato Quadro ajuda a garantir que não haja submissões de fornecedores tradicionais de data center ou hardware que tentam vender uma solução tradicional como "Cloud". Os participantes do RFP devem demonstrar como respondem aos requisitos administrativos mínimos do licitante, abaixo.

Novamente, note que este documento tem como foco o LOTE 1 - TECNOLOGIAS DE CLOUD. Entretanto, inserimos informações adicionais sobre o LOTE 2 - MARKETPLACE e o LOTE 3 - CONSULTORIA DE CLOUD

quando eles ajudam a fornecer contexto geral em termos de requisitos e ambito do RFP. Por exemplo, é importante incluir critérios de qualificação mínimos para um Revendedor CISP/MSP/SI/Empresa de consultoria/etc., e isso ajuda a garantir que eles sejam (1) diretamente afiliados ao CISP como revenda ou parceiro de canal, (2) certificados por um CISP para revender com acesso direto às ofertas do CISP para terceiros, e (3) certificados pelos CISPs que designam suas competências e conhecimento

Exemplo de linguagem do RFP: Requisitos mínimos do licitante – Administrativos

Este acordo Quadro outorga contratos a diversos fornecedores nas categorias a seguir. Os vendedores devem ser um CISP Comercial, revendedor third-party de um CISP, distribuidor de serviços de marketplace e/ou fornecedor de serviços para uso de um CISP (por exemplo, consultoria, serviços de migração, serviços geridos, FinOps, etc.). Identifique as funções que você está oferecendo:

LOTE 1

____ - Fornecedor direto (CISP) de serviço de Cloud pública (IaaS E PaaS)

____ - Fornecedor direto (CISP) de serviço de Cloud comunitária (IaaS E PaaS)

____ - Fornecedor direto (CISP) de serviço de Cloud privada (IaaS E PaaS)

____ - Revendedor third-party do CISP (capacidade de conceder acesso direto às ofertas de Cloud on-line dos CISPs).

- *Identifique a oferta do CISP que você consegue revender com acesso direto ao serviço: _____*
- *Entregue uma carta do CISP atestando que você é um revendedor autorizado de suas ofertas: _____*

LOTE 2

____ - Fornecedor direto de Serviços de marketplace executados em um CISP (PaaS e/ou SaaS)

____ - Distribuidor de Serviços de marketplace executados em um CISP (PaaS e/ou SaaS)

LOTE 3

____ - CISP que fornece Serviços profissionais

____ - Fornecedor de suporte técnico do CISP

____- Parceiro CISP que fornece serviços para utilizar ou operar em um CISP

____- Influencer/Consultor que fornece serviços para utilizar ou operar em um CISP

Identifique o tipo de oferta:

- *Serviços geridos de cargas de trabalho em um CISP (S/N): _____*
  - *Identifique as especialidades, se aplicável: _____*
- Serviços profissionais*: (S/N): _____*
- *Consultoria – Formação (S/N): _____*
- *Consultoria – Estratégia (S/N): _____*
- *Consultoria – Migração (S/N): _____*
- *Consultoria – Governação na Cloud (S/N): _____*
- *Consultoria – Operações financeiras (S/N): _____*

- *Consultoria – Outro (identifique): _____*

Identifique o CISP/CISPs para os quais você presta serviços: _____
Entregue uma carta do CISP que confirme a sua designação de parceiro conforme o modelo de CISPs: _____

REQUISITOS MÍNIMOS ADMINISTRATIVOS DO LOTE 1

Fornecedores de Serviços de Cloud (CISPs)
Para se qualificar como CISP, você deve demonstrar conformidade com os requisitos abaixo.

Critérios de qualificação propostos para um CISP	*Motivo*
Informações organizacionais, como nome, estrutura jurídica, registro/número DUNS, NIF, etc.	
Dimensão da empresa, posicionamento económico e financeiro[3]	*O cliente pode determinar a capacidade do CISP para executar o contrato.*
Causas de exclusão, como atividades criminais/fraudulentas etc.	
Casos de estudo/Referências de clientes (especifique o número/tipo de requisito)	*O cliente pode avaliar a experiência do CISP para entregar os serviços necessários.*
Responsabilidades sociais corporativas	*Devem ser versões publicamente acessíveis que o CISP fornece.*
Compromissos e práticas de sustentabilidade publicamente disponíveis.	*O cliente pode avaliar que o CISP se compromete a operar seus negócios da forma mais sustentável possível*
O CISP deve fornecer um registro comprovado por inovar e lançar serviços e recursos novos e úteis nos últimos cinco anos, principalmente na área de PaaS, Machine Learning e Analytics, Big Data, serviços geridos e recursos de otimização de uso da Cloud. Para fins de comprovação, podem ser usados changelogs ou feeds de atualização publicamente acessíveis.	*Demonstra que o CISP se esforça para que novos produtos cheguem rapidamente aos clientes, com agilidade na iteração e melhoria dos produtos. Isso ajuda os clientes a manterem uma infraestrutura de TI moderna sem ter de fazer investimentos de recapitalização*

Relação do revendedor/parceiro com o CISP

*A **<ORGANIZAÇÃO>** exige que o prime contractor seja diretamente afiliado ao CISP como revendedor ou parceiro de canal, certificado por um CISP para revender com acesso direto às ofertas do CISP a terceiros, com certificações dos CISPs que designem as suas habilidades e conhecimento. Isso elimina a exigência de a **<ORGANIZAÇÃO>** analisar os Termos e Serviços associados a um nível adicional de subcontratação entre o prime contractor do **Contrato Quadro** e o CISP. Esse requisito também reduz a complexidade que os níveis adicionais de revendedores geram quando a (1) **<ORGANIZAÇÃO>** realiza sua due diligence para garantir que a atribuição clara de responsabilidades referentes aos serviços seja fornecida, e a (2) **<ORGANIZAÇÃO>** realize atividades diárias que envolvam o consumo dos Serviços de Cloud*

[3] Note que um RFP de Serviços de Cloud avalia informações gerais da empresa, em oposição ao número de funcionários da empresa e da sua estrutura interna. Com a tecnologia de Cloud, não há correlação entre a garantia de desempenho do serviço e o número de funcionários. Em vez disso, os RFPs de Cloud analisam o tamanho geral da empresa para atender aos requisitos (escala adequada) e a experiência/desempenho comprovados.

2.2 Técnico

Um RFP de Serviços de Cloud deve exigir que os CISPs forneçam as tecnologias de Cloud padronizadas, necessárias para o cliente desenvolver sua solução personalizada. Conforme mencionado, essa diferença entre o que é padronizado e o que é personalizado é muito importante na abordagem do RFP de Serviços de Cloud. Os CISPs oferecem serviços padronizados a milhões de clientes, por isso as personalizações no RFP dos Serviços de Cloud têm como foco soluções e resultados a mais alto nível, em comparação com os métodos subjacentes, a infraestrutura ou o hardware usado para oferecer os Serviços de Cloud e obter resultados da solução.

2.2.1 Requisitos mínimos

As aquisições de TI tradicionais geralmente contam com requisitos corporativos desenvolvidos por meio de uma série de sessões de trabalho que documentam como a organização atualmente conduz as suas operações. Fazer com que esses requisitos estejam perfeitamente corretos é um processo difícil na melhor das circunstâncias. Quando bem-sucedidas, essas sessões de requisitos documentam o processo corporativo histórico que pode, por si só, ser desatualizado e ineficiente. Se esses requisitos então fizerem parte do RFP a ser replicado pelo CISP, a única solução poderá ser uma solução feita à medida. Este modelo é incompatível com as aquisições de Cloud.

As organizações do setor público conhecem os seus objetivos de negócio e necessidades de desempenho, mas não devem prescrever o RFP de forma a ditar o design e as funcionalidades do sistema. Em vez disso, a organização deve fazer a compra com foco em obter a solução mais adequada a atingir esses objetivos. Em vez de avaliar propostas sobre centenas ou até milhares de requisitos prescritivos, as organizações devem incluir critérios de avaliação com base em como a tecnologia e os serviços associados respondem ou mesmo superam os objetivos propostos, se atingem as suas necessidades de desempenho e a capacidade de ajustar as regras de negócio por meio da configuração.

Os RFPs de Cloud devem fazer as perguntas certas para obter as melhores soluções. Considerando que, em um modelo de Cloud, os ativos físicos não estão sendo comprados, muitos requisitos de aquisição tradicionais de data centers não serão aplicáveis. ***Reciclar perguntas sobre data centers inevitavelmente levará a respostas sobre data centers****, resultando na impossibilidade de concorrência dos CISPs ou levando a contratos mal formulados, que dificultam aos clientes do setor público extrair todas as capacidades e os benefícios da Cloud.*

Um RFP de Serviços de Cloud tem como foco os principais requisitos necessários de um CISP e Serviços de Cloud, garantindo que os fornecedores qualificados ao LOTE 1 atendam às mais elevadas exigências. Os requisitos também devem evitar ser muito prescritivos para não limitar o acesso do setor público a uma variedade de CISPs qualificados.

Exemplo de linguagem do RFP: Capacidades do fornecdor de Cloud

Veja também os requisitos mínimos administrativos do CISP referentes ao LOTE 1

Critérios de qualificação propostos para um CISP	*Motivo*
Infraestrutura	
A infraestrutura do CISP deve oferecer pelo menos 2 clusters de data centers. Cada cluster deve ser composto de, pelo menos, dois data centers conectados por ligações de baixa latência para possibilitar implementações Active-Active de alta disponibilidade e implementações de cenários DR-BC. Os data centers que contêm cada cluster devem estar fisicamente isolados e ter independência a falhas entre si.	*O CISP precisa de oferecer uma infraestrutura capaz de construir aplicações altamente disponíveis em que os pontos de falha individuais sejam evitados.*
O CISP deve fornecer regiões isoladas de forma lógica e geográfica. Os dados dos clientes não devem ser replicados fora dessas regiões pelo CISP.	*Os requisitos de residência dos dados impõem que o cliente tenha total controle sobre onde estão os seus dados localizados.*
O CISP deve ter capacidade de entregar conectividade direta, dedicada e privada entre os data centers.	*A conectividade privada é um requisito fundamental para conseguir construir uma infraestrutura híbrida e segura.*
O CISP deve fornecer mecanismos suficientes, que incluem criptografia de dados em trânsito.	*O cliente pode exigir que haja uma capacidade pela qual os dados não podem transitar descriptografados.*
Certificações mínimas do CISP	
O CISP deve ter certificação ISO 27001	*A auditoria de terceiros, a certificação e a credenciação garantem que os clientes possam comparar serviços (e, em particular, a plataforma) para avaliar qualidade, segurança e fiabilidade. É essencial atender a um mínimo de certificações.*
O CISP deve oferecer serviços certificados de GDPR sob o Código de Conduta de Proteção dos Dados do CISPE, para possibilitar que o Cliente desenvolva aplicações em conformidade com o GDPR	*O cliente deve conseguir desenvolver ou executar aplicações em conformidade com o GDPR, então oferecer serviços e ferramentas dentro dessa conformidade deve ser um pré-requisito*
O CISP deve disponibilizar relatórios auditados de terceiros, como SOC 1 e 2 (que abrangem locais e serviços usados pela CE) para garantir transparência com relação aos controles e procedimentos do CISP.	*O CISP precisa ser transparente quanto à forma como a aplicação é operada e gerida. Os relatórios SOC são instrumentais para garantir confiança e transparência*
Características do serviço	
A infraestrutura do CISP deve ser acessível por meio de interfaces programáticas (APIs) e consola de gestão da Web.	*O acesso por self-service e as interfaces programáticas são um padrão obrigatório dos fornecedores CISP para deixar de intermediar, ao máximo possível, o acesso do utilizador e o fornecedor em si.*
O CISP deve oferecer uma base dos Serviços que inclua: armazenamento de objetos, base de dados relacional gerida, base de dados não relacional gerida, load balancers geridos e escalabilidade automática (autoscaling) integrada.	*A simples oferta de máquinas virtuais não é suficiente para qualificar um fornecdor como fornecdor de Cloud. Fornecedores de Cloud devem oferecer um conjunto de serviços de PaaS e IaaS para acelerar e melhorar as aplicações dos clientes.*
O CISP deve permitir que o Cliente mude arbitrariamente a sua utilização dos serviços e a configuração, ou mova os dados dentro e fora do CISP (oferta self-service).	*O acesso por self-service aos serviços e dados é um requisito imperetrível pelo qual o cliente se torna totalmente independente.*

O CISP deve permitir a cobrança de "pagamento conforme a utilização" (pay per use) dos seus serviços.	*Com o pagamento conforme a utilização, o cliente otimiza o custo das suas cargas de trabalho, minimiza o risco e aproveita o CISP para aplicações de curta duração e PoCs.*
Segurança de dados e sistemas	
O CISP deve permitir que o Cliente tenha total controle dos dados, deve dar a ele a liberdade de escolher onde os dados serão armazenados (área urbana da cidade) e garantir que os dados não sejam movidos, a não ser pelo próprio cliente.	*O cliente deve ter controle sobre onde os dados são armazenados, como gerir o acesso ao conteúdo e o acesso do utilizador a serviços e recursos*
As características do CISP devem conceder ao Cliente total controle de suas políticas de segurança, incluindo Confidencialidade, Integridade e Disponibilidade de dados e sistemas do Cliente.	*O cliente deve poder definir e implementar seus padrões de segurança entre as suas cargas de trabalho. Confiar no fornecedor para "fazer a coisa certa" com os dados do cliente não é suficiente.*
Controle de custo	
O CISP deve ter mecanismos e ferramentas para que o cliente monitore os gastos ao longo do tempo. As ferramentas devem possibilitar a segmentação básica com base em carga de trabalho, serviço e conta.	
O CISP deve oferecer ferramentas para alertar o cliente sempre que um limite de gasto é ultrapassado.	
O CISP deve enviar cobranças detalhadas ao cliente. Deve haver a possibilidade de estruturar a cobrança de forma a discriminar o custo por carga de trabalho, ambiente e conta.	

Os CISPs também devem fornecer respostas às perguntas de requisitos técnicos abaixo.

SOLUÇÕES

O CISP deve demonstrar como será capaz de fornecer modelos pré-construídos e soluções de software que sejam hospedadas no CISP ou que se integrem nele para as seguintes soluções:

- *Armazenamento*
- *DevOps*
- *Segurança/Conformidade*
- *Big data/Analytics*
- *Aplicações empresariais*
- *Telecomunicações e redes*
- *Geoespacial*
- *IoT*
- *[Outros]*

Apresente uma visão geral de como o CISP foi usado para as seguintes cargas de trabalho:

- *Recuperação de desastres*
- *Desenvolvimento e teste*
- *Arquivo*
- *Backup e recuperação*
- *Big Data*
- *Computação de alto desempenho (HPC)*
- *Internet das coisas (IoT)*

- *Sites*
- *Computação sem servidor*
- *DevOps*
- *Entrega de conteúdos*
- *[Outros]*

2.2.2 Comparação entre fornecedores

Além dos requisitos mínimos em um RFP de Serviços de Cloud, é importante informar os critérios pelos quais as tecnologias do CISP podem ser comparadas durante uma avaliação concorrencial.

Os RFPs de Serviços de Cloud devem solicitar os recursos de Cloud de que uma organização precisa, com o conhecimento daquilo que o cliente já possui, e usar esses recursos para elaborar a solução. As funcionalidades que vão para além do padrão que um CISP pode oferecer (como soluções pré-construídas pelo CISP, ou recursos de automação) podem ser usadas para uma análise mais significativa de "opções de valor acrescentado" ou "melhor valor" num RFP de Serviços de Cloud.

O setor público geralmente exige concorrência entre licitantes usando critérios de avaliação como melhor valor, proposta economicamente mais vantajosa (MEAT) ou menor preço. Consoante as entidades do setor público planeiam esta parte do RFP de Serviços de Cloud, é importante criar uma abordagem que leve em conta os recursos exclusivos da Cloud. Por exemplo, entender que apenas comparar os itens linha a linha entre as ofertas dos fornecedores de Cloud (por exemplo, computação ou armazenamento) não é uma forma eficaz de comparar ofertas. Em vez disso, recomendamos ter como foco soluções de nível mais alto, como as que estão listadas acima, na seção *2.2.1*. As entidades do setor público podem-se concentrar em requisitos específicos da Cloud, como os que estão listados no *Apêndice A - Requisitos técnicos de comparação entre os* licitantes.

Os RFPs devem apresentar as características essenciais da Cloud, necessárias para criar a sua solução. Para isso, as organizações do setor público podem usar as Características básicas da Cloud do NIST (National Institute of Standards and Technology), além de usar relatórios de analistas de terceiros para assegurar que o CISP tenha a melhor oferta de "Cloud verdadeira", que opere em escala massiva.

Exmplo de linguagem do RFP – Comparação entre fornecedores

Os CISPs também devem fornecer as respostas a TODAS as perguntas obrigatórias no ***Apêndice A****.*

Os participantes devem ter os seguintes atributos e descrever como as suas ofertas de Serviços de Cloud respondem às cinco características básicas da computação em Cloud [4].

1) ***Self-Service sob pedido:*** *o Participante deve informar a capacidade de provisionar, de forma unilateral, recursos de computação, como o tempo de servidor e armazenamento da rede, conforme necessário, automaticamente, sem exigir interação humana com os fornecedores de serviços. O Participante deve demonstrar a capacidade da atividade de solicitação para provisionar de forma unilateral (ou seja, sem análise ou aprovação de fornecedor) os serviços. Explique como isso funciona com sua oferta ou com a oferta que você está representando.*

2) ***Acesso ubiquo à rede:*** *o Participante deve oferecer diversas opções de conectividade de rede, sendo uma delas baseada na Internet. Explique como isso funciona com sua oferta ou com a oferta que você está representando.*

[4] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

3) ***Distribuição de recursos:*** *O CISP do Participante deve fornecer recursos de computação distribuídos que atendam os diversos consumidores usando um modelo multi-tenant com diferentes recursos virtuais dinamicamente atribuídos e reatribuídos de acordo com a procura do consumidor. O utilizador consegue especificar um local em um nível mais alto de abstração (por exemplo, país, região ou local do data center). O Participante deve oferecer a possibilidade de dimensionamento desses recursos em questão de minutos ou horas após a solicitação de provisionamento. Explique como isso funciona com sua oferta ou com a oferta que você está representando.*

4) ***Elasticidade rápida:*** o CISP deve oferecer suporte aos recursos de provisionamento e desprovisionamento de recursos (escalabilidade horizontal e vertical), disponibilizando esse serviço dentro dos tempos mínimos prescritos (máximo de "x" horas) após a solicitação de provisionamento. *O Participante deve proporcionar os ajustes de cobrança resultantes dessas solicitações de provisionamento diariamente, tanto por hora como por dia.*

5) ***Serviço medido:*** *o Participante deve oferecer visibilidade quanto ao uso do serviço por meio de um painel on-line ou meios eletrônicos semelhantes.*

Além disso, o CISP deve:

- *Ser um líder reconhecido no fornecimento de Serviços de Cloud, conforme demonstrado pelo Quadrante Mágico do Gartner para IaaS*[5]
- *Providenciar relatórios de analistas de terceiros com reconhecimento do setor que demonstrem as capacidades e a fiabilidade comprovadas dos CISPs.*

Por fim, os CISPs serão comparados usando cenários que aparecem no Apêndice B.

2.2.2.1 Acordos de Nível de Serviço (SLAs)

Os CISPs fornecem SLAs comerciais padronizados para milhões de clientes e, portanto, não podem oferecer SLAs personalizados, como é o caso de um modelo de data center local. No entanto, os clientes do CISP (geralmente auxiliados por parceiros) podem arquitetar o seu uso da Cloud para aproveitar os SLAs comerciais de um CISP para suprir e superar os requisitos específicos do cliente e os SLAs exclusivos.

Os RFPs de Serviços de Cloud devem garantir que os CISPs ofereçam os recursos e as orientações necessárias para aproveitar os seus serviços e SLAs comerciais, para que os utilizadores finais individuais possam atender aos requisitos de desempenho e disponibilidade.

Exemplo de linguagem do RFP: Acordos de Nível de Serviço (SLA)

Forneça informações e links para a abordagem dos CISPs aos Acordos de Nível de Serviço (SLAs).

A ***<ORGANIZAÇÃO>*** *terá conhecimento dos SLAs do CISP e implementará cargas de trabalho e aplicações importantes de forma a que continuem operando no caso de um SLA não ser atendido.*

A ***<ORGANIZAÇÃO>*** *será responsável por manter os devidos SLAs associados a qualquer equipamento de posse da* ***<ORGANIZAÇÃO>*** *ou serviços operados pela* ***<ORGANIZAÇÃO>*** *usados com o CISP.*

O CISP deve fornecer à ***<ORGANIZAÇÃO>*** *a capacidade de ter visibilidade contínua e relatórios do seu desempenho operacional do SLA, além de práticas recomendadas documentadas para aproveitar a infraestrutura que o CISP tem de arquitetar serviços para fins de desempenho, durabilidade e fiabilidade.*

[5] https://www.gartner.com/doc/reprints?id=1-2G2O5FC&ct=150519&st=sb

2.2.3 Contratação

Os termos e condições do CISP foram criados para refletir como funciona um modelo de serviço de Cloud (ativos físicos não estão sendo comprados, e os CISPs operam em escala massiva oferecendo serviços padronizados), portanto é importante que os termos e condições do CISP sejam incorporados e utilizados ao ponto máximo praticável. Consulte a seção *2.5* abaixo para ver mais informações sobre termos e condições, e contratação.

