Aquisição de serviços de cloud no setor público

Manual com exemplos de linguagem de pedido de proposta (RFP) para um acordo-quadro de cloud

Versão 2: fevereiro de 2022

Avisos

Este documento destina-se apenas a fins informativos. Não foi desenvolvido em conformidade com os requisitos legais para processos de contratação pública numa determinada região. Os clientes de serviços de cloud são responsáveis por fazer a sua própria avaliação independente das informações presentes neste documento e de qualquer utilização dos produtos ou serviços do fornecedor de cloud. Este documento não cria garantias, representações, compromissos contratuais, condições ou certezas.

Os exemplos de linguagem e documentos não devem ser considerados como orientação, recomendação ou aconselhamento jurídico. Os clientes de serviços de cloud devem consultar os seus próprios conselheiros jurídicos acerca das responsabilidades perante a legislação aplicável no país em que operam. O CISPE isenta-se expressamente de quaisquer garantias, responsabilidades ou danos associados a ou provenientes das informações presentes neste documento.

Acerca do CISPE

O CISPE (Cloud Infrastructure Services Providers in Europe, https://cispe.cloud) é um grupo independente do setor sem fins lucrativos. Representamos fornecedores de serviços de infraestrutura de cloud na Europa e trabalhamos com o setor 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.

Os nossos membros cada vez mais numerosos incluem empresas que operam em todos os países da União Europeia (UE) e com sede mundial em 16 países europeus. A associação está aberta às empresas, desde que confirmem que, pelo menos, um dos seus serviços cumpre os requisitos do Código de Conduta de Proteção de Dados do CISPE. Nós:

- Defendemos os benefícios de políticas de contratação pública cloud-first dentro da UE e respetivos Estados-Membros
- Interagimos com o setor de infraestruturas de cloud para alcançar a neutralidade climática em 2030
- Promovemos requisitos de segurança e normas técnicas coerentes por toda a UE
- Suportamos requisitos de privacidade abrangentes com o Código de Conduta de Proteção de Dados
- Trabalhamos para manter o mercado de infraestruturas de cloud da UE aberto, competitivo e livre de impedimentos
- Prevenimos obrigações injustificadas de monitorização de conteúdos no quadro jurídico da UE

Os nossos membros 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 essenciais para milhares de milhões de cidadãos. Nesta função, estamos a ajudar a potenciar o desenvolvimento de tecnologias e serviços de última geração que incorporam inteligência artificial (IA), objetos ligados, veículos autónomos, 5G e a próxima geração de tecnologia de ligação móvel.

Código de conduta para serviços de infraestrutura de cloud

O Código de Conduta de Proteção de Dados do CISPE foi publicamente lançado em setembro de 2016 e precedeu a aplicação do Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia. Está alinhado com os requisitos rigorosos do RGPD para ajudar os fornecedores de infraestruturas de cloud a estar em conformidade com as medidas de proteção de dados e oferecer uma estrutura sólida que ajuda os clientes a selecionar fornecedores de cloud e a confiar nos seus serviços. O Código de Conduta do CISPE foi validado pelo Comité Europeu para a Proteção de Dados (CEPD) em maio de 2021 e aprovado pela autoridade de proteção de dados francesa (CNIL), na qualidade de autoridade competente, em junho de 2021. https://www.codeofconduct.cloud/

Pacto para a neutralidade climática em datacenters

O CISPE colaborou com a Comissão Europeia no final de 2019 para desenvolver um conjunto de métricas e uma iniciativa autorreguladora para assegurar a neutralidade climática dos datacenters até 2030. A iniciativa foi desenvolvida com a European Data Centre Association (EUDCA) em conjunto com outras associações comerciais e intervenientes no mercado de datacenters e foi

lançada em janeiro de 2021 com o nome Climate Neutral Data Centre Pact (Pacto para a neutralidade climática em datacenters) https://www.climateneutraldatacentre.net/

Iniciativa de software justo

Em conjunto com a associação francesa de CIO (CIGREG) e com o apoio de outras associações comerciais de CIO e fornecedores de toda a Europa, o CISPE lançou os 10 Principles of Fair Software Licensing for Cloud Customers (10 princípios de licenciamento justo de software para clientes que utilizam a cloud), um conjunto de melhores práticas para as empresas que procuram inovação, flexibilidade e crescimento na cloud e que desafiam os seus fornecedores de software a garantir termos de licenciamento justos. https://www.fairsoftware.cloud/

GAIA-X

O CISPE é um dos 22 membros fundadores do GAIA-X, a iniciativa europeia com o objetivo de fornecer um ecossistema digital aberto e transparente. Como tal, o CISPE tem estado empenhado com a visão e os princípios da organização GAIA-X desde a sua fundação e, em junho de 2021, o seu secretário-geral foi reeleito para fazer parte do conselho de administração. Algumas das ferramentas referidas no manual, como o Código de Conduta de Proteção de Dados do CISPE e o Código de Conduta para IaaS da SWIPO, são úteis para demonstrar a conformidade com os princípios do GAIA-X. https://www.gaia-x.eu

O CISPE e o setor público

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

Embora os modelos de compras públicas devam condicionar o processo de adoção e utilização de computação na cloud, a aquisição de serviços de cloud difere da maioria das aquisições tecnológicas tradicionais conhecidas pelo setor público. As abordagens de aquisição têm de ser repensadas: o CISPE incentiva os legisladores da UE a desenvolver uma abordagem mais ambiciosa e visionária ao nível da UE, baseada em iniciativas de políticas cloud-first, para estimular o crescimento de um mercado único de infraestruturas de cloud na Europa e consolidar os objetivos de crescimento do Mercado Único Digital (MUD).

Este manual foi concebido para oferecer uma orientação útil e apoiar as autoridades públicas aquando da aquisição de serviços de cloud.

Mais informações

Membros do CISPE: https://cispe.cloud/members
Conselho executivo: https://cispe.cloud/board-of-directors
Serviços de computação na cloud declarados ao abrigo do Código de Conduta do CISPE: https://www.codeofconduct.cloud/public-register/

Índice

v2 2022 – fevereiro

Resumo e finalidade deste manual

O objetivo desde **manual sobre a aquisição de serviços de cloud** consiste em fornecer orientações aos clientes de serviços de cloud que pretendem comprar os mesmos através de um processo de aquisição competitivo **(pedido de proposta [RFP] de serviços de cloud)**, mas que não possuem a experiência necessária para redigir um acordo-quadro de cloud

Este documento destina-se apenas a fins informativos. Não foi desenvolvido em conformidade com os requisitos legais para processos de contratação pública num determinado país ou região.

O manual também analisa exemplos de critérios de seleção adicionais para **call-offs** ou **miniconcursos** quando se realizam compras a partir de um acordo-quadro de cloud. As secções do manual estão organizadas de forma a assemelhar-se a um RFP de TI genérico. Os exemplos de linguagem de um pedido de proposta genérico e de critérios de seleção são acompanhados por comentários para ajudar a compreender as diferenças entre um pedido de proposta de serviços de cloud e um pedido de proposta de TI tradicionais.

No seguimento da publicação da estratégia para cloud da Comissão Europeia, que estabelece como as instituições e agências europeias irão modernizar as suas infraestruturas de TI com uma abordagem cloud-first, o CISPE entregou o manual à Comissão Europeia em junho de 2019 durante o evento *How to transform governments through a smart cloud policy* (Como transformar governos através de uma política de cloud inteligente).

A **versão 2** deste manual inclui novas orientações relativamente a: proteção de dados (secção 2.3.1.1), mudança de fornecedores de cloud e portabilidade de dados (secção 2.3.1.2), termos e condições de software (secção 2.5.2), sustentabilidade na cloud (secção 3.6) e uma nova avaliação técnica em tempo real no Apêndice B.

> ***"Serviços de cloud"*** *refere-se a todas as tecnologias de cloud e serviços relacionados aos quais o utilizador final pode precisar de aceder. Estão incluídos os serviços geridos/profissionais ou de consultoria necessários para auxiliar e executar uma migração para a cloud e suportar cargas de trabalho na cloud, além da própria infraestrutura de cloud e de serviços de marketplace de cloud, como produtos de software como serviço (SaaS).*

Com a computação na cloud a ser a escolha predefinida para as TI no setor público, esta é uma oportunidade para modernizar estratégias de aquisição existentes. Os processos de aquisição centrados na cloud podem permitir que as entidades do setor público extraiam todos os benefícios da cloud, como o acesso a inovação pioneira, maior velocidade e agilidade, procedimentos de segurança e conformidade administrativa melhorados, e obtenham um aumento de eficiência e poupança.

Os métodos de aquisição de TI tradicionais para comprar hardware, software e datacenters não são adequados para comprar serviços de cloud. As abordagens em matéria de preços, gestão de contratos, termos e condições, segurança, requisitos técnicos, SLA e muito mais mudam num modelo de cloud e a utilização de métodos de aquisição existentes simplesmente reduz ou elimina os benefícios que a cloud oferece.

Um dos melhores meios de aquisição de serviços de cloud para o setor público é com um **acordo-quadro de cloud**, uma adjudicação multiorganizacional com diversas opções de cloud, através do qual os compradores elegíveis, afiliados à organização compradora, podem adquirir as tecnologias de cloud e os serviços associados que atendem às suas necessidades. Como um veículo para contratos de serviços de cloud, os acordos-quadro permitem a compra de serviços de cloud de forma eficiente. Desta forma, as organizações compradoras e as entidades de utilizadores finais têm acesso a uma ampla variedade de serviços de cloud e podem tirar partido de todos os benefícios da cloud: agilidade, elevadas economias de escala, escalabilidade para alcançar uma melhor disponibilidade a um custo mais baixo, variedade de funcionalidades, ritmo de inovação e capacidade de crescer para novas áreas geográficas.

Tenha em atenção que **este documento se foca na compra de tecnologias de cloud de infraestrutura como serviço (IaaS) e plataforma como serviço (PaaS), conforme fornecido por um *fornecedor de serviços de infraestrutura de cloud (CISP)*.** Tais tecnologias de cloud podem ser compradas diretamente a um CISP ou através de um revendedor de CISP. *Serão necessárias considerações adicionais de RFP para distribuidores de serviços de marketplace de cloud (PaaS e SaaS) e serviços de consultoria de cloud.*

Tenha também em atenção que este documento não abrange todos os aspetos da criação de um acordo-quadro de aquisição de cloud completo. Existem muitos outros documentos do setor e de analistas que abrangem assuntos como melhores práticas de aquisição de cloud, como orçamentar serviços de cloud, governança de cloud, etc. Recomendamos vivamente que tais conselhos e documentos sejam considerados aquando do desenvolvimento de uma estratégia de aquisição de cloud.
A **Tabela 1** abaixo fornece um resumo do manual de RFP de serviços de cloud, com exemplos de linguagem de RFP para cada componente do RFP de serviços em cloud.