2.2.3.1 Serviços novos e alterados

Os CISPs oferecem desempenho por meio de um serviço. Diferentemente das soluções locais tradicionais, que exigem upgrades e contratos de manutenção de serviço que têm data de validade, os fornecedores de Cloud apenas oferecem um serviço padronizado. Para que o modelo de Cloud atinja economias de escala, os upgrades e as alterações na infraestrutura subjacente são implementados para todos os utilizadores e não para utilizadores individuais, e os clientes podem, então, escolher os serviços que utilizam. O serviço é mais contínuo do que os tradicionais sistemas on-premises, e os fornecedores de Cloud estão constantemente a adicionar serviços novos e aprimorados para os clientes usarem como quiserem.

Se serviços novos ou aprimorados do CISP não puderem ser adicionados após o prazo do envio do RFP, as organizações do setor público serão limitadas à avaliação de novos serviços ou recursos aprimorados até que a próxima iteração de um Contrato Quadro seja lançada. Portanto, recomendamos que o fornecimento dos serviços descritos no Contrato Quadro seja amplo a ponto de permitir a adição de novos serviços do CISP após o prazo de envio. A legislação de aquisições da União Europeia pode restringir a introdução de novos serviços materialmente diferentes do CISP ao Contrato Quadro, mas atualizações e novas versões de serviços que não são julgadas mudanças materiais poderão ser adicionadas sem problemas de aquisição.

Exemplo de linguagem do RFP: Serviços novos e alterados

O CISP deve fornecer uma solução económica que utilize tecnologias de virtualização comprovadas e estáveis e também tecnologias inovadoras que são constantemente atualizadas. A ***<ORGANIZAÇÃO>*** *reconhece e concorda que as Tecnologias de Cloud podem ser fornecidas na base de serviço compartilhado à* ***<ORGANIZAÇÃO>*** *e outros clientes do CISP a partir de uma base de código comum e/ou Ambiente comum, e que o CISP pode, de tempos em tempos: alterar, adicionar ou excluir as funções, os recursos, o desempenho ou outras características dos Serviços de Cloud e, se essa alteração, adição ou exclusão for feita, as especificações do Serviço de Cloud serão adequadamente corrigidas.*

O âmbito desse pedido de entrega inclui todos os Serviços do CISP, existentes, novos ou aprimorados, ***DENTRO DO ÂMBITO DO QUADRO****. Os Serviços de Cloud fornecidos pelo CISP disponíveis a clientes comerciais devem ser disponibilizados à* ***<ORGANIZAÇÃO>****.*

2.2.3.2 Aprisionamento tecnológico/Reversibilidade

A tecnologia de Cloud reduz o aprisionamento tecnológico a um fornecedor, pois não há compra de ativos físicos, e os clientes podem migrar os seus dados de um fornecedor de Cloud para outro a qualquer momento.

No entanto, certo nível de dependência tecnológica a um único fornecedor é inevitável na compra de Serviços de Cloud – já que nem todas as Clouds são iguais, um CISP pode oferecer serviços e recursos que outro CISP não oferece – o que acaba reduzindo a possibilidade de usar esses serviços com outro fornecedor. Uma abordagem prudente é exigir que os CISPs ofereçam os recursos e serviços obrigatórios para sair da Cloud, com documentação de como usar esses serviços com uma "estratégia de saída" razoável

– considerando que é impossível que um CISP conheça a configuração exclusiva de uso dos serviços padronizados do cliente e, para isso, é necessário um plano de saída personalizado.

Os Códigos de Conduta do Setor para gerir "Porte de dados" e "Troca de fornecedor de Cloud" estão em desenvolvimento para cumprir com os requisitos do Artigo 6 da "Regulamentação de fluxo livre de dados pessoais" da União Europeia, e devem ser usados como ferramentas para demonstrar essa reversibilidade assim que forem publicados. Essa referência estará disponível no site do CISPE.

Exemplo de linguagem do RFP: Entrada e Saída

*A **<ORGANIZAÇÃO>** procura propostas que forneçam uma estratégia de saída razoável para evitar o aprisionamento tecnológico. A **<ORGANIZAÇÃO>** não está comprando ativos físicos, e o CISP fornecerá a capacidade de migrar as diversas cargas e de retroceder novamente. O CISP fornecerá serviços e ferramentas de portabilidade para ajudar a migrar de e para a plataforma do CISP, minimizando o aprisionamento tecnológico. A documentação detalhada de como usar as ferramentas e os serviços de portabilidade do CISP servirá de plano de saída razoável.*

*O CISP não deve ter compromissos mínimos nem contratos de longo prazo **obrigatórios**.*

*Os dados armazenados num fornecedor de serviço podem ser exportados a qualquer momento pelo cliente. O CISP deve permitir que a **<ORGANIZAÇÃO>** migre os seus dados conforme necessário, para dentro ou fora do armazenamento do CISP. O CISP também deve permitir que as imagens da máquina virtual sejam descarregadas e transferidas para um novo fornecedor de Cloud. A **<ORGANIZAÇÃO>** pode exportar suas imagens de máquina e usá-las no local ou em outro fornecedor (sujeito a restrições de licenciamento de software).*

2.3 Segurança

Segurança e conformidade são responsabilidades compartilhadas entre o CISP e os clientes de Cloud. Neste modelo, os clientes de Cloud controlam como arquitetar e proteger as suas aplicações e dados colocados na infraestrutura, enquanto que os CISPs são responsáveis por fornecer serviços numa plataforma controlada e altamente segura, e por fornecer um amplo conjunto de recursos de segurança adicionais. O nível de responsabilidade do CISP e do cliente neste modelo depende do modelo de implementação da Cloud (IaaS/PaaS/SaaS), e os clientes devem conhecer as suas responsabilidades em cada modelo.

Entender esse modelo de responsabilidade partilhada é crucial para a elaboração de um bom RFP de Serviços de Cloud. As organizações do setor público devem assegurar que conhecem de fato as responsabilidades de um CISP, as suas próprias responsabilidades e onde os parceiros de consultoria/ISVs e suas soluções se enquadram para ajudar.

2.3.1 Requisitos mínimos

Quando o assunto é segurança na Cloud, a palavra-chave é **Capacidade**. As organizações do setor público devem ficar atentas com os CISPs e exigir que eles forneçam as capacidades de segurança necessárias para garantir que os clientes cumpram com todas as responsabilidades no modelo de responsabilidade partilhada. Conforme presente na lista de requisitos representativos abaixo, o CISP é incumbido de fornecer uma capacidade padronizada que o cliente utiliza para proteger o seu ambiente de Cloud exclusivo.

- ***Forneça** firewalls de rede e **capacidades** de firewall de aplicações web para criar redes privadas e controlar o acesso a instâncias e aplicações.*
- ***Forneça opções** de conectividade que possibilitem conexões privadas ou dedicadas do seu escritório ou ambiente on-premises.*
- ***Forneça** a **capacidade** de implementar uma defesa em estratégia de profundidade e impedir ataques de DDoS.*

- ***Capacidades*** *de criptografia de dados, disponíveis em serviços de armazenamento e bases de dados.*
- ***Forneça opções*** *de gestão de chaves flexíveis, permitindo escolher se quer que o CISP gestione as chaves de criptografia ou deixe que o cliente tenha controle completo sobre as chaves.*
- ***Forneça APIs*** *para os clientes integrarem a criptografia e a proteção de dados com qualquer serviço desenvolvido ou implementado em um ambiente do CISP.*
- ***Forneça ferramentas*** *de implementação para gerir a criação e o descomissionamento de recursos do CISP de acordo com os padrões da organização.*
- ***Forneça ferramentas*** *de gestão de inventário e configuração para identificar recursos do CISP, rastrear e gerir alterações feitas nesses recursos ao longo do tempo.*
- ***Forneça ferramentas e recursos*** *que possibilitem aos clientes ver exatamente o que acontece no seu ambiente do CISP.*
- ***Permita visibilidade*** *detalhada das chamadas à APIs, incluindo quem, o que, quando e onde as chamadas foram feitas.*
- ***Forneça opções*** *e agregação de logs, simplificação de investigações e de relatórios de conformidade.*
- ***Forneça*** *capacidade de configurar notificações de alerta quando ocorrem eventos específicos ou os limites são excedidos.*
- ***Forneça capacidades*** *de definir, aplicar e gerir políticas de acesso de utilizador nos serviços do CISP.*
- ***Forneça*** *a* ***capacidade*** *de definir contas de utilizador individuais com permissões entre recursos do CISP*
- ***Forneça*** *a* ***capacidade*** *de integrar e federar, com diretórios corporativos para reduzir a sobrecarga administrativa e melhorar a experiência do utilizador final.*

Mais requisitos encontram-se no *Apêndice A - Requisitos técnicos de comparação entre os* licitantes.

As funcionalidades que vão além do padrão mínimo de segurança podem ser usadas para uma análise mais significativa de "opções de valor acrescentado" ou "melhor valor" em um RFP. E, com relação à segurança, quanto mais funcionalidades integradas ou automatizadas, melhor. Mais uma vez, consulte o *Apêndice A - Requisitos técnicos de comparação entre os* licitantes para conhecer os requisitos para comparação entre os licitantes.

As organizações do setor público devem buscar certificações de credenciamento de Cloud e avaliações para a garantia de que os controles de segurança do CISP estejam implementados. Por exemplo: pense em um CISP que foi validado e certificado por um auditor independente para confirmar o alinhamento com a norma de certificação ISO 27001. O Anexo A da ISO 27001, domínio 14, retrata os controles específicos aos quais o CISP adere conforme as exigências da ISO em relação a aquisição, desenvolvimento e manutenção do sistema. É provável que esses controles cubram a maioria, se não todos, dos controles relacionados com a aquisição, desenvolvimento e manutenção do sistema que, geralmente, seriam pedidos por uma organização num RFP relacionado com TI. Portanto, procede o fato de que uma organização apenas exija que um CISP tenha certificação ISO 27001, em vez de duplicar os esforços e listar os requisitos de controle em relação a aquisição, desenvolvimento e manutenção do sistema em um RFP de Serviços de Cloud.

Essa abordagem de usar relatórios de conformidade de terceiros pode ser aplicada a muitos controles de segurança e conformidade, como, por exemplo: GDPR, ISO, SOC, etc.

Exemplos de linguagem do RFP: Segurança

O CISP deve divulgar os seus processos de segurança não proprietários e limitações técnicas para a ***<ORGANIZAÇÃO>****, de forma que a proteção e a flexibilidade adequadas sejam obtidas entre a* ***<ORGANIZAÇÃO>*** *e o fornecedor de serviços.*

O CISP deve informar as suas funções e responsabilidades com relação à segurança e conformidade:

- *Descreva as funções e as responsabilidades do CISP e da **<ORGANIZAÇÃO>** na oferta proposta. Deixe clara a delineação das responsabilidades e descreva os serviços do CISP para ajudar a **<ORGANIZAÇÃO>** a criar e automatizar funções de segurança em seu ambiente de Cloud.*
- *Forneça respostas às especificações técnicas no **APÊNDICE A** relacionadas com os requisitos de segurança da **<ORGANIZAÇÃO>**.*

PROPRIEDADE E CONTROLE DO CONTEÚDO DA <ORGANIZAÇÃO>

*Descreva como as capacidades do CISP podem proteger a privacidade dos dados da **<ORGANIZAÇÃO>**. Inclua os controles implementados para gerir a proteção do conteúdo da **<ORGANIZAÇÃO>**. O CISP deve oferecer um forte isolamento regional, de modo a que os objetos armazenados em uma região nunca deixem a região, a menos que a **<ORGANIZAÇÃO>** os transfira explicitamente para outra região.*

- *A **<ORGANIZAÇÃO>** gere o acesso ao seu conteúdo, serviços e recursos. O CISP deve fornecer um conjunto avançado de recursos de acesso, criptografia e registro para ajudar a **<ORGANIZAÇÃO>** a ser eficaz nessa gestão. O CISP não acede nem usa conteúdo da **<ORGANIZAÇÃO>** para quaisquer fins que não sejam legalmente exigidos e para manter os serviços do CISP e fornecê-los à **<ORGANIZAÇÃO>** e seus utilizadores finais.*
- *A **<ORGANIZAÇÃO>** escolherá as regiões em que o seu conteúdo será armazenado. O CISP não moverá nem replicará o conteúdo da **<ORGANIZAÇÃO>** para fora das regiões escolhidas por ela, exceto quando legalmente obrigatório e necessário para manter os serviços do CISP e fornecê-los à **<ORGANIZAÇÃO>** e a seus utilizadores finais.*
- *A **<ORGANIZAÇÃO>** escolherá como pretende proteger seu conteúdo. O CISP deve fornecer uma criptografia sólida para o conteúdo da **<ORGANIZAÇÃO>**, seja em trânsito ou parado, e dar a opção para que a **<ORGANIZAÇÃO>** gestione as suas próprias chaves de criptografia.*
- *O CISP tem um programa de garantia de segurança que utiliza as melhores práticas globais de privacidade e proteção de dados para ajudar a **<ORGANIZAÇÃO>** a estabelecer, operar e utilizar o ambiente de controle de segurança do CISP. Esses processos de controle e proteções de segurança são validados de forma independente por várias avaliações independentes feitas por terceiros.*

As avaliações e as certificações de credenciamento da Cloud fornecem garantias às organizações públicas de que os CISPs têm controles efetivos de segurança físicos e lógicos em vigor. Quando esses credenciamentos são utilizados nos RFPs, eles simplificam o processo de aquisição e ajudam a evitar processos duplicados e sobrecarregados ou fluxos de trabalho de aprovação que podem não ser exigidos para um ambiente de Cloud.

Os RFPs de Cloud devem fornecer aos CISPs a oportunidade de provar que eles se alinham com os credenciamentos e avaliações de conformidade. Conforme mencionado, existe uma sobreposição considerável nos cenários de risco e práticas de gestão de riscos entre os esquemas de credenciamento, e, como controles e requisitos vão juntos nesses credenciamentos, exigir que os CISPs os obedeçam é a forma mais rápida de gerar conformidade num RFP, em vez de duplicar o trabalho de listar esses controles individuais (muitos dos quais extraídos de RFPs anteriores que estão diretamente em data centers locais e, portanto, podem não se aplicar à computação em Cloud).

OBSERVAÇÃO: também é muito importante entender como os relatórios listados abaixo podem ser acedidos. Por exemplo, os relatórios SOC 1 e SOC 2 costumam ser documentos sigilosos. Conheça os requisitos para acedê-los (por exemplo, a assinatura de um acordo de não divulgação – NDA) e não peça simplesmente que esses documentos sejam enviados como parte da resposta do RFP (esses documentos

poderiam ser publicados pelas leis de Open Records ou legislação semelhante o que poderia comprometer a segurança na Cloud).

Exemplo de linguagem do RFP: Conformidade

O uso de padrões reconhecidos de segurança, conformidade e operações, derivado das práticas recomendadas nas operações dos Serviços de Cloud — incluindo manipulação de dados, segurança dos dados, confidencialidade, disponibilidade, etc. — simplificam a aquisição da tecnologia de Cloud.

A <ORGANIZAÇÃO> avaliará as ofertas de propostas exclusivas com relação aos padrões aceites de segurança, conformidade e operação, conforme descrito abaixo e no Apêndice A. Quando confia na certificação de conformidade do fornecedor em relação a cada padrão, a <ORGANIZAÇÃO> pode usar a conformidade mínima com o padrão como linha de base de avaliação da proposta.

Exigir que o CISP mantenha a conformidade com o padrão mínimo durante a vigência do contrato é um benefício para manter a conformidade do serviço atualizada.

O CISP que está em licitação (diretamente ou por revendedor) deve ter a capacidade de demonstrar sua capacidade de atender às seguintes declarações, relatórios e certificações independentes de terceiros (Observação: se algumas dessas declarações, relatórios e certificações estiverem sob restrições de divulgação por questões de riscos de segurança, a <Organização> trabalhará com o CISP para obter um consenso conjunto sobre o acesso):

Certificações/Declarações	Leis, regulamentos e privacidade	Alinhamentos/Estruturas
☐ C5 (Alemanha)		☐ CDSA
☐ Código de Conduta de Proteção de Dados do CISPE (GDPR)		
☐ DIACAP	☐ Diretiva de Proteção de Dados da UE	☐ CIS
☐ DoD SRG Níveis 2 e 4	☐ Cláusulas Modelo da UE	☐ Criminal Justice Info. Service (CJIS)
☐ HDS (França, Saúde)		
☐ FedRAMP	☐ FERPA	☐ CSA
☐ FIPS 140-2	☐ GDPR	☐ Privacy Shield entre UE e EUA
☐ ISO 9001	☐ GLBA	☐ EU Safe Harbor
☐ ISO 27001	☐ HIPAA	☐ FISC
☐ ISO 27017	☐ HITECH	☐ FISMA
☐ ISO 27018	☐ IRS 1075	☐ G-Cloud (Reino Unido)
☐ IRAP [Austrália]	☐ ITAR	☐ GxP (FDA CFR 21 Parte 11)
☐ MTCS Nível 3 [Cingapura]	☐ PDPA – 2010 [Malásia]	☐ ICREA
☐ PCI DSS, nível 1	☐ PDPA – 2012 [Cingapura]	☐ IT-Grundschutz [Alemanha]
☐ Regra 17-a-4 (f) da SEC	☐ PIPEDA [Canadá]	☐ MARS – E

☐ *SecNumCloud (França)*		
☐ *SOC1 / ISAE 3402*	☐ *Lei da Privacidade [Austrália]*	☐ *MITA 3.0*
☐ *SOC2 / SOC3*	☐ *Lei da Privacidade [Nova Zelândia]*	☐ *MPAA*
	☐ *Autorização da DPA da Espanha*	☐ *NIST*
	☐ *Reino Unido DPA - 1988*	☐ *Níveis do Uptime Institute*
	☐ *VPAT/Seção 508*	☐ *Princípios de segurança em Cloud do Reino Unido*

A lista acima serve apenas para fins ilustrativos e não deve ser considerada uma relação completa das certificações e padrões que se podem aplicar aos Serviços de Cloud.

2.3.2 Comparação entre fornecedores

Assim como nos critérios técnicos nas seções acima, além dos requisitos mínimos de segurança em um RFP de Serviços de Cloud, é importante fornecer critérios pelos quais as capacidades e serviços de segurança do CISP possam ser comparados durante uma avaliação competitiva.

Consulte o *Apêndice A - Requisitos técnicos de comparação entre os* licitantes para ver uma amostra dos requisitos de segurança do CISP. Recomendamos que as capacidades abaixo sejam importantes considerações de segurança para as entidades do setor público que avaliam os CISPs:

Exemplo de linguagem do RFP: Principais considerações de segurança

- *Conhecimento do CISP sobre o modelo de responsabilidade partilhada e a documentação para ajudar os clientes a entenderem a delineação das responsabilidades da segurança dos recursos e serviços do CISP (por exemplo, no contexto de GDPR)*
- *Histórico comprovado da segurança da infraestrutura do CISP, com documentação não proprietária publicada do posicionamento de segurança e controles físicos/lógicos do CISP*
- *Suporte do CISP específico à segurança na Cloud*
- *Serviços que possibilitem aos clientes formalizar o design da conta, automatizar os controles de governação e segurança e simplificar a auditoria.*
- *A capacidade de criar, provisionar e gerir um conjunto de recursos como em um modelo (inclui modelos de segurança padrão-ouro do CISP/Parceiro do CISP)*
- *A capacidade de estabelecer operações de controles confiáveis e repetíveis*
- *Recursos para auditoria contínua e em tempo real*
- *A capacidade de elaborar o script técnico de políticas de governação na Cloud*
- *A capacidade de criar funções obrigatórias que não podem ser ignoradas pelos utilizadores que não têm permissão para alterar essas funções.*
- *A capacidade de executar a implementação confiável do que foi anteriormente escrito em políticas, padrões e regulamentos, além de criar segurança e conformidade aplicáveis, o que, por sua vez, cria um modelo de governação confiável para ambientes de TI*
- *Serviços para proteger contra ataques comuns e frequentes da rede e de negação distribuída de serviço (DDoS) da camada de transporte, junto com a capacidade de gravar regras personalizadas para mitigar ataques sofisticados da camada aplicacional*
- *Serviço gerido de detecção de ameaças*

2.3.3 Contratação

Conforme observado anteriormente, os termos e condições do CISP foram criados para refletir como funciona um modelo de serviço de Cloud (ativos físicos não estão sendo comprados, e os CISPs operam em escala massiva oferecendo serviços padronizados), portanto é importante que os termos e condições do CISP sejam incorporados e utilizados ao ponto máximo praticável. Consulte a seção *2.5* abaixo para ver mais informações sobre termos e condições, e contratação.

Com relação à segurança, mais uma vez recomendamos permitir que os CISPs atualizem constantemente as suas ofertas ou que os fornecedores possam adicionar produtos após o prazo de envio, contanto que estejam de acordo com os parâmetros originais do RFP**.** Isso reflete o fato de que os recursos e serviços de segurança evoluam rapidamente, e os CISPs dispnibilizem serviços com foco em segurança geralmente, que, em muitos casos, são de uso gratuito. É importante ter um nível de segurança básico (consulte os requisitos mínimos, acima) para garantir que as alterações nas ofertas de segurança não sejam prejudiciais.

O modelo de responsabilidade partilhada é, obviamente, o centro da segurança em um RFP de Serviços de Cloud. Cada parte precisa de conhecer claramente as suas responsabilidades de segurança, e os CISPs devem ser encarregados de documentar as responsabilidades de segurança do CISP/Cliente para as tecnologias de Cloud fornecidas por eles, juntamente com a documentação que ajuda os clientes a elaborar e automatizar práticas de segurança recomendadas.

Um Contrato de Estrutura de Cloud deve fornecer flexibilidade para remover um fornecedor no caso de ele deixar de cumprir os requisitos mínimos de segurança e conformidade, conforme previsto no RFP de Serviços de Segurança.

2.4 Definição de preço

Para contratar a tecnologia de Cloud de forma que a procura flutuante seja considerada, as organizações do setor público precisam de um contrato que lhes permita pagar pelos serviços conforme são utilizados, com a governação e a visibilidade da Cloud exigidas com relação a uso e despesas.

É importante que que os RFPs dos Serviços de Cloud analisem o valor e o custo total de propriedade (TCO), em comparação com a simples comparação de preços unitários. Essa prática tradicional de analisar o menor preço unitário não reflete o modelo de Cloud, por isso não tende a gerar a proposta mais vantajosa economicamente, ou o menor preço total.

Para auxiliar na avaliação de definição de preços do CISP, é útil primeiro ter a pré-qualificação ou lista de preferências do CISP, com os ***requisitos mínimos relacionados à definição de preços*** *para que os CISPs com menos capacidades possam ser eleitos no contrato Quadro. O processo de avaliação para fornecimento programado (call-offs) e miniconcorrências pode então destinar-se a uma seleção de arquiteturas típicas de Cloud de exemplo e* ***cenários de preços*** *correspondentes a algumas cargas de trabalho comuns do setor público, depois deixar que os CISPs os precifiquem. Demonstrações de testes ao vivo também são recomendadas para possibilitar a comparação de desempenho e elasticidade dos serviços de tecnologias de Cloud fornecidos pelos CISPs. Consulte o Apêndice B para ver um exemplo de demonstração de script de teste para tecnologias de Cloud.*

2.4.1 Requisitos mínimos

A seção de definição de preços em um RFP de Serviços de Cloud é composta de quatro elementos principais:

1. **Definição de preço do utilitário:** clientes de Cloud estão incorporando o modelo de utilitário de pagar conforme a utilização, pelo qual, ao final de cada mês, eles pagam apenas pelo que usaram, o que é excelente para as métricas de utilização e recursos.
2. **Definição de preços transparente:** a definição de preços do CISP deve ser publicamente disponível e transparente.
3. **Definição de preços dinâmica:** inclui a flexibilidade de permitir que os preços da Cloud oscilem com base nos preços do mercado. Essa abordagem leva a vantagem da natureza dinâmica e competitiva da definição de preços da Cloud, para além de ajudar na inovação e nas reduções de preços.
4. **Controle de gastos:** os CISPs devem fornecer ferramentas de geração de relatórios, monitoramento e previsão que permitam aos clientes (1) monitorar o uso e o gasto em níveis granulares e resumidos, (2) receber alertas de quando o uso e o gasto atingem os limites personalizados e (3) estimar o uso e o gasto para planear futuros orçamentos de Cloud.

Exemplo de linguagem do RFP: Definição de preço

*A **<ORGANIZAÇÃO>** solicita que os CISPs participantes incluam o seu método proposto e modelo de preços para oferecer os seus serviços aos utilizadores finais como um recurso de Cloud comercial.*

O CISP deve fornecer:

- *Um documento da definição do serviço ou links para definições dos serviços*
- *Documento de termos e condições*
- *Documento de preços (links para preços públicos são aceitáveis, com a suposição de que uma tabela de preços completa/documento de preços esteja disponível mediante solicitação)*

O preço será o custo da configuração mais comum do serviço. Os CISPs devem fornecer opções de descontos com base em volume, além das ferramentas da calculadora de preços, para saber o preço real do que está sendo comprado, e o valor geral fornecido ao comprador (por exemplo, serviços para otimização e a redução de custo resultante).

Compradores presentes no Contrato Quadro devem pedir que os fornecedores expliquem a descrição de seu serviço, os termos e condições, os preços ou os documentos/modelo de definição de serviços. Será mantido um registro de todas as conversas com os fornecedores.

Requisitos adicionais de definição de preço

- *Dê às tecnologias de Cloud um modelo de definição de preço dinâmico, que proporcione máxima flexibilidade dos negócios e possibilite escalabilidade e crescimento.*
- *Os atributos de definição de preço devem incluir o seguinte:*
  - *A definição de preço é fornecida em um serviço sob procura, estilo de utilitário ou pagamento conforme o uso? Explique seu modelo de definição de preço.*
  - *Você consegue mais descontos quando há comprometimento com a utilização e/ou compra em lote? Dê os detalhes de como fazer isso.*
  - *A definição de preços é publicamente disponível e transparente? Inclua links para a definição de preços disponível publicamente.*

- *A definição de preço é dinâmica e responde de forma rápida e eficiente à concorrência no mercado?*
- *Você oferece práticas recomendadas e recursos para rastrear os gastos?*
- *Você oferece práticas recomendadas e recursos para otimização de custos?*

Transparência na definição de preço
Em razão da constante tendência descendente de definição de preço nas tecnologias de Cloud comerciais conduzidas pela inovação e concorrência, o custo de unidade de serviço medido do CISP, pago pela ***<ORGANIZAÇÃO>,*** *conforme o Contrato Quadro, nunca deve exceder a definição de preço unitário do fornecedor de Cloud publicado no site dele, que passa a vigorar no momento em que a unidade de serviço é usada pelo cliente.*

Alertas/relatórios sobre orçamento e faturação
Para demonstrar a entrega e o uso das tecnologias de Cloud, os CISPs devem fornecer à ***<ORGANIZAÇÃO>*** *as ferramentas para gerar relatórios de faturação detalhados que discriminam os custos por hora, dia ou mês; pelas contas na organização; por produto ou recurso do produto; ou por marcas definidas pelo cliente. A* ***<ORGANIZAÇÃO>*** *reconhece que, como parte do modelo de responsabilidade partilhada da Cloud, a* ***<ORGANIZAÇÃO>*** *será responsável por usar recursos e ferramentas de orçamento e faturação fornecidos pelo CISP para atender aos requisitos exclusivos de previsão e relatório.*

- *Forneça informações sobre como a* ***<ORGANIZAÇÃO>*** *pode exibir informações de faturação e uso em níveis granulares e resumidos, visualizando padrões nos gastos com recursos do CISP ao longo do tempo, além de prever despesas futuras.*
- *Forneça informações sobre como a* ***<ORGANIZAÇÃO>*** *pode filtrar a exibição de uso/faturação por serviço, por conta vinculada ou por marcas personalizadas aplicadas aos recursos, e crie alertas de faturação que enviem notificações quando o uso dos serviços atingir ou superar os limites/orçamentos definidos pela <****ORGANIZAÇÃO****>.*
- *Forneça informações sobre como a* ***<ORGANIZAÇÃO>*** *pode prever quanto dos Serviços de Cloud ela usa durante um período previsto definido, com base no uso passado. O CISP deve oferecer uma* ***estimativa*** *de como será a faturação do CISP da* ***<ORGANIZAÇÃO>*** *e possibilitar que a* ***<ORGANIZAÇÃO>*** *use alarmes e orçamentos para valores previstos de uso, para conseguir melhor governação em relação aos custos e despesas.*

2.4.2 Comparação entre fornecedores

As organizações do setor público geralmente exigem concorrência entre licitantes usando critérios de avaliação como melhor valor, proposta economicamente mais vantajosa (MEAT) ou menor preço. No planeamento dos preços de fornecimento programado (call-offs) ou miniconcorrências da estrutura, é importante criar uma abordagem que leve em conta os recursos exclusivos da Cloud. Por exemplo, entenda que apenas comparar itens linha a linha entre ofertas de fornecedores de Cloud (como computação ou armazenamento) não é uma forma eficiente de comparação, pois não leva em conta recursos como desempenho, otimização de custos que usam serviços nativos de Cloud e ferramentas de monitorização de CISP, ou serviços diferenciados que os CISPs podem oferecer gratuitamente. Além disso, o preço de catálogo de um CISP pode ter dezenas de milhares de itens de linha, os modelos de preços diferenciam-se entre serviços e entre fornecedores.

Analisar o TCO

Recomendamos que se concentre no custo total de propriedade (TCO) dos casos de uso definidos, que leva em consideração todos os aspectos de uma solução de Cloud (incluindo serviços de parceiros, descontos padronizados do CISP, recursos técnicos que podem aumentar o desempenho e reduzir/otimizar custos, etc.).

Comparar por cenários

O processo de avaliação também pode abranger cenários comuns que correspondem a sistemas ou aplicações comuns. Esses cenários (como hospedagem na Web ou a implementação de um sistema de recursos humanos com um número x de utilizadores, etc.) podem incluir variáveis como velocidade e escala dos recursos, desempenho da aplicação ou solução, quantidade de acesso ao armazenamento, dados complexos de baixo volume em comparação com tarefas de computação simples de elevado volume, etc. As aplicações ou sistemas também podem ter cenários típicos, como processamento de elevado volume por exemplo na altura da entrega de impostos e notificações de emergência. Os cenários devem ser abrangentes a ponto de incluir o âmbito de tecnologias e serviços que o cliente pode usar durante o projeto. Dessa forma, o cliente consegue comparar o custo total estimado do projeto.

Comparar cenários de forma financeira e técnica

Também é importante levar em consideração as vantagens técnicas ao comparar preços entre ofertas do CISP. Por exemplo, um CISP pode permitir que os clientes criem uma topologia de Recuperação de desastres (DR) ativa-ativa graças ao seu modelo de data centers em clusters dentro de uma região geográfica. Um CISP que não tem esse tipo de redundância e configuração do data center pode ser x% mais caro em razão do custo de considerar as necessidades de recuperação de desastres. Como exemplo do motivo pelo qual uma abordagem holística à definição de preço que inclua recursos técnicos adicionais é crucial para avaliar os CISPs, pense na alternativa abaixo de uma comparação direta.

Exemplo: um cliente quer comparar o preço do armazenamento de objetos fornecido por CISPs qualificados em um contrato Quadro. O preço do item da "unidade" de armazenamento do CISP 1 é € 0,023/GB. O preço da mesma "unidade" do CISP 2 é € 0,01/GB. Em uma comparação simples de unidade com unidade, o cliente não faz perguntas importantes, como:

1. Quantas cópias redundantes do objeto estão disponíveis em caso de falha? No exemplo acima, o CISP 1 precisa sustentar a perda de dados simultânea em dois locais diferentes e mantém diversas cópias doas dados. No caso do CISP 2, não são feitas cópias redundantes.
2. Qual é o nível de sustentabilidade dos objetos armazenados? Do CISP 1 é 99,999999999%, e do CISP 2 é 99%.
3. Leve em conta o custo ao longo do tempo da propriedade de todo o projeto ou carga de trabalho, e como os recursos de otimização de custo podem reduzir o custo quando se trata da forma como os dados são armazenados e usados (por exemplo, aumentar o uso de funções Sem servidor de um CISP pode reduzir custos em x%).

Essas são apenas algumas das muitas outras considerações técnicas que envolvem preço, particularmente relacionadas à segurança e conformidade.

Considerações para cenários de definição de preço

Taxas básicas – são basicamente os preços públicos dos CISPs. Os CISPs precisam informar esses preços publicamente; entretanto, conforme observado acima, para comparar corretamente os CISPs, os clientes

Avaliar o conjunto abrangente de capacidades de um CISP é algo fundamental para clientes que procuram obter o melhor valor. Por exemplo, os CISPs podem ter alguns serviços gratuitos ou basicamente gratuitos, e uma avaliação de preços deve levar esses serviços em conta, enquanto outros CISPs podem cobrar pelas mesmas funcionalidades.

podem solicitar cerca de 3 a 5 cenários específicos (ou quantos ele achar necessário) para serem cotados por todos os fornecedores. Os cenários devem ser abrangentes para incluir uma gama de serviços e tecnologias que o cliente tende a usar durante o projeto. Dessa forma, o cliente consegue comparar o custo total estimado do projeto. Comparações feitas por item de linha/SKU tendem a ser mais problemáticas do que úteis para clientes e fornecedores (clientes precisam de comparar dezenas de milhares de itens de linha entre diversos CISPs, e fornecedores precisam informar esse nível de detalhamento e geri-lo quando o preço real é determinado apenas com base no uso do serviço).

Os critérios de avaliação podem ser redigidos de forma que permitam que os CISPs enfatizem os seus recursos "x padrão incluídos" e como o custo desses serviços provoca impacto de forma geral. Os critérios de avaliação também podem considerar os preços com base em volume/em camadas do CISP e os descontos disponíveis comercialmente, como Instâncias reservadas/Instâncias spot. Por exemplo:

- Economia de x% se os clientes comprarem uma capacidade de computação reservada (1 ano, 3 anos, etc.)
- Desconto de x% no preço em camada/por volume
- Economia de x% com base nas avaliações da arquitetura e na otimização da infraestrutura, como migrar para uma opção de computação mais adequada
- Conforme observado acima, leve em conta o custo por toda a duração e como os recursos de otimização de custo podem reduzir os custos

CENÁRIO DE DEFINIÇÃO DE PREÇO
Os licitantes devem informar os preços no cenário abaixo somente para fins de avaliação. O preço real será baseado na utilização dos serviços, em um modelo de pagamento conforme a utilização (pay per use).

Abaixo estão os requisitos representativos para a finalidade da definição de preço, apresentados mediante a observação de que, durante o contrato, esses requisitos nominais sofrerão alterações. Apresente os preços para capacidade conforme a utilização de 12 e 36 meses e capacidade reservada de 12 e 36 meses.

Apresente o seguinte:

- *Nome das soluções propostas:*
- *Melhor preço do licitante:*

- *Horário de atendimento: 24x7x365*
- *Disponibilidade do serviço: 99,95%*

Os cenários de definição de preço também podem incluir exemplos de clientes existentes com cargas de trabalho semelhantes, que otimizaram as suas despesas no período de 1/2/3 anos - seja usando ferramentas de monitorização e otimização do CISP, adotando soluções de Cloud nativa otimizadas e por reduções de preço do CISP.

2.5 Configuração de execução do contrato/Termos e condições

As tecnologias e as operações que o CISP oferece são padronizadas por design, portanto as condições contratuais também são padronizadas. Entretanto, existe uma possibilidade marginal de ajustar esses contratos de forma a que se adaptem aos contextos legislativos e regulatórios locais.

Geralmente, os métodos tradicionais de aquisição de TI incluem regras estritas com as quais os candidatos precisam de estar em conformidade total ou em parte para não serem rejeitados. Eles também podem incluir um subconjunto estrito de requisitos obrigatórios. Quando esse tipo de método de fornecimento é

usado com tecnologias de Cloud, que são, na verdade, um conjunto de ferramentas e componentes padronizados que ajudam a arquitetar uma solução personalizada, as aquisições tendem a falhar.

2.5.1 Termos e condições

A primeira etapa na contratação, num RFP de Serviços de Cloud, é ler e entender os termos comerciais existentes do CISP que, em muitos casos, podem ser encontrados publicamente em sites do CISP. Entidades do setor público estão cada vez mais à vontade para aceitar os termos comerciais dos CISPs. Parte dessa iniciativa de entender os termos é reunir-se com os CISPs e seus parceiros para consolidar as suas abordagens. A principal pergunta a ser feita é 'por que' os CISPs operam com termos específicos. Alguns desses termos podem parecer diferentes dos termos tradicionais de TI, mas existem motivos bem específicos "pelos quais" eles fazem parte de um contrato de Cloud. Se os termos publicamente disponíveis não forem aceitáveis, os CISPs geralmente terão contratos ligeiramente modificáveis para clientes empresariais que podem ser explorados.

Além de ler os termos e condições do CISP, é importante entender as políticas existentes, as regulamentações e/ou as leis (por exemplo, que envolvem tecnologia, classificação dos dados, privacidade, pessoas, etc.). Às vezes, existem políticas/regulamentações/leis elaboradas para a compra e a utilização de ofertas de TI tradicionais que podem confrontar com um modelo do CISP. Por exemplo, apenas permitir o uso de tecnologias de Cloud que tenham sido incluídas na licitação do Contrato Quadro pelo RFP de Serviços de Cloud. Os CISPs estão constantemente a adicionar novos serviços e recursos. Restringir o acesso a novos serviços simplesmente porque você segue uma abordagem de atualização de produtos de TI tradicional não faz sentido para o utilizador final. Se esse for o caso, é importante conversar abertamente com os CISPs que incluem a consideração dessas políticas/regulamentações e/ou leis.

Aproveitar as conversas antes do RFP:

Conforme mencionado acima, antes de elaborar um RFP, aproveite para se encontrar com os CISPs e os fornecedores relacionados para conhecer os seus termos e condições e informá-los sobre a abordagem, as políticas, as regulamentações e as leis da entidade. A parte mais importante dessas conversas é que os dois lados saibam 'por que' os termos relevantes funcionam de tal maneira. Por exemplo, os termos e condições de Serviços de Cloud são diferentes para data centers tradicionais, serviços geridos, hardware, software pacotizado e condições de integração de sistemas. Como são modelos únicos e envolvem inovação constante, os seus modelos corporativos exigem que o processo de RFP seja flexível o suficiente para possibilitar negociações ou discussões de esclarecimento.

Com a adição da possibilidade de esclarecer termos e condições nas discussões e negociações, as organizações do setor público adquirem melhor entendimento dos modelos de Cloud e evitam o problema de rejeitar fornecedores que na verdade poderiam responder às necessidades da organização. Um processo típico é a organização identificar certos termos com antecedência que queira debater e negociar antes da outorga. Ao negociar termos aceitáveis com os licitantes, a organização consegue a outorga mais adequada e resolve diferenças que poderiam resultar na rejeição de uma proposta eficiente. As entidades do setor público também podem rever as suas políticas, regulamentações e leis, e as duas partes podem entender como a utilização da Cloud se enquadra nesses modelos. Às vezes, há maneiras de trabalhar com as cláusulas existentes. No entanto, se existir uma área problemática, as duas equipas podem trabalhar para encontrar uma solução (recomenda-se abordar esse tema bem antes de um RFP e da negociação contratual subsequente).

Flexibilidade na negociação

Para assinar contratos em conformidade com a legislação local, ainda confiando nos termos contratuais padronizados do CISP, recomenda-se (1) solicitar dos candidatos o seu contrato padrão, (2) não requerer condições contratuais inadequadas ao criar o contrato Quadro para o RFP de Serviços de Cloud, e (3) fornecer uma opção de negociação sobre todas as provisões da consulta e propostas, que resultarão no contrato Quadro (exceto, obviamente, as cláusulas obrigatórias impostas pela lei).

Nota: o âmbito da responsabilidade partilhada é inerente ao modelo de Cloud e deve aparecer nos termos do contrato (por exemplo, o CISP confirma que os clientes detêm os seus dados, onde residem e fornece ferramentas para garantir que os locais dos dados sejam limitados, MAS é da responsabilidade do cliente ou parceiro usar essas ferramentas.

Note que é importante que haja ***conjuntos distintos de termos e condições*** *do contrato para cada um dos LOTEs de um Contrato Quadro de Cloud. Uma "abordagem de tamanho único" no contrato para todos os LOTEs gera problemas de viabilidade e compatibilidade técnicas.*

Conforme já observado, os RFPs que incluem termos obrigatórios não negociáveis são basicamente propostas do tipo "pegar ou largar" para os fornecedores, e podem fazer com que uma proposta que de outra forma seria aceitável seja recusada. As organizações do setor público devem considerar atentamente as consequências de usar termos obrigatórios, a menos que seja exigido por lei. As organizações devem conhecer a necessidade de um requisito obrigatório ou termo, pois futuras negociações são impedidas por sua classificação de obrigatoriedade. O uso de requisitos ou termos obrigatórios deve ser mínimo para que a organização tenha a flexibilidade necessária de adquirir a melhor tecnologia e solução.

Lembre-se de que as tecnologias de Cloud do CISP são completamente padronizadas e entregues de forma totalmente automatizada. Portanto, um CISP não consegue fazer alterações nos termos e condições que exijam qualquer personalização de serviço subjacente. Além disso, os preços dos serviços são geralmente públicos e padronizados para todos os utilizadores, o que significa que um CISP não pode ajustar os preços na tentativa de absorver mais riscos em nome de um cliente em particular.

Compras indiretas

Uma opção [alternativa] de comprar tecnologias de Cloud diretamente de um CISP é por um revendedor CISP. Encontram-se mais informações sobre os Revendedores CISP na seção *2.1.3*, acima.