Tabela 1 – Resumo das secções do manual de RFP de serviços de cloud

Secção	Vista geral e exemplos de linguagem de RFP
1.0 Vista geral de um acordo-quadro de cloud	Uma visão de alto nível do modelo de acordo-quadro de cloud (lotes, como competir e contratar)
2.0 Vista geral de RFP de serviços de cloud	Exemplos genéricos de linguagem de RFP que abrangem as secções abaixo, bem como comentários que explicam a lógica por trás da estrutura e linguagem utilizadas do RFP de serviços de cloud

Secção	Vista geral e exemplos de linguagem de RFP
2.1 Configuração de RFP de serviços de cloud	2.1.1 Introdução e objetivos estratégicos 2.1.2 Calendário de respostas do RFP 2.1.3 Definições 2.1.4 Descrição detalhada do modelo de compra e concorrência ao abrigo do acordo-quadro 2.1.5 Requisitos mínimos do concorrente: administrativos
2.2 Requisitos técnicos	2.2.1 Requisitos mínimos 2.2.2 Comparação de fornecedores 2.2.3 Contratação
2.3 Segurança	2.3.1 Requisitos mínimos 2.3.1.1 Proteção de dados 2.3.1.2. Mudança de fornecedores de cloud e portabilidade de dados 2.3.2. Comparação de fornecedores 2.3.3 Contratação
2.4 Preços	2.4.1 Requisitos mínimos 2.4.2 Comparação de fornecedores
2.5 Termos e condições/Configuração da execução do contrato	2.5.1 Termos e condições 2.5.2 Termos e condições do software 2.5.3 Como selecionar entre adjudicatários 2.5.4. Integração e saída
3.0 Melhores práticas/lições aprendidas	3.1 Governança de cloud 3.2 Orçamentação de cloud 3.3 Compreender o modelo empresarial dos parceiros 3.4 Agentes de cloud 3.5 Aprovisionamento e estudo de mercado antes do RFP 3.6 Sustentabilidade
Apêndice A – Requisitos técnicos de comparação entre os concorrentes	Uma lista de requisitos genéricos de tecnologias de cloud para call-offs ou miniconcursos
Apêndice B – Avaliação técnica em tempo real	Um exemplo de guião para um produto tecnológico de cloud a demonstrar a pontuação (demonstrações de cloud como parte de um call-off ou miniconcurso)

1.0 Vista geral de um acordo-quadro de cloud

Um acordo-quadro de cloud bem elaborado pode permitir a compra de serviços de cloud de forma a beneficiar tanto as organizações do setor público como os fornecedores de serviços de cloud. Os benefícios de um acordo-quadro de cloud bem elaborado incluem:

- Cooperativo por natureza:
    - Quando várias organizações se juntam para realizar pedidos com requisitos semelhantes isso resulta em conveniência, eficiência, custos reduzidos e até num processo de pedidos simplificado. Define uma forma eficaz de agregar a procura de várias organizações do setor público por tecnologias de cloud comuns e serviços de cloud associados, como soluções de marketplace e consultoria.
- Gama completa de serviços de cloud:
    - Pode incluir no seu âmbito todos os serviços de consultoria/profissionais/geridos necessários para suportar e executar totalmente a migração para a cloud e suportar cargas de trabalho na cloud, além das tecnologias de cloud fornecidas pelo CISP e serviços de marketplace.
    - As tecnologias de cloud podem ser compradas diretamente a um CISP ou através de um revendedor designado.
- Gestão de contratos:
    - Alinha diferentes organizações/compradores em torno de um conjunto comum de termos e condições e de uma adjudicação contratual principal única, em vez de contratos diferentes para cada organização.
    - Também é benéfico para os fornecedores porque proporciona um processo de aquisição, termos e condições e mecanismos de pedidos estandardizados, em vez de processos diferentes para cada organização do setor público.
    - Oferece flexibilidade. Criar, aprovar e executar um contrato de cloud eficiente ao abrigo de políticas/regulamentos governamentais existentes exige experimentação e a capacidade de se adaptar rapidamente. É muito mais benéfico criar um acordo-quadro que permita que o setor público e os fornecedores de cloud trabalhem em conjunto para melhorar o contrato, a nível contratual, mecânico e de forma eficiente. Um contrato multianual que não funcione e não possa ser ajustado causa uma má experiência para os utilizadores finais do setor público, organizações de aquisição e fornecedores de cloud.
- Capacidade de escolha:
    - Permite aos compradores escolher entre vários CISP qualificados e eleva a fasquia para todos os serviços de cloud e serviços associados, como um marketplace de PaaS/SaaS na cloud e consultoria de cloud.
    - Permite controlar a quantidade de fornecedores num acordo ao garantir que os padrões de cada adjudicatário são adequadamente examinados.