Exemplo de linguagem do RFP: Termos e condições

*Os CISPs ou fornecedores representantes devem fornecer os seus termos e condições publicamente disponíveis e dar feedback sobre os principais termos e condições fornecidos pela <**ORGANIZAÇÃO**>.*

*A <**ORGANIZAÇÃO**> pretende assinar um contrato escrito com o licitante vencedor com base nos termos contratuais do licitante. O licitante deve fornecer um conjunto de termos contratuais propostos para a <**ORGANIZAÇÃO**> ler, o que representa a sua melhor proposta legal e comercial. Os ofertantes e a <ORGANIZAÇÃO> podem abordar os conjuntos de termos e condições durante a fase de <DISCUSSÃO/NEGOCIAÇÃO>.*

- *Os termos-chave de alto nível do acordo Quadro devem consistir, em grande parte, nos seguintes componentes:*
  - *Duração do acordo Quadro*

- *Governação do acordo Quadro*
- *Desempenho do acordo Quadro*
- *Terminação do acordo Quadro*
- *Âmbito do acordo Quadro*
- *Processo de Pedidos*
- *Provisões de confidencialidade*
- *IP e informações específicos da categoria*
- *Requisitos técnicos mínimos a serem atendidos pelos CISPs – por exemplo, padrões de qualidade, credenciação, segurança e proteção dos dados*

- ***Haverá termos diferentes para cada um dos lotes do Contrato Quadro***
- *Especificidades do serviço do CISP serão levadas em conta e geridas durante o plano de fornecimento programado (call-offs)*
- *Permitir alterações contratuais—os termos não devem restringir os clientes e os fornecedores a concordar com alterações contratuais, a renunciar a novos serviços ou melhorias. A natureza evolutiva dos Serviços de Cloud é tal que as melhorias do serviço serão disponibilizadas continuamente, ajudando a entregar eficiência aos clientes*
- *Os Acordos de Nível de Serviço (SLAs) não devem ser especificados pelo cliente. Os termos do cliente não devem definir SLAs específicos que diferem dos modelos de entrega de serviço padrão dos CISPs. Ao permitir SLAs padrão dos CISPs, os CISPs conseguem manter o custo baixo e passá-lo aos clientes, e os clientes ficam mais seguros de que o CISP pode manter o SLA.*
- *Limites de responsabilidade devem ser proporcionais. A responsabilidade deve ser proporcional aos serviços comprados, não devendo haver grandes responsabilidades desproporcionais. Se os limites forem desproporcionais e altos, será um desestímulo para os CISPs aceitarem projetos de baixo valor. Esses projetos geralmente aparecem como uma introdução útil e caso de "teste" para os clientes determinarem onde certas soluções de Cloud são eficientes em sua organização.*
- *Os clientes devem ter a propriedade dos seus dados. Os clientes devem controlar e reter os seus dados e ter capacidade de determinar a localização geográfica em que eles são mantidos. Isso permite que os clientes evitem o aprisionamento tecnológico e transfiram os dados para novos fornecedores livremente.*

2.5.2 Como fazer a seleção entre outorgados por projeto

Órgãos do setor público que fazem parte do acordo Quadro podem solicitar ou 'programar o fornecimento de' serviços necessários quando precisam. Com um contrato de fornecimento programado dentro do acordo, os compradores podem refinar os requisitos com especificações funcionais adicionais, ainda retendo os benefícios oferecidos no contrato Quadro.

Se houver necessidade, é possível estabelecer uma mini concorrência para identificar o melhor fornecedor para determinada carga de trabalho ou projeto. Uma mini concorrência é quando o cliente entra na concorrência conforme o Quadro, convidando todos os fornecedores dentro de um lote a responder a alguns requisitos. O cliente convida todos os fornecedores em potencial de um mesmo lote a licitar e, por isso, a importância dos requisitos mínimos para os outorgados em um RFP de Serviços de Cloud, já que isso garante um alto padrão de opções dentro de cada lote.

Mais uma vez, note que é importante haver conjuntos distintos de termos e condições do contrato para cada uma das categorias de lotes de Tipo de Oferta (por exemplo, IaaS/PaaS público, IaaS/PaaS comunitário, IaaS/PaaS privado), pois uma "abordagem de tamanho único" na contratação de cada lote ocasionará problemas de viabilidade e compatibilidade técnicas.

Consulte a seção *2.1.4* para ver a amostra de linguagem do RFP na seleção de Outorgados.

2.5.3 Entrada e saída

Uma consideração a ter em mente na criação do Contrato Quadro de Cloud é a opção de um Sistema de Compra Dinâmica (Dynamic Purchasing System - DPS). Com um modelo de DPS, todos os fornecedores que respondam aos requisitos mínimos do Contrato Quadro são admitidos no Quadro. Não há limites rígidos para o número de fornecedores que podem ingressar no Quadro e, diferentemente do acordo quadro tradicional, os fornecedores também se podem candidatar a participar do "Quadro DPS" a qualquer momento.

Recomendamos que as entidades do setor público definam padrões elevados para assegurar a qualidade e a garantia do serviço prestado por fornecedores qualificados, mas não tão específicos ao ponto de desqualificar os CISPs de maneira que não garante a concorrência leal. O objetivo é evitar saturar o utilizador final com demasiadas opções, mantendo o padrão alto das tecnologias de Cloud disponíveis.

3.0 Melhores práticas/lições aprendidas

Abaixo, destacamos algumas lições aprendidas sobre como elaborar um bom Contrato Quadro de Cloud com um RFP bem redigido de Serviços de Cloud.

3.1 Governação da Cloud

Governação na Cloud é uma responsabilidade partilhada. Os CISPs oferecem recursos e serviços para integrar a governação da Cloud em todos os aspectos de um ambiente de Cloud, enquanto os clientes trazem os seus padrões existentes de governação e aprendem como a Cloud é um capacitador de governação.

Na Cloud, os clientes têm a oportunidade de criar o ambiente de TI que desejarem, além de poderem gerir o que já possuem. A Cloud permite que os clientes: (1) comecem com um inventário completo de todos os ativos de TI; (2) gestionem todos os ativos centralmente; e (3) criem alertas relacionados com a utilização/faturação/segurança/etc. Todos esses benefícios vitais da Cloud ajudam os clientes a ter uma arquitetura otimizada e automatizada ao máximo, sem a necessidade de adquirir e instalar continuamente hardware novo. Isso é feito pelo CISP, permitindo que os clientes mudem o foco da gestão de infraestrutura indiferenciada para o nível de operações mission-critical.

Uma forma útil de ver uma Cloud do CISP é como sendo efetivamente uma API muito abrangente. Se estiver a arrancar com um novo servidor ou a alterar configurações de segurança, está apenas a fazer chamadas de APIs. Toda a alteração no ambiente é registada e gravada (o quem, o quê, onde, e o quando de cada alteração é gravado). Isso fornece governação na Cloud, controle e visibilidade que só são possíveis num ambiente de Cloud. Permite que os clientes repensem os seus modelos existentes de governação de TI e determinem como eles podem ser simplificados e aprimorados, considerando-se os benefícios que a Cloud traz.

A governação na Cloud também significa comunicar e incorporar alterações processuais positivas e novos conjuntos de competências que vêm com a Cloud. Por exemplo, gestores de projeto já estão acostumados com os meses de espera para implementar um ambiente de TI, por isso, podem superestimar demais os seus cronogramas para criar um ambiente de desenvolvimento ou teste na Cloud (algo que, com a Cloud, leva apenas alguns minutos). Adaptar-se a essa recém-encontrada agilidade será um processo evolutivo, que acontece programa a programa. Essas lições aprendidas devem ser partilhadas para que o Contrato

Quadro de Cloud possa continuar a evoluir de maneira a que os requisitos sejam adequados para novos processos e maior agilidade.

3.2 Orçamento para Cloud

Quando é necessário estruturar o preço de pagamento conforme o uso (pay per use) da Cloud de forma a se adequar aos requisitos de aquisição e orçamentação do setor público, descobrimos que é útil compactar serviços do CISP num único item de linha (computação, armazenamento, rede, base de dados, IoT, etc.), tudo abaixo de um item de linha de **Tecnologias de Cloud**. Essa abordagem concede flexibilidade para oferecer todas as novas e atuais tecnologias do CISP para utilizadores em tempo real, oferecendo o acesso rápido aos recursos necessários, quando eles precisam. Também acomoda a procura flutuante, que leva à utilização otimizada e a custos baixos.

As organizações do setor público podem adicionar outros itens de linha dos pedidos a partir de outros lotes num acordo Qaudro de Cloud, caso queiram serviços de consultoria/profissionais ou geridos, software de um "marketplace", serviços de suporte na Cloud e formação para as ofertas do CISP.

Mais flexibilidade contratual pode ser oferecida ao empregar itens de linha contratuais opcionais dentro de categorias de recursos apropriadas para acomodar o crescimento futuro. Como alternativa, se uma organização quiser incluir Tecnologias de Cloud com serviços de consultoria/profissionais/geridos em um item de linha, é possível, com o item de linha "Tecnologias de Cloud e mão de obra complementar".

Abaixo está um exemplo representativo dessa abordagem. No exemplo abaixo, cada unidade do item de linha '#1001 - Tecnologias de Cloud, é igual a € 1,00 das "Tecnologias de Cloud" usadas. Todo mês, os incrementos ao pedido podem ser custeados com base em projeções de utilização atuais e previstas.

Tabela 3 - Exemplo de estrutura de preços de item de linha único.

ITEM Nº	SUPRIMENTOS/SERVIÇOS	QUANTIDADE	UNIDADE	PREÇO UNITÁRIO	VALOR
1001	Tecnologias de Cloud	1.000	Cada	€ 1	€ 1.000
1002	Serviços de consultoria	1	Por semana	€ 3.000	€ 3.000
1003	Suporte à Cloud	1	Por mês	€ 1.000	€ 1.000
1004	Formação para Cloud	1	Por dia	€ 3,00	€ 3.000
1005	Marketplace de Cloud	10	Cada	€ 10	€ 100

Segue um exemplo de como essa estrutura pode funcionar: uma organização pública conversa com um CISP para estimar quanto dos serviços de tecnologia de Cloud ela irá usar. A organização concorda com os termos do fornecedor, como de € 10 milhões durante 5 anos, o que totaliza € 2 milhões por ano. A organização se compromete com o valor anual inicial de € 2 milhões. Todo mês, há uma cobrança, e o dinheiro é retirado do fundo. Há um desembolso na conta. O fundo restante é monitorado para fins de controlo de custos utilizando ferramentas de monitorização e previsão do CISP. Se o fundo restante for baixo, a organização solicita mais fundos do Diretor Financeiro para que os serviços sejam mantidos.

Exemplo de linguagem do RFP: Definição de preço - Contratação

PRAZOS DE PAGAMENTO
Os prazos de pagamento devem ser estruturados corretamente para pagar somente os recursos usados pela <ORGANIZAÇÃO>, conforme indicado abaixo:

1. *Pagamento mensal, com base no uso/consumo real de serviços e conforme os preços dos CISPs disponibilizados publicamente.*

GARANTIA MÍNIMA E DESPESA MÁXIMA
*Como é impossível que a **<ORGANIZAÇÃO>** determine exatamente qual o volume de recursos de um Fornecedor de Serviços de Cloud específico que será consumido durante certo período, os pedidos serão especificados por quantidades unitárias de preço fixo de um item de linha de pedido único para "Tecnologias de Cloud".*

*Cada unidade do item de linha pedido será igual a **<€ 1,00>** do valor das Tecnologias de Cloud pedidas. Pedidos incrementais serão periodicamente feitos pela modificação deste pedido em diversas quantidades, para que a **<ORGANIZAÇÃO>** tenha flexibilidade de pedir previamente diversas quantidades em "euro" de Tecnologias de Cloud do CISP com base no seu uso estimado para necessidades de duração variada. As quantidades serão periodicamente pedidas previamente pela **<ORGANIZAÇÃO>** em valores suficientes para cobrir o custo estimado das tecnologias de Cloud que serão usadas para atender aos diversos requisitos.*

Item Nº	Descrição	Qtde	Unidade	Preço
01	Tecnologias de Cloud do CISP	1.000	EA	€ 1.000,00

PEDIDO MÍNIMO/PEDIDO INCREMENTAL
*Os pedidos serão feitos periodicamente para diversas quantidades de **<10,000>** unidades de item de linha com base no uso estimado que a **<ORGANIZAÇÃO>** faz das tecnologias de Cloud. Essa disposição fornecerá à **<ORGANIZAÇÃO>** a flexibilidade de pedir previamente **<10.000>** unidades de "Tecnologias de Cloud", conforme a necessidade, para auxiliar as operações e permanecer consistente com as práticas comerciais de "pagamento conforme a utilização" da computação em Cloud.*

*Um incremento inicial de **<100.000>** unidades pelo custo de **<€ 100,000>** será pedido assim que o fornecimento programado (call-off) for realizado. O número mínimo de unidades de item de linha que pode ser feito num pedido incremental único que usa um ou mais itens de linha é **<x>.** O número máximo de unidades que podem ser pedidas conforme o pedido de entrega não pode exceder **<x>,** mas está sujeito a nunca exceder o valor do fornecimento programado quando combinado com todas as unidades anteriores pedidas. A **<ORGANIZAÇÃO>** será responsável por garantir que todos os pedidos estejam dentro dos limites especificados nesta seção.*

MÁXIMO DO PEDIDO
*O valor máximo total do pedido é até **<x>** consistindo em até **< x>** unidades de um item de linha único com o preço de **<x>** por unidade. O valor baseia-se numa estimativa dos requisitos da **<ORGANIZAÇÃO>** com relação ao período de desempenho, mas não é garantido.*

3.3 Sobre o modelo empresarial do parceiro

As entidades do setor público devem entender os modelos nos quais os CISPs fornecem as suas ofertas e reconhecer que os parceiros que fornecem consultoria, serviços geridos, revenda e muito mais são essenciais para o processo. Vários clientes precisam de um fornecedor de Cloud para a sua infraestrutura e terceirizam o trabalho «prático» de planeamento, migração e gestão a um integrador de sistemas (SI) ou a um fornecedor de serviços geridos. Dada essa combinação de "serviços", pode haver requisitos que não são aplicáveis a fornecedores de Cloud, como cláusulas de provisão de contrato para subcontratados.

Tomando tais cláusulas de provisão do contrato como um exemplo para ilustrar por que é importante entender como os parceiros e revendedores operam em relação aos CISPs, em alguns tipos de aquisição há cláusulas que exigem que o contratante principal repasse certas cláusulas obrigatórias a todos os seus parceiros/subcontratantes. Normalmente, os CISPs não fornecerão nem farão proposta como parceiros formais de subcontratação, já que eles oferecem um serviço padronizado em grande escala que não é feito para atender aos requisitos exclusivos de determinada finalidade do cliente (inclusive necessidades de um cliente do setor público, sob contrato com o setor público). Em um modelo de aquisição indireta (aquisição de serviços em Cloud por meio de um Revendedor CISP), um CISP pode rejeitar essas cláusulas oriundas de revendedores como não aplicáveis a um fornecedor de serviços comerciais de "2ª camada". Nesse caso, o CISP propriamente dito não está executando o âmbito de trabalho sob o contrato; o parceiro do CISP está usando a infraestrutura do CISP para tal. Portanto, o CISP é um fornecedor comercial (não subcontratado) das operações de um parceiro. Em um modelo de aquisição direta (compra de serviços em Cloud diretamente de um CISP), um CISP 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 CISPs não exige que subcontratados forneçam os seus serviços comerciais.

3.4 Cloud Brokers

O conceito de um agente de Cloud (Cloud broker) como meio de reduzir a possibilidade de aprisionamento tecnológico pode ser problemático. Embora um agente de Cloud possa ser uma boa ideia na teoria, na prática, isso provavelmente poderá gerar mais complexidade e confusão do que o valor realizado.

Tentar adquirir interfaces de Cloud para que funcionem em várias nuvens de forma simultânea ou intercambiável leva inevitavelmente a concessões na capacidade (não existe uma **Pedra de Roseta para a Cloud**). Essa abordagem acaba adicionando uma camada desnecessária de complexidade entre clientes do setor público e os seus serviços em Cloud, o que pode comprometer as eficiências e os ganhos de segurança que eles buscam obter, levando a escalabilidade e agilidade reduzidas, ao aumento nos custos e à desaceleração das inovações.

3.5 Fornecimento antes do RFP/pesquisa de mercado

Na medida em que a entidade do setor público planeia criar um RFP de Serviços de Cloud, deve incluir as partes interessadas de todos os aspectos da organização—liderança, partes interessadas de negócio, tecnologia, finanças, aquisição, jurídico e contratos—desde o início do processo. Essa abordagem garante que todas as partes interessadas conheçam o modelo de Cloud e, por consequência, uma abordagem educada para reavaliar os métodos tradicionais de aquisição de TI.

Quando o assunto é dialogar com o setor, recomendamos que as entidades do setor público tenham conversas detalhadas para recolher o feedback de CISPs, parceiros CISP, fornecedores de marketplaces de PaaS/SaaS, e especialistas do setor. Por exemplo, esse diálogo pode acontecer durante workshops de segurança e aquisição. Outra maneira eficiente de entender claramente a aquisição na Cloud é publicar um RFI, ou então idealmente um documento de rascunho do RFP. Geralmente, eles incluem possíveis problemas que podem ser identificados, abordados e ajustados antes que o RFP de Serviços de Cloud final seja publicado.

Apêndice A - Requisitos técnicos de comparação entre os licitantes

Segue abaixo uma lista de requisitos genéricos de tecnologia de Cloud que podem ser usados para comparação de CISPs durante planos de fornecimento programado ou mini concorrências em um Contrato de Estrutura de Cloud.

1. Perfil do fornecedor de Cloud

	Requisito
1.	***EXPERIÊNCIA DE MERCADO:*** *Há quantos anos o fornecedor de Cloud opera no segmento do mercado de Cloud?*
2.	***ABERTURA E PROTEÇÃO DE DADOS:*** *O fornecedor de Cloud adere a Códigos de conduta de Proteção ou reversibilidade de dados do setor? O fornecedor de Cloud adere a princípios de desenvolvimento de código aberto e API abertas?*

2. Infraestrutura global

	Requisito
1.	***ALCANCE GLOBAL:*** *O fornecedor de Cloud oferece uma infraestrutura global para ajudar os utilizadores a alcançarem baixa latência e alta taxa de transferência?*
2.	***REGIÕES:*** *O fornecedor de Cloud tem uma presença regional nas áreas geográficas necessárias?*
3.	***DOMÍNIOS/ZONAS:*** *O fornecedor de Cloud implementa o conceito de domínios ou zonas, onde vários data centers são agrupados em uma rede de baixa latência para oferecer um nível maior de alta disponibilidade e tolerância a falhas?* • *Se sim, liste o número de domínios e zonas e o número de data centers dentro da geografia necessária*
4.	***DISTÂNCIA DOS DOMÍNIOS/ZONAS:*** *O fornecedor de Cloud constrói seus domínios ou zonas com data centers separados fisicamente para oferecer suporte à redundância, alta disponibilidade e baixa latência?*
5.	***DATACENTERS CRIADOS:*** *O fornecedor de Cloud oferece data centers projetados para estarem isolados de falhas em outros data centers, com alimentação, arrefecimento e redes redundantes?*
6.	***REPLICAÇÃO DE DATACENTER:*** *O fornecedor de Cloud oferece replicação de dados entre os data centers dentro de um domínio ou zona com failover automático?*
7.	***REPLICAÇÃO DOS DOMÍNIOS/ZONAS:*** *O fornecedor de Cloud oferece replicação de dados entre domínios ou zonas dentro de uma região?*

3. Infraestrutura

3.1 Computação

	Requisito
1.	***COMPUTAÇÃO – INSTÂNCIA REGULAR – USO GERAL*** *O fornecedor de Cloud oferece os tipos de instância a seguir?* • *Uso geral – otimizado para aplicações genéricas e fornece um equilíbrio de computação, memória e recursos de rede.* o *Se sim, qual é a maior instância?*
2.	***COMPUTAÇÃO – INSTÂNCIA REGULAR – OTIMIZADA PARA MEMÓRIA:*** *O fornecedor de Cloud oferece os tipos de instância a seguir?* • *Otimizado para memória – otimizado para aplicações com uso intensivo de memória* o *Se sim, qual é a maior instância?*
3.	***COMPUTAÇÃO – INSTÂNCIA REGULAR – OTIMIZADA PARA COMPUTAÇÃO:*** *O fornecedor de Cloud oferece os tipos de instância a seguir?* • *Otimizado para computação – otimizado para aplicações com uso intensivo de computação* o *Se sim, qual é a maior instância?*
4.	***COMPUTAÇÃO – INSTÂNCIA REGULAR – OTIMIZADA PARA ARMAZENAMENTO:*** *O fornecedor de Cloud oferece os tipos de instância a seguir?* • *Otimizado para armazenamento – oferece uma grande quantidade de capacidade de armazenamento local* o *Em caso afirmativo, qual é a capacidade máxima de armazenamento (ou seja, 5, 10, 20, 50 TB) e o número máximo de discos (HDDs/SSDs) que podem ser provisionados e anexados a uma instância?*
5.	***COMPUTAÇÃO – INSTÂNCIA REGULAR – OTIMIZADA PARA GRÁFICOS:*** *O fornecedor de Cloud oferece os tipos de instância a seguir?* • *Gráficos de baixo custo – oferece aceleração de gráficos de baixo custo para instâncias de computação?* o *Se sim, qual é a maior instância?*
6.	***COMPUTAÇÃO – INSTÂNCIA REGULAR – OTIMIZADA PARA GPU:*** *O fornecedor de Cloud oferece os tipos de instância a seguir?* • *GPU – oferece unidades de processamento gráfico de hardware (GPUs) para aplicaçõess com uso intensivo de gráficos* o *Em caso afirmativo, quantas GPUs e quais modelos de GPU o fornecedor de Cloud pode oferecer por instância?*
7.	***COMPUTAÇÃO – INSTÂNCIA REGULAR – OTIMIZADA PARA FPGA:*** *O fornecedor de Cloud oferece os tipos de instância a seguir?* • *FPGA - oferece FPGAs (Matriz de portas programável em campo) para desenvolvimento e implantação de aceleração de hardware personalizada para aplicaçõess.* o *Em caso afirmativo, quantas FPGAs o fornecedor de Cloud pode oferecer por instância?*
8.	***COMPUTAÇÃO – INSTÂNCIA COM CAPACIDADE DE INTERMITÊNCIA:***