Um acordo-quadro para comprar serviços de cloud funciona melhor quando inclui as principais tecnologias de IaaS/PaaS fornecidas pelo CISP, bem como um marketplace de PaaS/SaaS e serviços de consultoria aos quais os utilizadores finais do setor público podem aceder sempre que necessário, para os ajudar a planear, transformar, utilizar e manter uma carga de trabalho em execução na cloud. Por isso, para configurar um acordo-quadro de cloud, sugerimos que o RFP de serviços de cloud seja dividido em 3 lotes, conforme apresentado abaixo:

- LOTE 1: TECNOLOGIAS DE CLOUD
  Tecnologias de cloud compradas diretamente a um CISP ou através de um revendedor de CISP designado.

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

- LOTE 3: CONSULTORIA EM CLOUD
  Serviços de consultoria relacionados com cloud (formação, serviços profissionais, serviços geridos, etc.) e apoio técnico.

*Como referido anteriormente, este documento foca-se na compra de tecnologias de cloud IaaS e PaaS (**LOTE 1**) como fornecidas pelo CISP (compradas diretamente a um CISP ou através de um revendedor de CISP). Seriam necessários diferentes requisitos de qualificação para fornecedores nos LOTES 2 e 3 do RFP de serviços de cloud.*

A Figura 1 abaixo ilustra uma vista geral de como um RFP de serviços de cloud bem estruturado, dividido nestes três lotes, pode resultar num acordo-quadro de cloud que ofereça às entidades do setor público agilidade (técnica e contratual), visibilidade e controlo de despesas e utilização da cloud, bem como a capacidade de ter todos os serviços de cloud necessários para construir e manter as soluções necessárias.

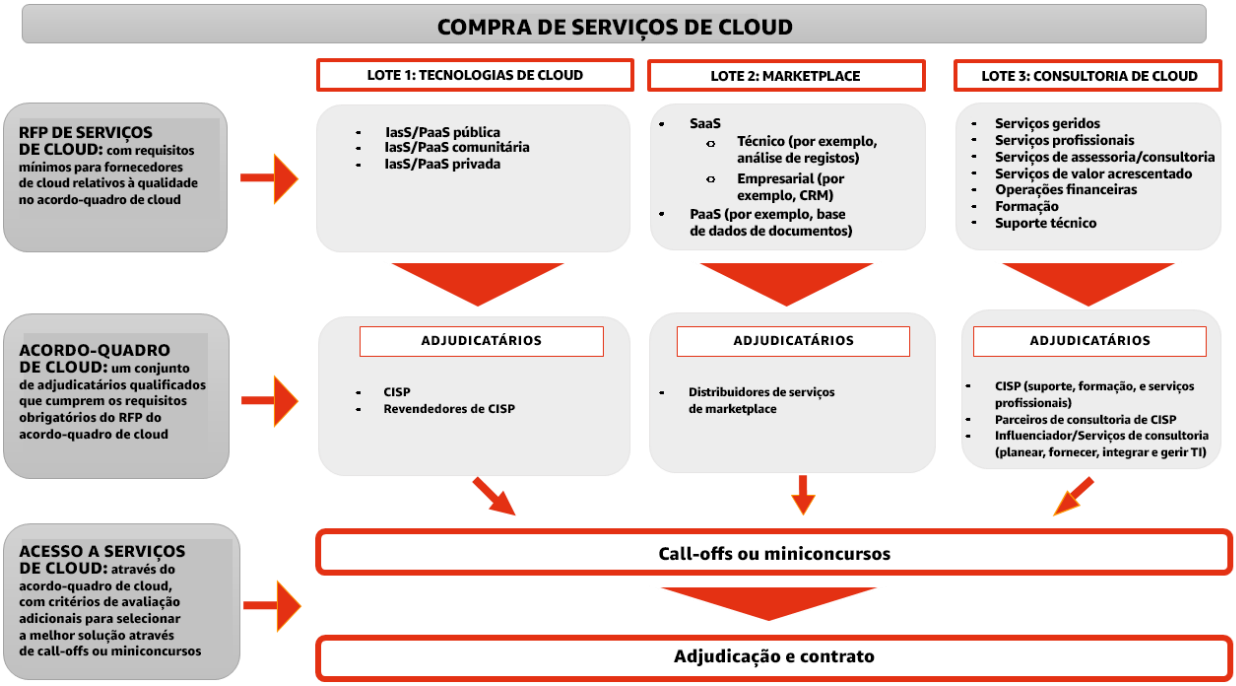

Figura 1 – Um RFP de serviços de cloud bem-sucedido separado em 3 lotes. Cada lote contém categorias ou "tipos de ofertas" para que a adequação técnica e contratual cumpra os requisitos do utilizador final durante a compra com o acordo-quadro de cloud.

Tenha em atenção que:

- Cada lote tem várias adjudicações.
- O LOTE 3 pode ser adjudicado através de outro RFP ou possivelmente através de outro serviço de consultoria.

Categorias do LOTE 1

Os acordos-quadro de cloud bem-sucedidos pedem aos CISP para descreverem o modelo de cloud que estão a oferecer, separado em categorias para cada lote. Recomendamos a utilização da norma do setor para computação na cloud (as características essenciais de cloud do Instituto Nacional de Normas e Tecnologia [NIST – National Institute of Standards and Technology] dos EUA), para as definições de cloud **pública**, cloud **comunitária** e cloud **privada**. A estruturação de um acordo-quadro de cloud desta forma permite que as agências e os órgãos públicos compradores utilizem o acordo-quadro para escolher entre vários modelos de cloud que se adaptem às suas necessidades.