	O fornecedor de Cloud oferece instâncias com capacidade de intermitência que fornecem um nível de referência do desempenho da unidade de processamento central (CPU) com capacidade de intermitência acima da linha de base? • *Se sim, qual é a maior instância com capacidade de intermitência?*
9.	*COMPUTAÇÃO – INSTÂNCIA COM E/S INTENSIVA:* *O fornecedor de Cloud oferece instâncias que usam unidades de estado sólido (SSDs) de memória expressa não volátil (NVMe) otimizadas para baixa latência, altíssimo desempenho de E/S aleatório e alta taxa de transferência de leitura sequencial?* • *Se sim, qual é a capacidade máxima de operações de entrada/saída por segundo (IOPS) da maior instância?*
10.	*COMPUTAÇÃO – ARMAZENAMENTO LOCAL TEMPORÁRIO:* *O fornecedor de Cloud oferece suporte ao armazenamento local para instâncias de computação a serem usadas para armazenamento temporário de informações que mudam com frequência?*
11.	*COMPUTAÇÃO – SUPORTE PARA VÁRIOS NICs:* *O fornecedor de Cloud oferece suporte a várias placas de interface de rede (NICs) (primárias e adicionais) a serem alocadas para uma determinada instância?* • *Se sim, qual é o número máximo de NICs por instância?*
12.	*COMPUTAÇÃO – AFINIDADE DE INSTÂNCIA:* *O fornecedor de Cloud oferece aos utilizadores a possibilidade de agrupar as instâncias logicamente no mesmo data center?*
13.	*COMPUTAÇÃO – ANTIAFINIDADE DE INSTÂNCIA:* *O fornecedor de Cloud oferece aos utilizadores a possibilidade de agrupar logicamente as instâncias e colocá-las em diferentes data centers dentro de uma região?*
14.	*COMPUTAÇÃO – PROVISIONAMENTO SELF-SERVICE:* *O fornecedor de Cloud oferece o provisionamento self-service de várias instâncias simultaneamente por meio de uma interface programática, uma consola de gestão ou um portal da Web?*
15.	*COMPUTAÇÃO – PERSONALIZAÇÃO:* *O fornecedor de Cloud oferece instâncias personalizáveis, ou seja, possibilidade de modificar configurações como unidades de processamento central virtual (vCPUs) e memória de acesso aleatório (RAM)?*
16.	*COMPUTAÇÃO – LOCAÇÃO:* *O fornecedor de Cloud oferece instâncias de locatário único que são executadas em hardware dedicado a um único utilizador?* • *Se sim, qual é a maior instância de locatário único disponível?*
17.	*COMPUTAÇÃO – AFINIDADE DE HOST:* *O fornecedor de Cloud oferece a possibilidade de iniciar uma instância e especificar que essa instância sempre reinicia no mesmo host físico?*
18.	*COMPUTAÇÃO – ANTIAFINIDADE DE HOST:* *O fornecedor de Cloud oferece a possibilidade de dividir e hospedar instâncias específicas em diferentes hosts físicos?*
19.	*COMPUTAÇÃO – ESCALABILIDADE AUTOMÁTICA:* *O fornecedor de Cloud oferece a possibilidade de aumentar automaticamente o número de instâncias durante picos de procura para manter o desempenho (ou seja, "escalabilidade horizontal")?*
20.	*COMPUTAÇÃO – MECANISMO DE IMPORTAÇÃO DE IMAGEM:* *O fornecedor de Cloud oferece aos utilizadores a possibilidade de importar suas imagens existentes e salvá-las como novas imagens disponíveis para uso particular que podem ser usadas para provisionar instâncias no futuro?*

	• *Se sim, quais formatos são compatíveis?*
21.	*COMPUTAÇÃO – MECANISMO DE EXPORTAÇÃO DE IMAGEM:* *O fornecedor de Cloud oferece a possibilidade de exportar uma instância em execução existente ou uma cópia de uma instância para um formato de máquina virtual?* • *Se sim, quais formatos são compatíveis?*
22.	*COMPUTAÇÃO – INTERRUPÇÃO DE SERVIÇO:* *O fornecedor de Cloud oferece mecanismos para evitar interrupções de instância ou tempo de inatividade quando o fornecedor está executando algum tipo de manutenção de hardware ou serviço no nível do host?*
23.	*COMPUTAÇÃO – REINÍCIO DA INSTÂNCIA:* *O fornecedor de Cloud oferece mecanismos para reiniciar automaticamente instâncias em um host íntegro, se o host físico original falhar?*
24.	*COMPUTAÇÃO – NOTIFICAÇÕES:* *No caso de um evento resiliente de computação, o fornecedor de Cloud pode notificar o utilizador de que um evento como esse ocorreu e o utilizador pode incluir ou excluir essa comunicação por meio de autoatendimento?*
25.	*COMPUTAÇÃO – PROGRAMAÇÃO DE EVENTO:* *O fornecedor de Cloud oferece a possibilidade de agendar eventos para as instâncias do utilizador, como reinicializar, interromper, iniciar ou retirar a instância?*
26.	*COMPUTAÇÃO – MECANISMO DE BACKUP E RESTAURAÇÃO:* *O fornecedor de Cloud oferece um mecanismo integrado de backup e recuperação?*
27.	*COMPUTAÇÃO – MECANISMO DE SNAPSHOT:* *O fornecedor de Cloud oferece um mecanismo manual de snapshot sob pedido?*
28.	*COMPUTAÇÃO – METADADOS:* *O fornecedor de Cloud oferece um serviço de meta dados de instância que permite aos utilizadores definir pares arbitrários de chave/valor para a instância?*
29.	*COMPUTAÇÃO – CHAMADA DE METADADOS:* *O fornecedor de Cloud oferece um serviço de meta dados de instância que fornece uma interface de programação de aplicaçõess (API) que a instância pode chamar para obter informações sobre si mesma?*
30.	*COMPUTAÇÃO – MECANISMO DE LANCES:* *O fornecedor de Cloud oferece um mecanismo de lances para definir lances para instâncias de custo mais baixo que podem ser imediatamente instanciadas para hospedar cargas de trabalho não críticas?*
31.	*COMPUTAÇÃO – MECANISMO DE PROGRAMAÇÃO:* *O fornecedor de Cloud oferece alguma maneira de programar e reservar a capacidade computacional adicional de forma recorrente, ou seja, programação diária, semanal ou mensal?*
32.	*COMPUTAÇÃO – MECANISMO DE RESERVA:* *O fornecedor de Cloud oferece alguma maneira de reservar a capacidade computacional adicional para o futuro (ou seja, 1 ano, 2 anos, 3 anos, etc.)?*
33.	*COMPUTAÇÃO – SISTEMA OPERATIVO LINUX:* *O fornecedor de Cloud oferece suporte às duas últimas versões de longo prazo compatíveis de pelo menos uma distribuição Linux comercial (como Red Hat, SUSE) e uma distribuição Linux gratuita comumente usada (como Ubuntu, CentOS e Debian)?*
34.	*COMPUTAÇÃO – SISTEMA OPERATIVO WINDOWS:*

	O fornecedor de Cloud oferece suporte às duas principais versões do Windows Server (Windows Server 2017 e Windows Server 2016)?
35.	***COMPUTAÇÃO – PORTABILIDADE DAS LICENÇAS:*** *O fornecedor de Cloud oferece portabilidade e suporte para licenças?* • *Se sim, liste o fornecedor do software, os nomes de software, as edições e suas versões.*
36.	***COMPUTAÇÃO – LIMITES DE SERVIÇO:*** *O fornecedor de Cloud possui alguma restrição (ou seja, limites de serviço) em relação à seção de computação acima?* *Exemplo:* *Número máximo de instâncias por conta* *Número máximo de hosts dedicados por conta* *Número máximo de endereços IP reservados*

3.2 Redes

	Requisito
1.	***REDES – REDES VIRTUAIS:*** *O fornecedor de Cloud oferece a possibilidade de criar uma rede virtual lógica e isolada que represente a própria rede de uma empresa na Cloud?*
2.	***REDES – CONECTIVIDADE NA MESMA REGIÃO:*** *O fornecedor de Cloud oferece suporte à conexão de duas redes virtuais na mesma região para rotear o tráfego entre elas usando endereços IP privados?*
3.	***REDES – CONECTIVIDADE EM REGIÕES DIFERENTES:*** *O fornecedor de Cloud oferece suporte à conexão de duas redes virtuais em regiões diferentes para rotear o tráfego entre elas usando endereços IP privados?*
4.	***REDES – SUBREDE PRIVADA*** *O fornecedor de Cloud oferece a possibilidade de criar redes e subredes virtuais totalmente isoladas (privadas) nas quais as instâncias podem ser provisionadas sem qualquer endereço IP ou roteamento de Internet pública?*
5.	***REDES – INTERVALO DE ENDEREÇOS DE REDE VIRTUAL:*** *O fornecedor de Cloud oferece suporte a intervalos de endereços IP especificados na solicitação de comentários (RFC) 1918, bem como a blocos de roteamento sem classe entre domínios (CIDR) publicamente roteáveis?*
6.	***REDES – VÁRIOS PROTOCOLOS:*** *O fornecedor de Cloud oferece suporte a vários protocolos, incluindo o protocolo de controle de transmissão (TCP), o protocolo de datagrama do utilizador (UDP) e o protocolo de mensagem de controle da Internet (ICMP)?*
7.	***REDES – ATRIBUIÇÃO AUTOMÁTICA PARA ENDEREÇOS IP:*** *O fornecedor de Cloud oferece a possibilidade de atribuir automaticamente endereços IP públicos às instâncias?*
8.	***REDES – ENDEREÇOS IP ESTÁTICOS RESERVADOS:*** *O fornecedor de Cloud oferece suporte a endereços IP associados a uma conta de utilizador e não a uma instância específica? O endereço IP deve permanecer associado à conta até ser liberado explicitamente.*
9.	***REDES – SUPORTE AO IPV6:***

	O fornecedor de Cloud oferece suporte ao protocolo de Internet versão 6 (IPv6) no nível do gateway ou da instância e expõe essa funcionalidade aos utilizadores?
10.	***REDES – VÁRIOS ENDEREÇOS IP POR NIC:*** *O fornecedor de Cloud oferece a possibilidade de atribuir um endereço IP primário e um secundário a uma placa de interface de rede (NIC) conectada a uma determinada instância?*
11.	***REDES – VÁRIOS NICS:*** *O fornecedor de Cloud oferece a possibilidade de atribuir várias placas de interface de rede (NICs) a uma determinada instância?*
12.	***REDES – MOBILIDADE DE NIC E IP:*** *O fornecedor de Cloud oferece a possibilidade de mover placas de interface de rede (NICs), bem como endereços IP entre instâncias?*
13.	***REDES – SUPORTE AO SR-IOV:*** *O fornecedor de Cloud oferece suporte a recursos como virtualização de entrada/saída de raiz única (SR-IOV) para maior desempenho (ou seja, pacotes por segundo - PPS), menor latência e menor variação?*
14.	***REDES – FILTRAGEM DE ENTRADA:*** *O fornecedor de Cloud possibilita adicionar ou remover regras aplicáveis ao tráfego de entrada para instâncias?*
15.	***REDES – FILTRAGEM DE SAÍDA:*** *O fornecedor de Cloud possibilita adicionar ou remover regras aplicáveis ao tráfego de saída originado de instâncias?*
16.	***REDES – ACL:*** *O fornecedor de Cloud oferece listas de controle de acesso (ACLs) para controlar o tráfego de entrada e de saída para subredes?*
17.	***REDES – SUPORTE AO REGISTRO DE FLUXO:*** *O fornecedor de Cloud oferece a possibilidade de capturar registros de fluxo de tráfego de rede?*
18.	***REDES – NAT:*** *O fornecedor de Cloud fornece um serviço gerido de gateway de conversão de endereços de rede (NAT) para permitir que instâncias em uma rede privada se conectem à Internet ou a outros serviços em Cloud, mas impede que a Internet inicie uma conexão com essas instâncias?*
19.	***REDES – VERIFICAÇÃO DE ORIGEM/DESTINO:*** *O fornecedor de Cloud oferece a possibilidade de desabilitar a verificação de origem/destino em placas de interface de rede (NICs)?*
20.	***REDES – SUPORTE AO VPN:*** *O fornecedor de Cloud oferece suporte à conectividade de rede privada virtual (VPN) entre o fornecedor de Cloud e o data center do utilizador?*
21.	***REDES – TÚNEIS DE VPN:*** *O fornecedor de Cloud oferece suporte a várias conexões de rede virtual privada (VPN) por rede virtual?*
22.	***REDES – SUPORTE À VPN DE IPSEC:*** *O fornecedor de Cloud permite que os utilizadores acessem serviços em Cloud por meio de um túnel de VPN de segurança de protocolo da Internet (IPsec) ou túnel de VPN de Secure Sockets Layer (SSL) pela Internet pública?*
23.	***REDES – SUPORTE AO BGP:*** *O fornecedor de Cloud aplica o Border Gateway Protocol (BGP) para melhorar o failover em túneis de rede virtual privada (VPN) de segurança de protocolo da Internet (IPsec)?*

24.	***REDES – CONECTIVIDADE DEDICADA PRIVADA:*** *O fornecedor de Cloud oferece um serviço de conectividade privada e direta entre os locais do fornecedor de Cloud e o ambiente de data center, escritório ou colocação de um utilizador que permite transferências de dados grandes e rápidas?*
25.	***REDES – LOAD BALANCER DE FRONT-END:*** *O fornecedor de Cloud oferece um serviço de balanceamento de carga de front-end (voltado para a Internet) que recebe solicitações de clientes pela Internet e distribui essas solicitações entre instâncias registradas com o load balancer?*
26.	***REDES – LOAD BALANCER DE BACK-END:*** *O fornecedor de Cloud oferece um serviço de balanceamento de carga de back-end (privado) que direciona o tráfego para instâncias hospedadas em subredes privadas?*
27.	***REDES – LOAD BALANCER DA CAMADA 7:*** *O fornecedor de Cloud oferece um serviço de load balancer de camada 7 (protocolo de transferência de hipertexto - HTTP) que pode balancear a carga de tráfego de rede em várias instâncias?*
28.	***REDES – LOAD BALANCER DA CAMADA 4:*** *O fornecedor de Cloud oferece um serviço de load balancer de camada 4 (protocolo de controle de transmissão - TCP) que pode balancear a carga de tráfego de rede em várias instâncias?*
29.	***REDES - AFINIDADE DE SESSÃO PARA LOAD BALANCERS:*** *O fornecedor de Cloud oferece um serviço de balanceamento de carga que possibilita a afinidade de sessão?*
30.	***REDES – BALANCEAMENTO DE CARGA BASEADO EM DNS:*** *O fornecedor de Cloud oferece um serviço de balanceamento de carga que pode balancear a carga de tráfego para instâncias hospedadas em vários hosts que pertencem a um único domínio?*
31.	***REDES – LOGS DO LOAD BALANCER:*** *O fornecedor de Cloud fornece logs que capturam informações detalhadas sobre todas as solicitações enviadas a um load balancer?*
32.	***REDES – DNS:*** *O fornecedor de Cloud oferece um serviço de sistema de nomes de domínio (DNS) altamente disponível e escalável?*
33.	***REDES – ROTEAMENTO DE DNS BASEADO EM LATÊNCIA:*** *O fornecedor de Cloud oferece um serviço DNS compatível com o roteamento baseado em latência (ou seja, o serviço DNS responde a consultas DNS com os recursos que fornecem a melhor latência)?*
34.	***REDES – ROTEAMENTO DE DNS BASEADO EM GEOGRAFIA:*** *O fornecedor de Cloud oferece um serviço DNS compatível com o roteamento baseado em geografia (ou seja, o serviço DNS responde a consultas DNS com base na localização geográfica dos utilizadores)?*
35.	***REDES – ROTEAMENTO DE DNS BASEADO EM FAILOVER:*** *O fornecedor de Cloud oferece um serviço DNS compatível com o roteamento baseado em failover (ou seja, o serviço DNS direciona consultas DNS para o recurso que está ativo no momento, enquanto um segundo recurso aguarda e só fica ativo no caso de uma falha no recurso principal)?*
36.	***REDES – SERVIÇO DE REGISTRO DE DOMÍNIO:***

	O fornecedor de Cloud oferece serviços de registro de nomes de domínio (por exemplo, os utilizadores podem pesquisar e registrar nomes de domínio disponíveis)?
37.	***REDES – VERIFICAÇÕES DE INTEGRIDADE DE DNS:*** *O fornecedor de Cloud oferece um serviço DNS que usa verificações de integridade para monitorar a integridade e o desempenho dos recursos?*
38.	***REDES – INTEGRAÇÃO DE DNS E LOAD BALANCER:*** *O fornecedor de Cloud oferece um serviço DNS que se integra ao load balancer do fornecedor de Cloud?*
39.	***REDES – EDITOR VISUAL:*** *O fornecedor de Cloud oferece uma ferramenta que permite aos utilizadores criar políticas para a gestão de tráfego?*
40.	***REDES – REDE DE ENTREGA DE CONTEÚDO (CDN):*** *O fornecedor de Cloud oferece um serviço de rede de entrega de conteúdo (CDN) para distribuir conteúdo com baixa latência e altas velocidades de transferência de dados?*
41.	***REDES – EXPIRAÇÃO DO CACHE DA CDN:*** *O fornecedor de Cloud oferece um serviço CDN que permite remover um objeto dos pontos de presença de caches antes que ele expire, incluindo recursos como a invalidação e o versionamento de objetos?*
42.	***REDES – ORIGENS EXTERNAS DA CDN:*** *O fornecedor de Cloud oferece um serviço CDN compatível com uma origem personalizada, ou seja, um servidor de protocolo de transferência de hipertexto (HTTP)?*
43.	***REDES – OTIMIZAÇÃO DA CDN:*** *O fornecedor de Cloud oferece um serviço de rede de entrega de conteúdo (CDN) com controle granular para configurar vários servidores de origem e armazenar em cache propriedades de diferentes URLs?*
44.	***REDES – CDN COM RESTRIÇÃO GEOGRÁFICA:*** *O fornecedor de Cloud oferece um serviço de rede de entrega de conteúdo (CDN) que oferece suporte à restrição geográfica, ou seja, impede que utilizadores em áreas geográficas específicas acessem o conteúdo?*
45.	***REDES – TOKENS DA CDN:*** *O fornecedor de Cloud oferece um serviço de rede de entrega de conteúdo (CDN) que oferece suporte a signed URLs que normalmente incluem informações adicionais, como data/hora de expiração, para dar aos utilizadores mais controle sobre o acesso ao conteúdo?*
46.	***REDES – CERTIFICADOS DA CDN:*** *O fornecedor de Cloud oferece um serviço de rede de entrega de conteúdo (CDN) que oferece suporte a certificados Secure Sockets Layer (SSL) customizados para fornecer conteúdo de forma segura por HTTPS de pontos de presença?*
47.	***REDES – CACHE MULTICAMADAS CDN:*** *O fornecedor de Cloud oferece um serviço de rede de entrega de conteúdo (CDN) que aplica uma abordagem de cache multicamadas com o uso de caches de ponto regional para reduzir a latência?*
48.	***REDES – COMPACTAÇÃO DA CDN:*** *O fornecedor de Cloud oferece um serviço de rede de entrega de conteúdo (CDN) compatível com a compactação de arquivos?*
49.	***REDES – UPLOADS CRIPTOGRAFADOS DA CDN:***

	O fornecedor de Cloud oferece uma rede de entrega de conteúdo (CDN) que permite que os utilizadores façam upload de seus dados confidenciais com segurança, de forma que essas informações só possam ser visualizadas por determinados componentes e serviços na infraestrutura de origem do utilizador?
50.	***REDES – ENDPOINTS:*** *O serviço de rede do fornecedor de Cloud oferece aos utilizadores endpoints que podem rotear o tráfego por meio da conectividade de rede interna do fornecedor (ou seja, conectividade privada) para reduzir os custos de comunicação e melhorar a segurança do tráfego?*
51.	***REDES – LIMITES DE SERVIÇO:*** *O fornecedor de Cloud possui alguma restrição (ou seja, limites de serviço) em relação à seção de redes?* *Exemplo:* *Número máximo de redes virtuais por conta* *Tamanho máximo de uma rede virtual* *Número máximo de subredes por conta* *Número máximo de load balancers por conta* *Número máximo de entradas da lista de controle de acesso (ACL)* *Número máximo de túneis de rede virtual privada (VPN)* *Número máximo de origens por distribuição* *Número máximo de certificados por load balancer*

3.3 Armazenamento

	Requisito
1.	***SERVIÇO DE ARMAZENAMENTO EM BLOCO:*** *O fornecedor de Cloud oferece volumes de armazenamento em nível de bloco para usar com instâncias de computação?*
2.	***ARMAZENAMENTO DE BLOCOS – IOPS:*** *O fornecedor de Cloud oferece a opção de comprar um nível de desempenho ou destino de desempenho explícito em volumes de armazenamento em bloco, como um determinado número de operações de entrada/saída por segundo (IOPS) ou megabytes por segundo (MB/S) de taxa de transferência?*
3.	***ARMAZENAMENTO EM BLOCO – UNIDADES DE ESTADO SÓLIDO:*** *O fornecedor de Cloud oferece suporte ao meio de armazenamento com base em unidade de estado sólido (SSD) que oferece latências de milissegundo com único dígito?* • *Se sim, qual é o número máximo de SSDs que podem ser anexados por instância?*
4.	***ARMAZENAMENTO EM BLOCO – ESCALABILIDADE:*** *O fornecedor de Cloud oferece aos utilizadores a possibilidade de aumentar o tamanho de um volume de armazenamento em bloco existente sem precisar provisionar um novo volume e copiar/mover os dados?*
5.	***ARMAZENAMENTO EM BLOCO – SNAPSHOTS:*** *O fornecedor de Cloud tem recursos de snapshot para o serviço de armazenamento em bloco?*
6.	***ARMAZENAMENTO EM BLOCO – ELIMINAÇÃO DE DADOS:*** *O fornecedor de Cloud oferece suporte à eliminação completa de dados, de modo que os dados não sejam mais legíveis ou acessíveis por utilizadores não autorizados e/ou terceiros?*

7.	***ARMAZENAMENTO EM BLOCO – CRIPTOGRAFIA EM REPOUSO:*** *O fornecedor de Cloud oferece criptografia de dados em repouso no lado do servidor para os dados armazenados em volumes e seus snapshots?* • *Se sim, qual é o algoritmo de criptografia aplicado?*
8.	***SERVIÇO DE ARMAZENAMENTO DE OBJETOS:*** *O fornecedor de Cloud oferece armazenamento de objetos seguro, durável e altamente escalável para armazenar e recuperar qualquer quantidade de dados da Web?*
9.	***ARMAZENAMENTO DE OBJETOS – ACESSO POUCO FREQUENTE:*** *O fornecedor de Cloud oferece um nível de serviço de armazenamento de baixo custo destinado a armazenar objetos e arquivos acedidos com menos frequência?*
10.	***ARMAZENAMENTO DE OBJETOS – DURABILIDADE MAIS BAIXA:*** *O fornecedor de Cloud oferece um nível de redundância reduzido no qual um utilizador pode armazenar objetos não críticos e de fácil reprodução a um preço menor?*
11.	***ARMAZENAMENTO DE OBJETOS – ACESSO MENOS FREQUENTE:*** *O fornecedor de Cloud oferece um nível para dados acedidos com menos frequência, mas isso ainda exige acesso rápido?*
12.	***ARMAZENAMENTO DE OBJETOS – CAMADAS DE OBJETOS:*** *O fornecedor de Cloud oferece o recurso de nivelamento de camadas de objetos, ou seja, a possibilidade de recomendar a transição de um objeto entre classes ou níveis de armazenamento de objetos com base em sua frequência de acesso?*
13.	***ARMAZENAMENTO DE OBJETOS – GESTÃO DO CICLO DE VIDA:*** *O fornecedor de Cloud oferece suporte à gestão do ciclo de vida de um objeto usando uma configuração de ciclo de vida, que define como os objetos são geridos durante sua vida útil, desde a criação até a exclusão?*
14.	***ARMAZENAMENTO DE OBJETOS – GESTÃO CONTROLADA POR POLÍTICA:*** *O fornecedor de Cloud oferece a possibilidade de criar e usar políticas para gerir dados armazenados, o ciclo de vida e as configurações de nivelamento?*
15.	***ARMAZENAMENTO DE OBJETOS – POLÍTICAS BASEADAS EM LOCALIZAÇÃO E HORA:*** *O fornecedor de Cloud oferece aos utilizadores a possibilidade de criar políticas que possam restringir o acesso aos dados com base na localização do utilizador e na hora da solicitação?*
16.	***ARMAZENAMENTO DE OBJETOS – HOSPEDAGEM DE SITE:*** *O fornecedor de Cloud oferece suporte à hospedagem de sites estáticos fora do serviço de armazenamento de objetos?*
17.	***ARMAZENAMENTO DE OBJETOS – CRIPTOGRAFIA EM REPOUSO:*** *O fornecedor de Cloud oferece suporte à criptografia do lado do servidor (SSE) de dados em repouso, com o fornecedor de Cloud gerenciando as chaves de criptografia?* • *Se sim, qual é o algoritmo de criptografia aplicado?*
18.	***ARMAZENAMENTO DE OBJETOS – CRIPTOGRAFIA COM CHAVES DO UTILIZADOR:*** *O fornecedor de Cloud oferece recursos de criptografia do lado do servidor (SSE) usando chaves criptográficas fornecidas pelo cliente?*
19.	***ARMAZENAMENTO DE OBJETOS – SERVIÇO GERIDO POR CHAVE:***

	O fornecedor de Cloud oferece suporte à criptografia no lado do servidor (SSE) usando um serviço de gestão de chaves que cria chaves de criptografia, define as políticas que controlam como as chaves podem ser usadas e faz auditorias do uso das chaves para provar que estão sendo usadas corretamente?
20.	***ARMAZENAMENTO DE OBJETOS – CHAVE MESTRA NO LADO DO CLIENTE:*** *O fornecedor de Cloud oferece aos utilizadores a opção de manter o controle das chaves de criptografia e concluir a criptografia/descriptografia de objetos do lado do cliente?*
21.	***ARMAZENAMENTO DE OBJETOS – CONSISTÊNCIA FORTE:*** *O fornecedor de Cloud oferece suporte à consistência de leitura após gravação para operações PUT para novos objetos?*
22.	***ARMAZENAMENTO DE OBJETOS – LOCALIDADE DOS DADOS:*** *O fornecedor de Cloud oferece um forte isolamento regional, de modo que os objetos armazenados em uma região nunca deixem a região, a menos que o utilizador os transfira explicitamente para outra região?*
23.	***ARMAZENAMENTO DE OBJETOS – REPLICAÇÃO:*** *O fornecedor de Cloud oferece um recurso de replicação entre regiões que replicará automaticamente os objetos nas regiões selecionadas pelo utilizador?*
24.	***ARMAZENAMENTO DE OBJETOS – VERSIONAMENTO:*** *O fornecedor de Cloud oferece suporte ao versionamento, ou seja, a possibilidade de armazenar e manter várias versões de um objeto?*
25.	***ARMAZENAMENTO DE OBJETOS – MARCADOR DE ITEM INDELETÁVEL:*** *O fornecedor de Cloud permite que um utilizador marque um item como nãondeletável?*
26.	***ARMAZENAMENTO DE OBJETOS – EXCLUSÃO DE MFA:*** *O fornecedor de Cloud oferece suporte à autenticação multifator (MFA) para operações de exclusão como uma opção de segurança adicional?*
27.	***ARMAZENAMENTO DE OBJETOS – MULTIPART UPLOAD:*** *O fornecedor de Cloud permite o upload de um objeto como um conjunto de partes, em que cada parte é uma parte contígua dos dados do objeto, e o upload dessas partes de objetos pode ser feito de forma independente e em qualquer ordem?*
28.	***ARMAZENAMENTO DE OBJETOS – TAGS:*** *O fornecedor de Cloud oferece a possibilidade de criar e associar tags dinâmicas mutáveis no nível do objeto?*
29.	***ARMAZENAMENTO DE OBJETOS – NOTIFICAÇÕES:*** *O fornecedor de Cloud oferece a possibilidade de enviar notificações quando determinados eventos ocorrem no nível do objeto (ou seja, operações de adição/exclusão)?*
30.	***ARMAZENAMENTO DE OBJETOS – LOGS:*** *O fornecedor de Cloud oferece a possibilidade de gerar logs de auditoria que incluem detalhes sobre uma única solicitação de acesso, como o solicitante, o horário da solicitação, a ação da solicitação, o status da resposta e o código de erro?*
31.	***ARMAZENAMENTO DE OBJETOS – INVENTÁRIO PARA OBJETOS:*** *O fornecedor de Cloud oferece recursos de inventário de objetos para fornecer aos utilizadores a possibilidade de visualizar rapidamente os objetos e o status, permitindo que os utilizadores identifiquem rapidamente os objetos com acesso público?*

32.	***ARMAZENAMENTO DE OBJETOS – INVENTÁRIO PARA METADADOS:*** *O fornecedor de Cloud oferece recursos de inventário de objetos para fornecer aos utilizadores a possibilidade de visualizar rapidamente os metadados de objetos?*
33.	***ARMAZENAMENTO DE OBJETOS – OTIMIZAÇÃO DE UPLOADS:*** *O fornecedor de Cloud oferece a possibilidade de rotear dados de pontos de presença para o serviço de armazenamento usando um caminho de rede otimizado?*
34.	***ARMAZENAMENTO DE OBJETOS – RECURSO DE CONSULTAS:*** *O fornecedor de Cloud oferece aos utilizadores a possibilidade de consultar seu serviço de armazenamento de objetos usando instruções de linguagem de consulta estruturada (SQL)?*
35.	***ARMAZENAMENTO DE OBJETOS – RECUPERAÇÃO DE SUBCONJUNTOS:*** *O fornecedor de Cloud oferece aos utilizadores a possibilidade de recuperar apenas um subconjunto de dados de um objeto usando expressões simples de linguagem de consulta estruturada (SQL)?*
36.	***SERVIÇO DE ARMAZENAMENTO DE ARQUIVOS:*** *O fornecedor de Cloud oferece um serviço de armazenamento de arquivos simples e escalável para usar com instâncias de computação na Cloud?*
37.	***ARMAZENAMENTO DE ARQUIVOS – REDUNDÂNCIA:*** *O fornecedor de Cloud armazena de forma redundante os objetos do sistema de arquivos (ou seja, diretório, arquivo e link) em vários data centers ou instalações para atingir níveis mais altos de disponibilidade e durabilidade?*
38.	***ARMAZENAMENTO DE ARQUIVOS – ELIMINAÇÃO DE DADOS:*** *O fornecedor de Cloud oferece suporte à eliminação completa de dados de armazenamento de arquivos, de modo que eles não sejam mais legíveis ou acessíveis por utilizadores não autorizados ou terceiros?*
39.	***ARMAZENAMENTO DE ARQUIVOS – ALTA DISPONIBILIDADE:*** *O sistema de arquivos geridos do fornecedor de Cloud fornece um alto nível de alta disponibilidade?*
40.	***ARMAZENAMENTO DE ARQUIVOS – NFS:*** *O fornecedor de Cloud é compatível com o protocolo do sistema de arquivos de rede (NFS)?*
41.	***ARMAZENAMENTO DE ARQUIVOS – SMB:*** *O fornecedor de Cloud oferece suporte ao protocolo de bloco de mensagens do servidor (SMB)?*
42.	***ARMAZENAMENTO DE ARQUIVOS – CRIPTOGRAFIA EM REPOUSO:*** *O serviço de armazenamento de arquivos do fornecedor de Cloud oferece suporte à criptografia em repouso?*
43.	***ARMAZENAMENTO DE ARQUIVOS – CRIPTOGRAFIA EM TRÂNSITO:*** *O serviço de armazenamento de arquivos do fornecedor de Cloud oferece suporte à criptografia de dados enquanto eles estão em trânsito?*
44.	***ARMAZENAMENTO DE ARQUIVOS – FERRAMENTA DE MIGRAÇÃO DE DADOS*** *O fornecedor de Cloud oferece alguma ferramenta de migração de dados para permitir que os utilizadores movam dados de sistemas locais para o sistema de arquivos baseado em Cloud?*
45.	***SERVIÇO DE ARMAZENAMENTO DE ARQUIVOS:*** *O fornecedor de Cloud oferece um serviço de armazenamento de custo muito baixo destinado a arquivar objetos e arquivos menos acedidos e praticamente imutáveis?*

46.	***ARMAZENAMENTO DE ARQUIVOS – TOLERÂNCIA A FALHAS:*** *A arquitetura do fornecedor de Cloud fornece tolerância a falhas para o serviço de armazenamento de arquivos?*
47.	***ARMAZENAMENTO DE ARQUIVOS – IMUTABILIDADE:*** *O fornecedor de Cloud oferece suporte à imutabilidade dos arquivos e objetos arquivados?*
48.	***ARMAZENAMENTO DE ARQUIVOS – WORM:*** *O fornecedor de Cloud oferece o recurso "uma gravação e muitas leituras" (WORM)?*
49.	***ARMAZENAMENTO DE ARQUIVOS – RECUPERAÇÃO DE SUBCONJUNTOS:*** *O fornecedor de Cloud oferece aos utilizadores a possibilidade de recuperar apenas um subconjunto de dados de um objeto arquivado usando expressões simples de linguagem de consulta estruturada (SQL)?*
50.	***ARMAZENAMENTO DE ARQUIVOS – RECUPERAÇÃO VELOZ:*** *O fornecedor de Cloud oferece aos utilizadores várias opções de recuperação de dados com diferentes custos e tempos de recuperação?*
51.	***ARMAZENAMENTO DE ARQUIVOS – CRIPTOGRAFIA EM REPOUSO:*** *O serviço de armazenamento de arquivos do fornecedor de Cloud oferece suporte à criptografia em repouso?*
52.	***ARMAZENAMENTO – LIMITES DE SERVIÇO:*** *O fornecedor de Cloud possui alguma restrição (ou seja, limites de serviço) em relação à seção de armazenamento acima?* *Exemplo:* *Tamanho máximo do volume* *Número máximo de unidades anexadas a uma instância* *Máximo de operações de entrada/saída por segundo (IOPS)* *Tamanho máximo do objeto* *Número máximo de objetos por conta de armazenamento* *Número máximo de snapshots*

4. Administração

	Requisito
1.	***ADMINISTRAÇÃO – UTILIZADORES E GRUPOS:*** *O fornecedor de Cloud oferece um serviço para criar e gerir utilizadores e grupos de utilizadores da sua infraestrutura e seus recursos?*
2.	***ADMINISTRAÇÃO – REDEFINIÇÃO DE SENHA:*** *O fornecedor em Cloud permite que os utilizadores redefinam suas próprias senhas, como autoatendimento?*
3.	***ADMINISTRAÇÃO – PERMISSÕES:*** *O fornecedor de Cloud oferece a capacidade de adicionar permissões para utilizadores e grupos em nível de recurso?*
4.	***ADMINISTRAÇÃO – PERMISSÕES TEMPORÁRIAS:*** *O fornecedor de Cloud oferece a capacidade de criar permissões válidas para um intervalo de tempo específico?*

5.	***ADMINISTRAÇÃO – CREDENCIAIS TEMPORÁRIAS:*** *O fornecedor de Cloud oferece aos utilizadores a capacidade de criar e fornecer credenciais de segurança temporárias para utilizadores confiáveis configuradas para durar desde alguns minutos até várias horas?*
6.	***ADMINISTRAÇÃO – CONTROLE DE ACESSO:*** *O fornecedor de Cloud oferece controles de acesso granulares para seus recursos de infraestrutura?* • *Se sim, quais condições podem ser usadas por esses controles (ou seja, hora do dia, endereço IP de origem, etc.)?*
7.	***ADMINISTRAÇÃO – POLÍTICAS INTEGRADAS:*** *A infraestrutura do fornecedor de Cloud contém políticas de controle de acesso integradas que podem ser anexadas aos utilizadores e grupos?*
8.	***ADMINISTRAÇÃO – POLÍTICAS PERSONALIZADAS:*** *A infraestrutura do fornecedor de Cloud permite a criação e a personalização de políticas de controle de acesso que podem ser anexadas aos utilizadores e grupos?*
9.	***ADMINISTRAÇÃO – SIMULADOR DE POLÍTICAS:*** *O fornecedor de Cloud oferece um mecanismo para testar os efeitos das políticas de controle de acesso antes de confirmar tais políticas para produção?*
10.	***ADMINISTRAÇÃO – MFA DE CLOUD:*** *O fornecedor de Cloud oferece suporte ao uso de autenticação multifator (MFA) como uma camada adicional de controle de acesso e autenticação para sua infraestrutura?*
11.	***ADMINISTRAÇÃO – LIMITES DE SERVIÇO:*** *O fornecedor de Cloud possui alguma restrição (ou seja, limites de serviço) em relação à seção de administração acima?* *Exemplo:* *Número máximo de utilizadores* *Número máximo de grupos* *Número máximo de políticas gerenciadas*

5. Segurança

	Requisito
1.	***SEGURANÇA – VERIFICAÇÕES DE ANTECEDENTES:*** *Todo o pessoal do fornecedor de Cloud que tem acesso à infraestrutura de serviço (seja física ou não física) está sujeito a verificações de antecedentes?*
2.	***SEGURANÇA – ACESSO FÍSICO:*** *O fornecedor de Cloud restringe o acesso do pessoal à infraestrutura do serviço a menos que exista um tíquete específico com esse problema, solicitação de alteração ou autorização formal semelhante?*
3.	***SEGURANÇA – LOGS DE ACESSO:*** *O fornecedor de Cloud registra em log o acesso do pessoal à infraestrutura, onde tal acesso sempre é registrado em log e os logs são mantidos durante um mínimo de 90 dias?*
4.	***SEGURANÇA – LOGINS DE HOST:***

	O fornecedor de Cloud impede que o seu pessoal faça login em hosts computacionais, automatizando todas as tarefas realizadas em hosts computacionais onde o conteúdo desses trabalhos automatizados é registrado em log, com os logs mantidos durante um mínimo de 90 dias?
5.	*SEGURANÇA – CHAVES CRIPTOGRÁFICAS:* *O fornecedor de Cloud oferece um serviço para criar e controlar as chaves criptográficas usadas para criptografar dados do utilizador?*
6.	*SEGURANÇA – GESTÃO DA CHAVE DE ACESSO:* *O fornecedor de Cloud oferece a capacidade de identificar quando uma chave de acesso foi usada pela última vez, rodar chaves antigas e remover utilizadores inativos?*
7.	*SEGURANÇA – CHAVES FORNECIDAS PELO CLIENTE:* *O fornecedor de Cloud permite que os utilizadores importem chaves a partir de suas próprias infraestruturas de gestão de chaves para o serviço de gestão de chaves do fornecedor de serviço de Cloud?*
8.	*SEGURANÇA – INTEGRAÇÃO DO SERVIÇO DE CHAVES CRIPTOGRÁFICAS:* *O serviço de gestão de chaves do fornecedor de Cloud se integra a outros serviços na Cloud para fornecer capacidade de criptografia de dados em repouso?*
9.	*SEGURANÇA – HSM:* *O fornecedor de Cloud oferece módulos de segurança de hardware (HSM), ou seja, dispositivos de hardware que oferecem armazenamento de chaves e operações de criptografia seguras dentro de um módulo de hardware resistente à adulteração?*
10.	*SEGURANÇA – DURABILIDADE DE CHAVES CRIPTOGRÁFICAS:* *O fornecedor de Cloud oferece suporte à durabilidade de chaves, incluindo armazenamento de várias cópias para que as chaves estejam disponíveis sempre que for necessário?*
11.	*SEGURANÇA – SSO:* *O fornecedor de Cloud oferece um serviço de login único (SSO) gerido que permite aos utilizadores gerir de forma centralizada o acesso a várias contas e aplicaçõess comerciais?*
12.	*SEGURANÇA – CERTIFICADOS:* *O fornecedor de Cloud oferece um serviço gerido para provisionar, gerir e implantar certificados Secure Sockets Layer (SSL)/Transport Layer Security (TLS)?*
13.	*SEGURANÇA – RENOVAÇÃO DE CERTIFICADOS:* *O serviço de gestão de certificados do fornecedor de Cloud facilita a renovação de certificados?*
14.	*SEGURANÇA – CERTIFICADOS CURINGA:* *O serviço de gestão de certificados do fornecedor de Cloud oferece suporte ao uso de certificados curinga?*
15.	*SEGURANÇA – AUTORIDADE CERTIFICADORA:* *O serviço de gestão de certificados do fornecedor de Cloud também atua como uma autoridade certificadora (AC)?*
16.	*SEGURANÇA – ACTIVE DIRECTORY:* *O fornecedor de Cloud oferece um serviço gerido de Active Directory (AD) da Microsoft na Cloud?*
17.	*SEGURANÇA – ACTIVE DIRECTORY NO LOCAL:* *O serviço gerido de Active Directory (AD) da Microsoft do fornecedor de Cloud oferece suporte à integração com o Active Directory (AD) da Microsoft no local?*
18.	*SEGURANÇA – LADP:* *O serviço gerido de Active Directory (AD) da Microsoft do fornecedor de Cloud oferece suporte ao Lightweight Directory Access Protocol (LDAP)?*

19.	***SEGURANÇA – ACTIVE DIRECTORY:*** *O serviço gerido de Active Directory (AD) da Microsoft do fornecedor de Cloud oferece suporte à Security Assertion Markup Language (SAML)?*
20.	***SEGURANÇA – GESTÃO DE CREDENCIAIS:*** *O fornecedor de Cloud oferece um serviço gerido que ajuda os utilizadores a rotacionar, gerir e recuperar credenciais, como chaves da interface de programação de aplicações (API), credenciais de base de dados e outros segredos facilmente?*
21.	***SEGURANÇA – WAF:*** *O fornecedor de Cloud oferece um firewall de aplicações Web (WAF) que ajuda a proteger aplicações Web contra explorações comuns na Web que poderiam afetar a disponibilidade da aplicação, comprometer a segurança ou consumir recursos em excesso?*
22.	***SEGURANÇA – DDOS:*** *O fornecedor de Cloud oferece um serviço para proteger contra ataques comuns e frequentes da rede e de negação distribuída de serviço (DDoS) da camada de transporte, junto com a capacidade de gravar regras personalizadas para mitigar ataques sofisticados da camada de aplicação?*
23.	***SEGURANÇA – RECOMENDAÇÕES DE SEGURANÇA:*** *O fornecedor de Cloud oferece um serviço para avaliar automaticamente vulnerabilidades potenciais em aplicações e recursos?*
24.	***SEGURANÇA – DETECÇÃO DE AMEAÇAS:*** *O fornecedor de Cloud oferece um serviço gerido de detecção de ameaças?*
25.	***SEGURANÇA – LIMITES DE SERVIÇO:*** *O fornecedor de Cloud possui alguma restrição (ou seja, limites de serviço) em relação à seção de segurança acima?* *Exemplo:* *Número máximo de chaves mestras do cliente* *Número máximo de módulos de segurança de hardware (HSMs)*

6. Conformidade

A lista abaixo serve apenas para fins ilustrativos e não deve ser considerada uma relação completa das certificações e padrões que podem se aplicar aos Serviços de Cloud.