Veja a secção *2.1.3 Definições* para consultar a definição do NIST para cada modelo de cloud no LOTE 1 (IaaS/PaaS pública, IaaS/PaaS comunitária, IaaS/PaaS privada)

Como competir: call-offs ou miniconcursos?

Os critérios de qualificação para um RFP de serviços de cloud devem abranger elementos essenciais e padrões mínimos e não devem incluir critérios preferenciais. Caso sejam incluídos critérios adicionais superiores aos da referência para os fornecedores que se estão a qualificar para o

acordo-quadro, é possível que alguns fornecedores não possam apresentar propostas, resultando na redução de escolhas para os compradores.

Após o RFP e a configuração subsequente do acordo-quadro de cloud, os órgãos do setor publico que fazem parte do acordo podem realizar um pedido ou um "call-off" dos serviços de cloud quando necessário. Efetuar um contrato de call-off sob um acordo-quadro permite aos compradores refinar requisitos com especificações funcionais adicionais para um call-off, mantendo os benefícios oferecidos no acordo-quadro.

Se for necessário, pode ser efetuado um miniconcurso para identificar o melhor fornecedor para um projeto ou carga de trabalho específica. Com um miniconcurso, o cliente realiza um novo concurso ao abrigo do acordo-quadro, convidando todos os fornecedores num lote a responder a um conjunto de requisitos. O cliente convida todos os fornecedores aptos num mesmo lote a apresentar propostas, daí a importância dos requisitos mínimos para adjudicatários num RFP de serviços de cloud, já que isso garante um nível elevado de opções em cada lote.

Tenha em atenção que é importante existirem ***conjuntos distintos de termos e condições*** *de contrato para cada um dos lotes conforme apresentado na Figura 1 acima. Uma única abordagem para os contratos de todos os lotes irá criar problemas de viabilidade e compatibilidade técnicas.*

2.0 Vista geral de RFP de serviços de cloud

Esta secção descreve o modelo e âmbito do RFP de serviços de cloud, incluindo: objetivos estratégicos, participantes, definições, calendário, requisitos mínimos administrativos. Novamente, chamamos a atenção para o facto de o foco deste manual ser o LOTE 1: TECNOLOGIAS DE CLOUD.

2.1 Configuração de RFP de serviços de cloud

Recomendamos vivamente que as entidades do setor público sejam transparentes em relação aos seus requisitos e objetivos de alto nível na introdução de um RFP de serviços de cloud.

2.1.1 Introdução e objetivos estratégicos

Para efeitos de maior clareza em relação aos objetivos estratégicos, é recomendável incluir na introdução do RFP de serviços de cloud: **(1)** os objetivos empresariais e benefícios que a organização procura atingir ao utilizar a cloud; **(2)** a estrutura do acordo-quadro (quem compra, quem opera, quem orçamenta, etc.); **(3)** uma compreensão clara do modelo de responsabilidade partilhada entre o setor público e os fornecedores de cloud, que é a base da compra e utilização bem-sucedidas de cloud; **(4)** o tipo de relação criada entre os fornecedores de serviços de cloud (CISP), distribuidores de serviços de marketplace, parceiros de consultoria, agências de aquisição/contratação governamentais e utilizadores finais governamentais. A articulação destes quatro pontos ajuda as organizações a desenvolver um RFP que melhor responde às respetivas necessidades, além de garantir que tanto os clientes como os fornecedores compreendem os documentos do RFP final.

Um RFP de cloud é intencionalmente diferente de um RFP de TI tradicional. A tecnologia de cloud não é simplesmente uma substituição dos métodos tradicionais de computação por outros equivalentes, pois adiciona uma forma completamente nova de consumir tecnologia. Os RFP de serviços de cloud bem elaborados podem ajudar as entidades do setor público a tirar partido da cloud mais rapidamente.

De todos os aspetos da compra de cloud que citamos como boas práticas, a boa compreensão do modelo de responsabilidade partilhada é um bom ponto de partida. O modelo de responsabilidade partilhada[1] é utilizado frequentemente quando se analisa a segurança e conformidade na cloud, mas esta delineação de responsabilidades aplica-se a todos os aspetos da computação na cloud. Um RFP de serviços de cloud deve ser claro em relação ao que é da competência do CISP num ambiente de cloud e o que continua a ser da responsabilidade do cliente. Por exemplo, um CISP providencia capacidades para monitorizar aplicações e recursos que são executados na cloud, ***mas*** é da responsabilidade do cliente utilizar essas capacidades fornecidas pelo CISP, pois um CISP que opera a grande escala não o poderá fazer para milhões de clientes.

Além disso, os clientes da cloud devem compreender como é que a rede de parceiros do CISP ajuda os clientes a utilizar a cloud e a gerir as suas responsabilidades. Por exemplo, um fornecedor de serviços geridos (MSP) de cloud pode ajudar um cliente a configurar e utilizar capacidades de monitorização fornecidas pelo CISP para cumprir os seus requisitos exclusivos de conformidade e auditoria.

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

Em suma, as responsabilidades do modelo de cloud são:

Um CISP fornece a tecnologia de cloud

Um cliente utiliza a tecnologia de cloud

As **empresas de consultoria** (se aplicável) ajudam um cliente a aceder e a utilizar a tecnologia de cloud

*As **"empresas de consultoria"** são empresas de serviços profissionais/geridos e de consultoria que ajudam os clientes a conceber, arquitetar, criar, migrar e gerir cargas de trabalho e aplicações na cloud. Tais empresas incluem integradores de sistemas, consultorias estratégicas, agências, fornecedores de serviços geridos e revendedores de valor acrescentado.*

Considere as compras de serviços de cloud como compras numa loja de ferragens. Na loja de ferragens tem uma vasta gama de materiais e ferramentas para construir o que precisa. Pode construir um armário, uma piscina ou uma casa inteira. A escolha é sua. Quando compra os materiais e as ferramentas, a equipa da loja irá fornecer orientações e experiência, mas não vai à sua casa construir algo por si. Portanto, tem algumas opções:

1. Compra os materiais e as ferramentas e constrói algo por si mesmo.
2. Compra os materiais e as ferramentas e contrata alguém para construir e/ou operar algo por si.
3. Contrata alguém para construir ou operar algo por si e pede que essa pessoa forneça os materiais e ferramentas como parte do acordo geral.

Se uma organização tiver a capacidade interna para construir e gerir o seu próprio ambiente e soluções, então só precisa mesmo de acesso às tecnologias e ferramentas de cloud estandardizados do CISP (diretamente com um CISP ou através de um revendedor. Consulte o **LOTE 1**). O software de SaaS e PaaS necessário deve estar disponível num marketplace de cloud (**LOTE 2**). Se for necessária ajuda adicional de consultoria, migração, implementação e/ou gestão, é aqui que a rede de parceiros de um CISP começa a intervir (**LOTE 3**).

Exemplo de linguagem de RFP: introdução e objetivos estratégicos

A computação na cloud oferece às organizações do setor público um rápido acesso a uma vasta variedade de recursos de TI de baixo custo, flexíveis e com pagamento conforme a utilização. As organizações podem aprovisionar o tipo e o tamanho adequados dos recursos necessários para estimular as suas novas e mais brilhantes ideias ou operar os seus próprios departamentos de TI, eliminando a necessidade de grandes investimentos em hardware e/ou contratos de licenciamento de software a longo prazo.

*A **<ORGANIZAÇÃO>** tem um requisito para o acesso a estes tipos de tecnologias de cloud comercialmente disponíveis para cumprir as suas necessidades empresariais num largo espetro de organizações afiliadas.*

*O principal objetivo deste RFP é adjudicar um **<ACORDO-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 (CISP) ou revendedores de 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 fornecer um conhecimento adicional sobre a migração e utilização destas ofertas do CISP.*

Em relação ao ***LOTE 1****, as organizações concorrentes (CISP ou revendedores de CISP) têm de demonstrar como as suas ofertas cumprem os seguintes objetivos:*

- ***Agilidade:*** *disponibilizar recursos de TI a utilizadores finais em questão de minutos em vez dos períodos tradicionais de semanas ou meses.*
- ***Inovação:*** *ter acesso instantâneo às mais recentes e inovadoras tecnologias no mercado.*
- ***Custo:*** *trocar despesas de capital por despesas variáveis (por exemplo, CapEx para OpEx) e pagar somente pelo que é consumido.*
- ***Orçamentação:*** *consultar informações de faturação e utilização de forma detalhada e resumida, visualizando padrões nos gastos ao longo do tempo, além de prever despesas futuras.*
- ***Elasticidade:*** *obter custos variáveis mais baixos graças às economias de escala mais elevadas que a cloud proporciona.*
- ***Capacidade:*** *eliminar estimativas em relação às necessidades de capacidade de infraestrutura.*
- ***Parar de depender de datacenters:*** *focar nas necessidades dos cidadãos e não no esforço de montar em racks, empilhar e alimentar servidores.*
- ***Segurança:*** *formalizar a criação de contas com maior visibilidade e auditabilidade de recursos e eliminar o custo de proteção de instalações e hardware físico.*
- ***Responsabilidade partilhada:*** *aliviar a carga operacional à medida que o CISP opera, gere e controla os componentes do sistema operativo anfitrião e camada de virtualização até à segurança física das instalações em que os serviços operam.*
- ***Automatização:*** *integrar a automatização na arquitetura de cloud para melhorar a capacidade de escalar com maior segurança, rapidez e rentabilidade.*
- ***Governança de 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 à utilização/faturação/segurança/etc. (todos com capacidades de monitorização de ativos, gestão de inventário, gestão de mudanças, gestão e análise de registos, visibilidade geral e governança de cloud).*
- ***Controlo:*** *obter uma visibilidade completa de como os serviços de TI são consumidos e onde podem ser ajustados para fins de segurança, fiabilidade, desempenho e custo.*
- ***Reversibilidade:*** *ferramentas e serviços de portabilidade para ajudar a migrar de e para a infraestrutura do CISP, reduzindo a dependência do fornecedor, e respeitar os códigos de conduta do setor.*
- ***Proteção de dados:*** *capacidade de demonstrar conformidade com o Regulamento Geral sobre a Proteção de Dados (RGPD) através de um código de conduta do setor 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 a localização das infraestruturas utilizadas para tratar e armazenar os seus dados (zona urbana).*

- ***Neutralidade climática:*** *os clientes devem interagir com os CISP que estão a realizar passos comprovados e específicos para cumprir os objetivos de neutralidade climática até 2030 e que são signatários do Climate Neutral Data Centre Pact. Isto irá ajudar os clientes a cumprir os seus próprios objetivos de neutralidade climática.*

2.1.2 Calendário de respostas do RFP

É recomendável fornecer aos concorrentes um calendário da atividade antecipada de apresentação de propostas durante a criação de um acordo-quadro de cloud e o RFP de serviços de cloud associado. Quanto mais interação com o setor, melhor, pois isso ajuda a garantir que todos os intervenientes compreendem claramente os requisitos do RFP e, consequentemente, como todos os serviços dos fornecedores se enquadram no modelo dos serviços de cloud.