Indique qual conjunto de padrões de conformidade internacionais e específicos do setor o fornecedor de Cloud atende:

Certificações/Declarações	***Leis, regulamentos e privacidade***	***Alinhamentos/Estruturas***
☐ C5 [Alemanha]	*☐ Diretiva de Proteção de Dados da UE*	*☐ CDSA*
☐ Código de Conduta de Proteção de Dados do CISPE	*☐ Cláusulas Modelo da UE*	
☐ DIACAP	*☐ FERPA*	*☐ CIS*
☐ DoD SRG Níveis 2 e 4	*☐ GDPR*	*☐ Criminal Justice Info. Service (CJIS)*
☐ FedRAMP	*☐ GLBA*	*☐ CSA*

☐ *FIPS 140-2*	☐ *HIPAA*	☐ *Privacy Shield entre UE e EUA*
☐ *HDS (França, Saúde)*	☐ *HITECH*	☐ *EU Safe Harbor*
☐ *ISO 9001*	☐ *IRS 1075*	☐ *FISC*
☐ *ISO 27001*	☐ *ITAR*	☐ *FISMA*
☐ *ISO 27017*	☐ *PDPA – 2010 [Malásia]*	☐ *G-Cloud (Reino Unido)*
☐ *ISO 27018*	☐ *PDPA – 2012 [Singapura]*	☐ *GxP (FDA CFR 21 Parte 11)*
☐ *IRAP [Austrália]*	☐ *PIPEDA [Canadá]*	☐ *ICREA*
☐ *MTCS Nível 3 [Cingapura]*	☐ *Lei da Privacidade [Austrália]*	☐ *IT-Grundschutz [Alemanha]*
☐ *PCI DSS, nível 1*	☐ *Lei da Privacidade [Nova Zelândia]*	☐ *MARS – E*
☐ *Regra 17-a-4 (f) da SEC*	☐ *Autorização da DPA da Espanha*	☐ *MITA 3.0*
☐ *SOC1 / ISAE 3402*	☐ *Reino Unido DPA - 1988*	☐ *MPAA*
☐ *SOC2 / SOC3*	☐ *VPAT/Seção 508*	☐ *NIST*
		☐ *Níveis do Uptime Institute*
		☐ *Princípios de segurança em Cloud do Reino Unido*

Usar os relatórios de conformidade acima permite que as organizações do setor público avaliem as ofertas exclusivas em relação ao padrão aceite de segurança, conformidade e operação. Esses relatórios podem mostrar que o CISP, por meio de sua conformidade, atende aos controles de operação do data center abaixo, que são exigidos do fornecedor de Serviços de Cloud pública. Exigir conformidade com esses relatórios ajuda as entidades do setor público a garantir que os controles abaixo estejam implementados.

- ***Acesso verificado:*** *o CISP deve restringir o acesso físico a pessoas que precisam estar no local por motivo profissional justificável. Se o acesso for concedido, deverá ser revogado assim que o trabalho necessário estiver concluído.*
- ***Entrada controlada e monitorada:*** *a entrada em um nível do data center do perímetro deve ser um processo controlado. O CISP deve ter segurança no portão de entrada e encarregar supervisores para monitorar funcionários e visitantes pelas câmeras de segurança. Quando for aprovada a permanência de indivíduos no local, eles deverão receber um crachá que exija autenticação de vários fatores e limite o acesso às áreas pré-aprovadas.*
- ***Profissionais do data center do CISP:*** *funcionários do CISP que precisam de acesso diário a um data center devem receber as permissões às áreas relevantes do local com base no cargo, com acesso regularmente verificado. As listas de funcionários devem ser conferidas diariamente por um gerente de acesso da área para garantir que a autorização de cada funcionário ainda seja necessária. Se um funcionário não tiver a necessidade profissional de estar em um data center, deverá passar pelo processo de visitante.*
- ***Monitoramento para entrada não autorizada:*** *os CISPs devem monitorar continuamente a entrada não autorizada na propriedade do data center, usando vigilância por vídeo, detecção de invasões e sistemas de monitoramento de registro de acesso. As entradas devem estar protegidas por dispositivos que disparam alarmes caso uma porta seja arrombada ou mantida aberta.*

- ***Segurança global monitorada pelos Centros de operações de segurança do CISP:*** *os Centros de operações de segurança do CISP devem estar localizados no mundo todo com a responsabilidade de monitorar, triar e executar programas de segurança para data centers do CISP. Eles devem supervisionar a gestão de acesso físico e a resposta a detecções de invasão, ainda oferecendo suporte global, 24/7, para as equipes de segurança do data center local. Devem ser responsáveis pelas atividades de monitoramento contínuo, como rastrear atividades de acesso, revogar permissões de acesso e se prontificar a responder e analisar possíveis incidentes à segurança.*

- ***Análise de acesso por nível:*** *o acesso ao Nível da infraestrutura deve ser restrito com base na necessidade da empresa. Com a implementação da análise de acesso por nível, o direito de aceder cada nível não é concedido por padrão. O acesso a determinado nível deve ser concedido somente quando há necessidade específica.*

- ***A manutenção dos equipamentos faz parte das operações regulares:*** *as equipes do CISP devem executar diagnósticos em máquinas, redes e equipamentos de backup para que estejam funcionando hoje e no caso de emergência. Verificações de manutenção de rotina nos equipamentos do data center devem fazer parte das operações regulares do data center do CISP.*

- ***Equipamentos de backup disponíveis para emergência:*** *água, energia, telecomunicações e conexão com a internet devem ser projetadas com redundância para que o CISP mantenha operações contínuas em caso de emergência. Os sistemas de energia elétrica devem ser projetados com redundância total para que, em caso de falta, unidades de no-break estejam prontas para certas funções, enquanto os geradores alimentam todo o local. Pessoas e sistemas devem monitorar e controlar a temperatura e a umidade para evitar superaquecimento, reduzindo possíveis falhas no serviço.*

- ***Tecnologias e pessoas trabalham juntas para que haja mais segurança:*** *deve haver procedimentos obrigatórios para que se obtenha a autorização de acesso ao Nível dos dados. Isso inclui análise e aprovação de uma possível entrada de indivíduos autorizados. Enquanto isso, sistemas eletrônicos de detecção de ameaças e invasões devem monitorar ameaças identificadas ou atividades suspeitas e disparar alarmes. Por exemplo, se uma porta for arrombada ou mantida aberta, um alarme será disparado. O CISP deve implantar câmeras de segurança e guardar os vídeos gravados de acordo com os requisitos legais e de conformidade.*

- ***Impedir invasões física e tecnológica:*** *pontos de acesso para salas de servidor devem ser reforçadas com dispositivos de controle eletrônico que exigem autorização de vários fatores. O CISP também deve se preparar para evitar a invasão tecnológica. Os servidores do CISP devem ter a capacidade de alertar os funcionários sobre quaisquer tentativas de remoção de dados. No improvável caso de violação, o servidor deve ser desativado automaticamente.*

- ***Servidores e mídias recebem atenção imediata:*** *os dispositivos de armazenamento de mídia usados para armazenar dados dos clientes devem ser classificados pelo CISP como Críticos e tratados dessa maneira, de alto impacto, durante toda a sua vida útil. O CISP deve contar com padrões imediatos sobre como instalar, reparar e até destruir os dispositivos quando deixam de ser úteis. Quando um dispositivo de armazenamento chega ao fim de sua vida útil, o CISP deve suspender a mídia usando as técnicas dispostas no NIST 800-88. Mídias que armazenam dados dos clientes não são removidas do controle do CISP até que sejam seguramente suspendidas.*

- ***Auditores de terceiros conferem procedimentos e sistemas do CISP:*** *o CISP deve ser auditado por auditores externos para inspecionar data centers e confirmar se o CISP está seguindo as regras estabelecidas necessárias para obter suas certificações de segurança. Dependendo do programa de conformidade e seus requisitos, os auditores externos podem questionar funcionários do CISP a respeito de como eles manipulam e descartam mídias. Os auditores também podem assistir a gravações da câmera de segurança e observar entradas e corredores em um data center. E podem examinar equipamentos, como dispositivos de controle de acesso eletrônico e câmeras de segurança do CISP.*

- ***Preparado para inesperado:*** *o CISP deve se preparar de uma maneira proativa para possíveis ameaças ambientais, como desastres naturais e incêndios. Instalar sensores automáticos e equipamentos de resposta são duas maneiras de o CISP proteger seus data centers. Dispositivos de detecção de água devem ser instalados para alertar os funcionários quanto a problemas, enquanto as bombas automáticas removem líquidos e evitam danos. Da mesma forma, equipamentos de detecção e supressão automáticas de incêndio reduzem riscos e podem notificar funcionários do CISP e bombeiros sobre um problema.*

- ***Alta disponibilidade por meio de diversas zonas de disponibilidade:*** *o CISP deve fornecer diversas Zonas de disponibilidade para mais tolerância a falhas. Cada Zona de disponibilidade deve consistir em um ou mais data centers, estar fisicamente separada da outra e ter energia e rede redundantes. As Zonas de disponibilidade devem estar conectadas entre si com rede de fibra óptica rápida e privada para arquitetar aplicações que tenham failover automático entre as Zonas de disponibilidade sem interrupção.*

- ***Simular interrupções e medir a resposta****: o CISP deve contar com um plano de continuidade dos negócios como um guia de processo de operações que descreve como evitar e reduzir interrupções devidas a desastres naturais, com etapas detalhadas a realizar antes, durante e depois de um evento. Para atenuar e se preparar para o inesperado, o CISP deve testar regularmente o plano de continuidade dos negócios com exercícios que simulam diferentes cenários. O CISP deve documentar como as suas pessoas e processos se desempenham, depois resumir as lições aprendidas e as ações corretivas que possam ser necessárias para melhorar a taxa de resposta. Os funcionários do CISP devem ser treinados e estar prontos para* se recuperar rapidamente *das paradas, com um processo de recuperação metódico para minimizar outras paradas devido a erros.*

- ***Ajudar a atingir metas de eficiência:*** *além de tratar riscos ambientais, o CISP também deve incorporar considerações de sustentabilidade em seu projeto de data center. O CISP deve fornecer detalhes de seu comprometimento de usar energia renovável para seus data centers e fornecer informações sobre como seus clientes podem reduzir emissões de carbono em seus próprios data centers.*

- ***Seleção de local****: antes de escolher um local, o CISP deve fazer avaliações ambientais e geográficas iniciais. Os locais do data center devem ser selecionados atentamente para reduzir riscos ambientais, como inundações, intempéries e abalos sísmicos. As Zonas de disponibilidade do CISP devem ser criadas para serem independentes e fisicamente separadas umas das outras.*

- ***Redundância:*** *os data centers devem ser projetados para antecipar e tolerar falhas sem deixar de manter os níveis do serviço. Em caso de falha, processos automatizados desviam o tráfego de dados do cliente da área afetada. As principais aplicações são implantados em uma configuração N + 1, para que no caso de uma falha do data center, haja capacidade suficiente para permitir que o tráfego seja balanceado para os locais restantes.*

- ***Disponibilidade:*** *o CISP deve identificar componentes críticos do sistema necessários para manter a disponibilidade de seu sistema e recuperar o serviço no caso de parada. Componentes críticos do sistema devem ser copiados entre diversos locais isolados. Cada local ou Zona de disponibilidade deve ser projetada para operar de forma independente com alta confiabilidade. As Zonas de disponibilidade devem ser conectadas para que as aplicações façam failover entre as Zonas de disponibilidade sem interrupção. Sistemas altamente resilientes e, portanto, a disponibilidade do serviço, devem ser funções do projeto do sistema. O projeto do data center com Zonas de disponibilidade e replicação de dados permite que os clientes do CISP atinjam um tempo de recuperação extremamente curto e objetivos do ponto de recuperação, além dos mais altos níveis de disponibilidade do serviço.*

- ***Planeamento de capacidade****: o CISP deve estar sempre monitorando o uso do serviço para implantar a infraestrutura e ajudar nos compromissos e requisitos de disponibilidade. O CISP deve manter um modelo de planeamento de capacidade que avalie o uso da infraestrutura do CISP e as demandas pelo menos a cada mês. Este modelo deve ajudar no planeamento de futuras demandas e incluir considerações, como processamento de informações, telecomunicações e armazenamento de logs de auditoria.*

CONTINUIDADE DOS NEGÓCIOS e RECUPERAÇÃO DE DESASTRES

- ***Plano de continuidade dos negócios:*** *o Plano de continuidade dos negócios do CISP deve descrever medidas para evitar e reduzir interrupções ambientais. Deve incluir detalhes operacionais sobre as etapas a adotar antes, durante e depois de um evento. O Plano de continuidade dos negócios deve ser respaldado por testes que incluam simulações de diferentes cenários. Durante e após os testes, o CISP deve documentar o desempenho de pessoas e processos, as ações corretivas e as lições aprendidas com o intuito de obter melhorias contínuas.*

- ***Resposta pandêmica:*** *o CISP deve incorporar políticas e procedimentos de respostas pandêmicas no planeamento de recuperação de desastres para se preparar para responder com rapidez a ameaças de doenças infecciosas. Estratégias de atenuação incluem modelos alternativos de funcionários para transferir processos críticos para recursos fora da região e ativação de um plano de gestão de crises para ajudar nas operações corporativas mais importantes. Planos pandêmicos devem ter como referência agências e regulamentações de saúde internacionais, incluindo pontos de contato de agências no exterior.*

MONITORAMENTO e REGISTRO

- ***Análise de acesso ao data center:*** *o acesso aos data centers deve ser sempre analisado. O acesso também é automaticamente revogado quando o registro de um funcionário é encerrado no sistema de recursos humanos do CISP.*

Além disso, quando o acesso de um funcionário ou contratado expira após a duração da solicitação aprovada, seu acesso deve ser revogado mesmo que ele continue sendo funcionário do CISP.

- ***Registros de acesso ao data center**: o acesso físico aos data centers do CISP deve ser registrado, monitorado e mantido. O CISP deve correlacionar as informações obtidas dos sistemas de monitoramento lógico e físico para melhorar a segurança conforme a necessidade.*

- ***Monitoramento de acesso ao data center:** o CISP deve monitorar os data centers usando Centros de operações de segurança globais, responsáveis por monitorar, triar e executar programas de segurança. Eles devem fornecer suporte 24/7 global ao gerir e monitorar atividades de acesso ao data center, equipar equipes locais e outras equipes de suporte para responder aos incidentes de segurança com a triagem, análise e envio de respostas.*

VIGILÂNCIA e DETECÇÃO

- ***CCTV:** os pontos de acesso físico às salas de servidores devem ser registrados por CCTV (Câmeras de televisão em circuito fechado). As imagens devem ser mantidas conforme os requisitos legais e de conformidade.*

- ***Pontos de entrada do data center:** o acesso físico deve ser controlado em pontos de entrada do edifício por uma equipe de segurança profissional utilizando vigilância por vídeo, sistemas de detecção de intrusos e outros meios eletrônicos. Funcionários autorizados devem usar mecanismos de autenticação de vários fatores para aceder aos data centers. As entradas às salas de servidor devem ser protegidas com dispositivos que disparam alarmes para iniciar uma resposta a incidente caso a porta seja arrombada ou mantida aberta.*

- ***Detecção de invasões:** sistemas eletrônicos de detecção de invasões devem ser instalados no nível dos dados para monitorar, detectar e automaticamente alertar os funcionários apropriados sobre os incidentes de segurança. Os pontos de entrada e saída às salas de servidores devem ser protegidos com dispositivos que exijam aos indivíduos autenticação de vários fatores antes de entrar ou sair. Esses dispositivos disparam alarmes caso a porta seja arrombada sem autenticação ou mantida aberta. Os dispositivos de alarmes das portas também devem ser configurados para detectar instâncias em que um indivíduo sai ou entra no nível dos dados sem fornecer autenticação de vários fatores. Os alarmes devem ser imediatamente encaminhados aos Centros de operações de segurança do CISP em 24/7 para registro, análise e resposta imediatos.*

GESTÃO DE DISPOSITIVOS

- ***Gestão de ativos:** os ativos do CISP devem ser geridos de forma centralizada por meio de um sistema de gestão de inventário que armazena e rastreia informações sobre proprietário, local, status, manutenção e descrição. Depois da aquisição, os ativos devem ser verificados e rastreados, e os ativos que passam por manutenção devem ser verificados e monitorados para que se saibam a propriedade, o status e a resolução.*

- ***Destruição de mídias:** os dispositivos de armazenamento de mídia usados para armazenar dados dos clientes devem ser classificados pelo CISP como Críticos e tratados dessa maneira, de alto impacto, durante toda a sua vida útil. O CISP deve contar com padrões imediatos sobre como instalar, reparar e até destruir os dispositivos quando deixam de ser úteis. Quando um dispositivo de armazenamento chega ao fim de sua vida útil, o CISP deve suspender a mídia usando as técnicas dispostas no NIST 800-88. Mídias que armazenam dados dos clientes não devem ser removidas do controle do CISP até que sejam seguramente descomissionadas.*

SISTEMAS DE SUPORTE OPERATIVO

- ***Energia:** os sistemas de energia elétrica do data center do CISP são projetados para serem totalmente redundantes e passíveis de manutenção sem impacto para as operações, 24 horas por dia. O CISP deve garantir que os data centers sejam equipados com alimentação reserva para que haja energia para manter as operações no caso de uma pane elétrica de cargas críticas e essenciais no local.*

- ***Clima e temperatura:** os data centers do CISP devem usar mecanismos para controlar o clima e manter uma temperatura de operação apropriada para servidores e outros tipos de hardware para evitar superaquecimento e reduzir a possibilidade de falhas no serviço. Funcionários e sistemas monitoram e controlam a temperatura e a umidade em níveis adequados.*

- ***Detecção e supressão de incêndio**: os data centers do CISP devem ser equipados com sistemas de detecção e supressão de incêndio automáticos. Os sistemas de detecção de incêndio devem usar sensores de detecção de fumaça dentro dos espaços da rede, mecânica e infraestrutura. Essas áreas devem ser protegidas pelos sistemas de supressão.*

- ***Detecção de vazamento:** para detectar a presença de vazamento de água, o CISP deve equipar os data centers com funcionalidades para detectar a presença de água. Se a água for detectada, os mecanismos deverão removê-la para evitar outros danos.*

MANUTENÇÃO DA INFRAESTRUTURA

- ***Manutenção dos equipamentos**: o CISP deve monitorar e fazer a manutenção preventiva de equipamentos de mecanismos elétricos e mecânicos para manter a operabilidade continuada dos sistemas dentro dos data centers do CISP. Os procedimentos de manutenção de equipamentos devem ser realizados por profissionais qualificados e conforme uma programação de manutenção documentada.*

- ***Gestão do ambiente:** o CISP deve monitorar sistemas e equipamentos elétricos e mecânicos para possibilitar a identificação imediata de problemas. Isso deve acontecer com a utilização de ferramentas e auditoria contínuas e informações fornecidas pelos Sistemas de administração predial e monitoramento elétrico do CISP. A manutenção preventiva é executada para manter a operacionalidade contínua dos equipamentos.*

GOVERNAÇÃO E RISCOS

- ***Gestão de riscos contínuos do data center:** o Centro de operações de segurança do CISP deve fazer análises regulares e ameaças e vulnerabilidades dos data centers. A avaliação contínua e a atenuação de possíveis vulnerabilidades devem ser realizadas por atividades de avaliação de riscos do data center. Essa avaliação deve acontecer além do processo de avaliação de risco empresarial já usado para identificar e gerir riscos para a empresa de forma geral. Esse processo também deve levar em conta riscos regulatórios e ambientais.*

- ***Atestado de segurança de terceiros:** os testes de terceiros dos data centers do CISP, conforme documentado nos relatórios de terceiros, devem garantir que o CISP tenha medidas de segurança adequadamente implementadas em alinhamento com as regras estabelecidas, necessárias para obter certificações de segurança. Dependendo do programa de conformidade e seus requisitos, os auditores externos podem realizar testes de descarte de mídia, ver gravações da câmera de segurança, observar entradas e corredores de um data center, testar dispositivos de controle de acesso eletrônico e examinar equipamentos do data center.*

7. Migrações

	Requisito
1.	***SERVIÇO DE MIGRAÇÕES:*** *Quantos serviços de migração de dados diferentes o fornecedor de Cloud oferece?*
2.	***MIGRAÇÕES – MONITORAMENTO CENTRALIZADO:*** *O fornecedor de Cloud oferece às organizações um serviço centralizado (ou seja, um único painel de vidro), onde elas podem rastrear e monitorar o status de suas migrações de servidor e aplicação?*
3.	***MIGRAÇÕES – PAINEL:*** *A ferramenta de migração do fornecedor de Cloud oferece um painel para visualizar rapidamente o status da migração, as métricas relacionadas e o histórico de migração?*
4.	***MIGRAÇÕES – FERRAMENTAS DO FORNECEDOR DE CLOUD:*** *A ferramenta de migração do fornecedor de Cloud oferece integração com outras ferramentas de migração do fornecedor de Cloud que podem realizar migrações de servidores e aplicações?*
5.	***MIGRAÇÕES – FERRAMENTAS DE TERCEIROS:*** *A ferramenta de migração do fornecedor de Cloud permite incorporar ferramentas de migração de terceiros?* • *Se sim, quais são as ferramentas de migração de terceiros compatíveis?*