Tenha em atenção que o calendário do RFP está sujeito à legislação e às obrigações jurídicas locais e a lista abaixo serve apenas como um guia de melhores práticas e não como uma lista prescritiva de atividades e prazos.

Exemplo de linguagem de RFP: calendário de respostas

Veja o calendário de RFP abaixo referente ao RFP de serviços de cloud:

Calendário do RFP para serviços de cloud
• *Emissão do pedido de informações (RFI):* • *Resposta ao RFI:* • *Emissão do rascunho de um pedido de proposta (RFP):* • *Prazo da resposta ao rascunho do RFP:* • *Fase de consulta do setor: <prazos>* • *Emissão do RFP de pré-qualificação:* • *Resposta ao RFP de pré-qualificação:* • *Emissão do RFP:* • *Prazo para perguntas da ronda 1:* • *Respostas da ronda 1:* • *Prazo para perguntas da ronda 2:* • *Respostas da ronda 2:* • *Prazo da resposta ao RFP:* • *Período de esclarecimento da proposta:* • *Período de negociação:* • *Data de intenção da adjudicação:* • *Adjudicação do contrato:* • *Duração do contrato (opções de extensão):*

Tenha em atenção que o calendário do RFP está sujeito à legislação e às obrigações jurídicas locais e a lista abaixo serve apenas como um guia de melhores práticas e não como uma lista prescritiva de atividades e prazos.

2.1.3 Definições

Um RFP de serviços de cloud deve incluir uma lista detalhada de definições. Esta lista inclui as funções do fornecedor (por exemplo, fornecedor de serviços de cloud, revendedor de serviços de cloud, parceiro de cloud), conceitos gerais de tecnologia (computação, armazenamento, IaaS/PaaS, SaaS) e outras partes importantes do acordo. Veja o exemplo de lista de definições abaixo:

Exemplo de linguagem de RFP: definições

As definições abaixo de computação na cloud são do Instituto Nacional de Normas e Tecnologia (NIST – National Institute of Standards and Technology) dos EUA.[2]

- ***Infraestrutura como serviço (IaaS):*** *a capacidade oferecida ao consumidor de aprovisionar o processamento, armazenamento, redes e outros recursos de computação fundamentais em que o consumidor consegue implementar e executar software arbitrário, que pode incluir sistemas operativos e aplicações. O consumidor não faz a gestão nem controla a infraestrutura de cloud subjacente, mas tem controlo sobre sistemas operativos, armazenamento e aplicações implementadas e, possivelmente, um controlo limitado de componentes de redes específicos (por exemplo, firewalls do anfitrião).*

- ***Plataforma como serviço (PaaS):*** *a capacidade oferecida ao consumidor de implementar na infraestrutura de cloud aplicações adquiridas ou criadas pelo consumidor com linguagem de programação, bibliotecas, serviços e ferramentas suportadas pelo fornecedor. O consumidor não faz a gestão nem controla a infraestrutura de cloud subjacente, incluindo redes, servidores, sistemas operativos ou armazenamento, mas tem controlo sobre as aplicações implementadas e, possivelmente, configurações do ambiente de alojamento das aplicações.*

- ***Software como serviço (SaaS):*** *a capacidade fornecida ao consumidor de utilizar as aplicações do fornecedor que são executadas numa infraestrutura de cloud. As aplicações são acessíveis a partir de vários dispositivos cliente, tanto através uma interface de cliente simples, como um navegador Web (por exemplo, e-mail baseado na Web) ou uma interface de programa. O consumidor não faz a gestão nem controla a infraestrutura de cloud subjacente, incluindo redes, servidores, sistemas operativos, armazenamento ou até capacidades de aplicações individuais, com a possível exceção de definições de configuração de aplicações específicas do utilizador.*

- ***Cloud pública:*** *a infraestrutura de cloud é aprovisionada para utilização aberta pelo público em geral. Pode ser detida, gerida e operada por uma organização empresarial, académica ou governamental ou uma combinação destas entidades. Existe nas instalações do fornecedor de cloud.*

- ***Cloud comunitária:*** *a infraestrutura de cloud é aprovisionada para utilização exclusiva de uma comunidade específica de consumidores de organizações com preocupações semelhantes (por exemplo, missão, requisitos de segurança, política e considerações de conformidade). Pode ser detida, gerida e operada por uma ou mais organizações na comunidade, por terceiros ou por alguma combinação destas entidades e pode estar localizada dentro ou fora das instalações.*

- ***Cloud híbrida:*** *a infraestrutura de cloud é uma composição de duas ou mais infraestruturas de cloud distintas (privada, comunitária ou pública) que permanecem entidades exclusivas, mas que estão vinculadas por uma tecnologia estandardizada ou proprietária que permite a portabilidade de dados e aplicações (por exemplo, expansão na cloud para balanceamento de carga entre clouds).*