6.	*MIGRAÇÕES – MIGRAÇÕES EM VÁRIAS REGIÕES:* *A ferramenta de migração do fornecedor de Cloud oferece recursos de rastreamento e monitoramento para migrações de servidores e aplicações que acontecem em diferentes regiões?*
7.	*MIGRAÇÕES – MIGRAÇÃO DO SERVIDOR:* *A ferramenta de migração do fornecedor de Cloud oferece uma maneira de migrar servidores virtualizados locais para a Cloud?* • *Se sim, quais ambientes virtualizados são compatíveis no momento?*
8.	*MIGRAÇÕES – DESCOBERTA DE SERVIDOR:* *A ferramenta de migração do fornecedor de Cloud oferece recursos de descoberta para encontrar automaticamente servidores virtuais no local a serem migrados para a Cloud?*
9.	*MIGRAÇÕES – DADOS DE DESEMPENHO DO SERVIDOR:* *A ferramenta de migração do fornecedor de Cloud oferece o recurso de coletar e exibir o desempenho do servidor e/ou da máquina virtual, como a utilização da CPU e da memória de acesso aleatório (RAM)?*
10.	*MIGRAÇÕES – BASE DE DADOS DE DESCOBERTA:* *A ferramenta de migração do fornecedor de Cloud oferece a possibilidade de armazenar todos os dados coletados em uma base de dados centralizada?* • *Se sim, as organizações podem exportar esses dados? Para quais formatos?*
11.	*MIGRAÇÕES – CRIPTOGRAFIA EM REPOUSO:* *O fornecedor de Cloud criptografa em repouso todas as informações coletadas e armazenadas na base de dados de descoberta?*
12.	*MIGRAÇÕES – REPLICAÇÃO DE SERVIDOR INCREMENTAL:* *A ferramenta de migração do fornecedor de Cloud oferece replicação de servidor incremental, automatizada e dinâmica durante a migração do servidor ou da máquina virtual, como forma de oferecer suporte a todas as alterações feitas no servidor ou na máquina virtual, incluídas na imagem migrada final?* • *Se sim, por quanto tempo esse serviço pode ser executado?*
13.	*MIGRAÇÕES – VMWARE:* *A ferramenta de migração do fornecedor de Cloud oferece suporte às migrações de máquinas virtuais VMWare no local para a Cloud?*
14.	*MIGRAÇÕES – HYPER-V:* *A ferramenta de migração do fornecedor de Cloud oferece suporte às migrações de máquinas virtuais Hyper-V no local para a Cloud?*
15.	*MIGRAÇÕES – DESCOBERTA DE APLICAÇÕES:* *A ferramenta de migração do fornecedor de Cloud oferece a possibilidade de descobrir e agrupar aplicações antes de serem migrados?*
16.	*MIGRAÇÕES – MAPEAMENTO DE DEPENDÊNCIA:* *A ferramenta de migração do fornecedor de Cloud oferece a possibilidade de descobrir dependências entre servidores e aplicações antes de serem migrados?*
17.	*MIGRAÇÕES – MIGRAÇÃO DE BASE DE DADOS:* *A ferramenta de migração do fornecedor de Cloud oferece o recurso de migrar bancos de dados locais para a Cloud?*
18.	*MIGRAÇÕES – TEMPO DE INATIVIDADE DA MIGRAÇÃO DE BASE DE DADOS:*

	A ferramenta de migração do fornecedor de Cloud oferece o recurso de realizar uma migração de base de dados para a Cloud com tempo de inatividade mínimo, ou seja, a base de dados de origem deve permanecer totalmente operacional durante o processo de migração?
19.	*MIGRAÇÕES – BASE DE DADOS DE ORIGEM:* *A ferramenta de migração do fornecedor de Cloud oferece suporte à migração de diferentes origens de base de dados, como Oracle, SQL Server, etc.?* • *Se sim, liste todos os bancos de dados de origem compatíveis que podem ser migrados para a Cloud.*
20.	*MIGRAÇÕES – MIGRAÇÕES HETEROGÊNEAS:* *A ferramenta de migração do fornecedor de Cloud oferece o recurso de realizar migrações de base de dados heterogêneas, ou seja, de uma base de dados de origem para uma base de dados de destino diferente, como do Oracle para o SQL Server?* • *Se sim, liste todas as combinações de migração de base de dados heterogêneas possíveis.*
21.	*MIGRAÇÕES – MIGRAÇÃO DE DADOS EM ESCALA DE PETABYTES:* *O fornecedor de Cloud oferece uma solução de transporte de dados em escala de petabytes que usa dispositivos seguros para transferir grandes quantidades de dados para dentro e para fora da Cloud.*
22.	*MIGRAÇÕES – MIGRAÇÃO DE DADOS EM ESCALA DE EXABYTES:* *O fornecedor de Cloud oferece uma solução de transporte de dados em escala de exabytes para mover quantidades extremamente grandes de dados para a Cloud?*
23.	*MIGRAÇÕES – BACKUPS CORPORATIVOS:* *O fornecedor de Cloud oferece um serviço para integrar perfeitamente o data center de um cliente a serviços de armazenamento na Cloud que permitirão transferir e armazenar dados no serviço de armazenamento do fornecedor de Cloud?*
24.	*MIGRAÇÕES – BACKUPS CORPORATIVOS – ARMAZENAMENTO DE OBJETOS:* *O serviço de backup corporativo do fornecedor de Cloud oferece integração com o serviço de armazenamento de objetos na Cloud do fornecedor?*
25.	*MIGRAÇÕES – BACKUPS CORPORATIVOS – ACESSO A ARQUIVOS:* *O serviço de backup corporativo do fornecedor de Cloud permite que os utilizadores armazenem e recuperem objetos usando protocolos de arquivos, como o protocolo do sistema de arquivos de rede (NFS)?*
26.	*MIGRAÇÕES – BACKUPS CORPORATIVOS – ACESSO A BLOCOS:* *O serviço de backup corporativo do fornecedor de Cloud permite que os utilizadores armazenem e recuperem objetos usando protocolos de blocos como o protocolo iSCSI?*
27.	*MIGRAÇÕES – BACKUPS CORPORATIVOS – ACESSO A BANDAS:* *O serviço de backup corporativo do fornecedor de Cloud permite que os utilizadores façam backup de seus dados por meio de uma biblioteca de bandas virtuais e armazenem esses backups em banda na Cloud do fornecedor?*
28.	*MIGRAÇÕES – BACKUPS CORPORATIVOS – CRIPTOGRAFIA:* *O serviço de backup corporativo do fornecedor de Cloud oferece criptografia de dados em repouso e em trânsito?*
29.	*MIGRAÇÕES – BACKUPS CORPORATIVOS – INTEGRAÇÃO DE SOFTWARE DE TERCEIROS:* *O serviço de backup corporativo do fornecedor de Cloud se integra ao software de backup de terceiros normalmente usado?*
30.	*MIGRAÇÕES – LIMITES DE SERVIÇO:* *O fornecedor de Cloud possui alguma restrição (ou seja, limites de serviço) em relação à seção de migrações?* *Exemplo:*

	Número máximo de migrações simultâneas de máquinas virtuais *Número máximo de solicitações de soluções de transporte de dados*

8. Faturação

	Requisito
1.	***FATURAÇÃO – ACOMPANHAMENTO E RELATÓRIOS:*** *O fornecedor de Cloud oferece um serviço de rastreamento e relatórios do faturação para ajudar os utilizadores a gerir e monitorar o uso das ofertas de Cloud?*
2.	***FATURAÇÃO – ALARMES E NOTIFICAÇÕES:*** *O fornecedor de Cloud oferece aos utilizadores um mecanismo para configurar alarmes com notificações para alertá-los quando seus gastos ultrapassarem um limite específico?*
3.	***FATURAÇÃO – GESTÃO DE CUSTOS:*** *O fornecedor de Cloud oferece um mecanismo para criar e exibir gráficos que resumem os custos e os gastos?*
4.	***FATURAÇÃO – ORÇAMENTOS:*** *O fornecedor de Cloud oferece um mecanismo para exibir e gerir orçamentos e prever os custos estimados?*
5.	***FATURAÇÃO – VISUALIZAÇÃO CONSOLIDADA:*** *O fornecedor de Cloud oferece um mecanismo para consolidar a faturação de várias contas em uma única conta de pagamento primária?*
6.	***FATURAÇÃO – LIMITES DE SERVIÇO:*** *O fornecedor de Cloud possui alguma restrição (ou seja, limites de serviço) em relação à seção de faturação acima?* *Exemplo:* *Número máximo de contas que podem ser agrupadas juntas* *Número máximo de alarmes que podem ser criados* *Número máximo de orçamentos que podem ser geridos*

9. Gestão

	Requisito
1.	***GESTÃO – SERVIÇO DE MONITORAMENTO:*** *O fornecedor de Cloud oferece um serviço de monitoramento para gerir os recursos e as aplicações da Cloud, que coleta, monitora e relata usando métricas pré-definidas?*
2.	***GESTÃO – ALARMES:*** *O serviço de monitoramento do fornecedor de Cloud permite que os utilizadores definam alarmes?*
3.	***GESTÃO – MÉTRICAS PERSONALIZADAS:*** *O serviço de monitoramento do fornecedor de Cloud permite que os utilizadores criem e monitorem métricas personalizadas?*
4.	***GESTÃO – GRANULARIDADE DO MONITORAMENTO:*** *O serviço de monitoramento do fornecedor de Cloud oferece vários níveis de granularidade de monitoramento, até o nível de 1 minuto?*

5.	***GESTÃO – SERVIÇO DE RASTREAMENTO DE API:*** *O fornecedor de Cloud oferece um serviço que registra em log, monitora e armazena atividades em recursos da Cloud, em nível da consola e da interface de programação de aplicações (API), para melhorar a visibilidade?* • *Se sim, quais são os serviços do fornecedor de Cloud que se integram a esse serviço de rastreamento?*
6.	***GESTÃO – NOTIFICAÇÃO:*** *O fornecedor de Cloud habilita a capacidade de envio de notificações com base nos níveis de atividade da interface de programação de aplicações (API)?*
7.	***GESTÃO – COMPACTAÇÃO:*** *O fornecedor de Cloud oferece um mecanismo para compactar logs gerados pelo sistema de rastreamento da interface de programação de aplicações (API), com o objetivo de ajudar os utilizadores a reduzirem os custos de armazenamento associados a esse serviço?*
8.	***GESTÃO – AGREGAÇÃO DE REGIÕES:*** *O fornecedor de Cloud oferece a capacidade de registrar a atividade da interface de programação de aplicações (API) da conta em todas as regiões e entregar essas informações de forma agregada para facilitar o uso?*
9.	***GESTÃO – INVENTÁRIO DE RECURSOS:*** *O fornecedor de Cloud oferece um serviço para avaliar, auditar e analisar as configurações dos recursos implantados por um utilizador?*
10.	***GESTÃO – ALTERAÇÕES DE CONFIGURAÇÃO:*** *O fornecedor de Cloud registra automaticamente uma alteração na configuração de um recurso quando ela acontece?*
11.	***GESTÃO – HISTÓRICO DE CONFIGURAÇÕES:*** *O fornecedor de Cloud oferece a capacidade de examinar a configuração de recursos em qualquer ponto único anterior?*
12.	***GESTÃO – REGRAS DE CONFIGURAÇÃO:*** *O fornecedor de Cloud oferece diretrizes e recomendações para provisionar, configurar e monitorar continuamente a conformidade?*
13.	***GESTÃO – MODELOS DE RECURSOS:*** *O fornecedor de Cloud oferece aos utilizadores a capacidade de criar, provisionar e gerir um conjunto de recursos usando modelos?*
14.	***GESTÃO – REPLICAÇÃO DE MODELOS DE RECURSOS:*** *O fornecedor de Cloud oferece a capacidade de replicar rapidamente esses modelos de recursos entre regiões diferentes para o uso potencial em situações de recuperação de desastres (DR)?*
15.	***GESTÃO – DESIGNER DE MODELOS:*** *O fornecedor de Cloud oferece uma ferramenta gráfica fácil de usar com funcionalidade arrastar e soltar que acelera o processo de criação desses modelos de recursos?*
16.	***GESTÃO – CATÁLOGO DE SERVIÇOS:*** *O fornecedor de Cloud oferece um serviço para criar e gerir um catálogo de serviços, isto é, servidores, máquinas virtuais, software, bancos de dados, etc.?*
17.	***GESTÃO – ACESSO À CONSOLA:*** *O fornecedor de Cloud oferece uma interface de utilizador baseada na Web para facilitar a gestão e o monitoramento dos serviços na Cloud?*
18.	***GESTÃO – ACESSO À CLI:***

	O fornecedor de Cloud oferece uma ferramenta unificada para gerir e configurar vários serviços na Cloud a partir da interface da linha de comando (CLI) e permitir a automação de tarefas de gestão por meio do uso de scripts?
19.	***GESTÃO – ACESSO MÓVEL:*** *O fornecedor de Cloud oferece uma aplicação para smartphone a fim de permitir que os utilizadores se conectem ao serviço da Cloud e gerenciem seus recursos?* • *Se sim, essa aplicação está disponível para iOS e Android?*
20.	***GESTÃO – MELHORES PRÁTICAS:*** *O fornecedor de Cloud tem um serviço que ajuda os utilizadores a comparar o uso da Cloud em relação às melhores práticas?*
21.	***GESTÃO – LIMITES DE SERVIÇO:*** *O fornecedor de Cloud possui alguma restrição (ou seja, limites de serviço) em relação à seção de gestão acima?* *Exemplo:* *Número máximo de regras de configuração por conta* *Número máximo de alarmes que podem ser criados* *Número máximo de logs que podem ser armazenados*

10. Suporte

	Requisito
1.	***SUPORTE – SERVIÇO:*** *O fornecedor de Cloud oferece suporte a qualquer hora, 24 horas por dia, 7 dias por semana e 365 dias por ano, por telefone, chat e e-mail?*
2.	***SUPORTE – NÍVEIS DE SUPORTE:*** *O fornecedor de Cloud oferece diferentes níveis de suporte?*
3.	***SUPORTE – ALOCAÇÃO DE NÍVEL:*** *O fornecedor de Cloud permite que os utilizadores atribuam para si próprios os recursos/serviços consumidos a diferentes níveis de suporte com base na classificação granular, e não forçando os utilizadores a manter contas de Cloud separadas para alcançar e receber diferentes níveis de suporte?*
4.	***SUPORTE – FÓRUNS:*** *O fornecedor em Cloud oferece fóruns de suporte públicos para que os clientes discutam seus problemas?*
5.	***SUPORTE – PAINEL DE STATUS DOS SERVIÇOS:*** *O fornecedor de Cloud oferece um painel de status dos serviços que exibe as informações mais recentes sobre a disponibilidade de serviço em várias regiões?*
6.	***SUPORTE – PAINEL PERSONALIZADO:*** *O fornecedor de Cloud oferece um painel que exibe uma visualização personalizada sobre o desempenho e a disponibilidade dos serviços subjacentes aos recursos específicos do utilizador?*
7.	***SUPORTE – HISTÓRICO DE PAINÉIS:*** *O fornecedor de Cloud oferece 365 dias de histórico do painel de status dos serviços?*
8.	***SUPORTE – CONSULTOR DE CLOUD:***

	O fornecedor de Cloud oferece um serviço que atua como um especialista de Cloud personalizado e ajuda a comparar o uso dos recursos em relação às melhores práticas?
9.	*SUPORTE – TAM:* *O fornecedor de Cloud oferece um gerente de conta técnico (Technical Account Manager - TAM) que fornece experiência técnica para uma gama completa de serviços na Cloud?*
10.	*SUPORTE – SUPORTE A APLICAÇÕES DE TERCEIROS:* *O fornecedor de Cloud oferece suporte para sistemas operativos comuns e componentes de aplicações comuns?*
11.	*SUPORTE – API PÚBLICA:* *O fornecedor de Cloud oferece uma interface de programação de aplicações (API) pública que interage de forma programática com casos de suporte para criar, editar e encerrar tais casos?*
12.	*SUPORTE – DOCUMENTAÇÃO DO SERVIÇO:* *O fornecedor de Cloud oferece documentações técnicas de qualidade e publicamente visíveis para todos os seus serviços, incluindo, mas não limitado a, guias do utilizador, tutoriais, perguntas frequentes (FAQs) e notas de release?*
13.	*SUPORTE – DOCUMENTAÇÃO DA CLI:* *O fornecedor de Cloud oferece documentação técnica de qualidade e publicamente visível para sua interface da linha de comando (CLI)?*
14.	*SUPORTE – ARQUITETURAS DE REFERÊNCIA:* *O fornecedor de Cloud oferece um conjunto online gratuito de documentos de arquitetura de referência para ajudar os clientes a criar soluções específicas, combinando diversos serviços na Cloud do fornecedor de Cloud?*
15.	*SUPORTE – IMPLANTAÇÕES DE REFERÊNCIA:* *O fornecedor de Cloud oferece um conjunto de documentos online gratuitos que contêm procedimentos passo a passo detalhados, testados e validados, incluindo melhores práticas, para implementar soluções comuns (por exemplo, DevOps, Big Data, Data Warehouse, cargas de trabalho Microsoft, cargas de trabalho SAP, etc.) em suas ofertas da Cloud?*

Apêndice B - Demo

As demonstrações podem ser uma forma eficiente dos utilizadores finais testarem as ofertas de Cloud e para que a decisão da outorga reflita a opção mais adequada para as necessidades comerciais da organização. Abaixo está um exemplo de script demonstração de teste para tecnologias de Cloud.

1. *Demonstre detalhadamente a consola dos CISPs e as ofertas/recursos disponíveis publicamente:*
    - *Recursos de armazenamento*
    - *Recursos de computação*
    - *Recursos e tipos de bancos de dados*
    - *Redes*
    - *Ferramentas de gestão e análise*
    - *Segurança*
    - *Outros recursos*
2. *Descreva como opera as suas tecnologias de Cloud usadas na demonstração.*
3. *Demonstre como está a executar esta demonstração em tempo real usando a oferta de Cloud.*
4. *Contas:*
    - *Descreva o sistema de chaves da conta (raiz e utilizador) usado na demonstração.*
    - *Demonstre como gestiona e protege as chaves da conta*
5. *Demonstre como pode selecionar o local físico onde suas cargas de trabalho/dados estão armazenadas.*
6. *Demonstre a escala da sua oferta ao projetar soluções de computação e armazenamento de larga escala.*
7. *Ilustre como um utilizador final solicita vários serviços das ofertas de Cloud. Demonstre:*
    - *Como as contas são estabelecidas*
    - *Como as provisões de segurança são habilitadas*
    - *Como as principais contas podem ser divididas em subcontas*
    - *Como a sua Gestão de identidade e acesso (IAM) pode separar o acesso a vários recursos:*
        - *Como proteger uma conta*
        - *Criar utilizadores e grupos*
        - *Anexar a política*
        - *Configurar senhas*
8. *Demonstre como os ambientes virtuais podem ser isolados da perspectiva de segurança e rede:*
    - *Crie subredes*
    - *Roteamento da Internet*
9. *Demonstre como pode criar um ambiente em dois ou mais locais isolados separados.*
    - *Demonstre o balanceamento de carga entre os ambientes.*
10. *Demonstre a capacidade de usar diversos métodos para interagir com os serviços de computação em Cloud (por exemplo, Application Program Interface (API), Consola da Web, linha de comando).*
11. *Armazenamento:*
    - *Descreva opções de armazenamento*
    - *Demonstre os tipos de armazenamento disponíveis (por exemplo, bloco, objeto) e processos de ciclo de vida dos dados*
    - *Estabeleça um volume de armazenamento e demonstre como os dados são carregados e recuperados*
    - *Crie um volume de armazenamento X GB coms e sem opção de computação*
    - *Demonstre e valide permissões para aceder a esses volumes.*
12. *Computação:*
    - *Descreva as opções de computação – tamanho e capacidades dos recursos de computação*
    - *Demonstre a ativação e a desativação de um recurso de computação*

- *Demonstre propriedades (capacidade de iniciar X instâncias ao mesmo tempo, seleção de rede, proteção contra encerramento acidental, locação, etc.)*
- *Demonstre uma opção de computação com o equivalente de X núcleos e X GB de RAM*
- *Demonstre o dimensionamento de recursos baseados em carga ao executar uma carga de trabalho*
- *Demonstre recursos de escalabilidade automática*
- *Demonstre como a computação pode ser parada e retomada depois*
- *Demonstre como a opção de computação pode ter escalabilidade horizontal e vertical e manter configurações*
- *Demonstre como a opção de computação pode ser copiada*
- *Demonstre como configurar grupos de segurança*
- *Descreva quais sistemas operativos estão disponíveis na oferta do CISP*
- *Demonstre um exemplo de instalação de um sistema operativo Linux*
- *Descreva suas capacidades de fornecer imagens para ofertas de computação*
- *Que formatos de imagem você aceita?*
- *Demonstre como você pode carregar e operar uma imagem*
- *Demonstre a computação sem servidor*
- *Demonstre a capacidade de iniciar um cluster de instâncias de computação com preços variáveis baseados em um mercado local*

13. *Base de dados:*
    - *Descreva os recursos da base de dados*
    - *Demonstre os recursos do MySQL, MS SQL Server, Oracle e Postgres*
    - *Demonstre os recursos de Data Warehousing*
    - *Demonstre os recursos de backup desses recursos*
14. *Redes: demonstre opções de rede definidas por software e recursos de gestão de rede*
15. *Gestão e análise*
    - *Descreva os seus recursos de gestão de Cloud e análise*
    - *Demonstre opções de monitoramento*
    - *Demonstre as suas capacidades com o Hadoop Frameworks*
16. *Segurança: demonstre a segurança da rede*
    - *Descreva a sua abordagem quanto à segurança*
    - *Firewalls*
    - *Grupos de segurança*
    - *Gateways*
    - *NACLs*
    - *Logs do sistema*
    - *Criptografia*
    - *Credenciamentos de conformidade disponíveis*
    - *Armazenamento de chaves*
    - *Outros recursos*
17. *Provisionamento: demonstre como é capaz de criar uma coleção de recursos de Cloud relacionados e provisioná-los de forma ordenada e previsível, usando um modelo reutilizável*
18. *Software: demonstre as suas capacidades para aceder e usar softwares utilizados com mais frequência*
19. *Demonstre como pode conduzir uma transferência de dados de larga escala*
20. *Demonstre opções de faturação, incluindo:*
    - *Vista resumida, vista granular, vista por recursos marcados*
    - *Despesas/uso previstos com base em despesas/uso atuais*
21. *Demonstre os recursos de suporte e consultoria disponíveis*
    - *Quais as opções de suporte disponíveis*

- *Existem recursos para fornecer verificações e orientações sobre o uso do serviço?*

Demonstre outros recursos da oferta que considere sejam diferenciadores.