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

- ***Cloud privada:*** *a infraestrutura de cloud é aprovisionada para utilização exclusiva por uma única organização que engloba múltiplos consumidores (por exemplo, unidades de negócio). Pode ser detida, gerida e operada pela organização, por terceiros ou por alguma combinação destas entidades e pode estar localizada dentro ou fora das instalações.*

2.1.4 Descrição detalhada do modelo de compra e concorrência ao abrigo do acordo-quadro

Conforme mencionado anteriormente, as organizações do setor público devem identificar o modelo que determina como um acordo-quadro irá operar como um mecanismo de compra de tecnologias de cloud e serviços relacionados de implementação e gestão. Isto deve ser esclarecido no RFP de serviços de cloud, para que os fornecedores de tecnologias de cloud, as organizações de serviços de consultoria relacionados, os distribuidores de marketplace e as entidades compradoras compreendam as suas funções.

Quando se trata do âmbito do acordo-quadro e dos call-offs ou miniconcursos subsequentes, as organizações devem considerar:

- Quem será responsável pela integração e pelos serviços geridos que envolvem a utilização das tecnologias de cloud presentes no contrato.
- Existe algum requisito para que um revendedor/parceiro de CISP forneça serviços de valor acrescentado, além de manter uma relação contratual com o CISP, oferecendo serviços de faturação consolidados e acesso atempado e direto aos dados de utilização 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, fornecedor de serviços geridos ou qualquer forma de serviços de trabalho de TI?

É importante ter em atenção que um CISP não é um integrador de sistemas (SI) nem um fornecedor de serviços geridos (MSP). Muitos clientes do setor público exigem um CISP para a sua IaaS/PaaS e subcontratam o trabalho "prático" de consultoria, planeamento, migração e gestão para um SI ou MSP. A Figura 2 ilustra a delineação das funções e responsabilidades num modelo de serviços de cloud.

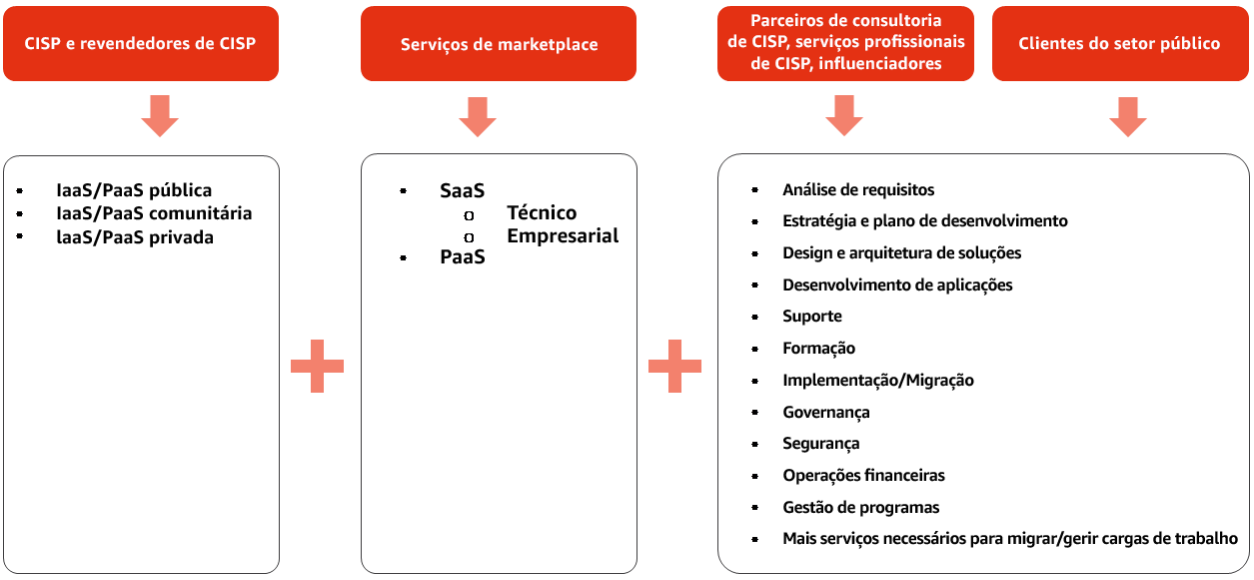

Figura 2 – Um RFP de serviços de cloud deve fornecer aos utilizadores finais um menu com todos os serviços de cloud de que precisem. Os clientes do setor público precisam de um CISP para tecnologias de cloud, um marketplace para produtos de PaaS e SaaS se necessário. Em seguida, o cliente pode determinar a importância da função que pretende assumir na entrega dos serviços de cloud e quanto pretende subcontratar para uma empresa de consultoria/integrador de sistemas/fornecedor de serviços geridos/etc.

Os exemplos de linguagem abaixo estão adaptados às funções e responsabilidades, conforme apresentado na Figura 2 acima. Um acordo-quadro de cloud, juntamente com o RFP de serviços de cloud associado, deve garantir que os compradores mantêm a capacidade de avaliar adequadamente as ofertas de cada fornecedor, permitindo escolher entre os serviços necessários para a carga de trabalho/projeto. Para tal, o melhor é separar os serviços em lotes, conforme já mencionado, e esclarecer como os call-offs e os miniconcursos são realizados ao abrigo do acordo-quadro.

Exemplo de linguagem de RFP: modelo de compra

*Este contrato servirá como um meio de compra do **acordo-quadro**. Este acordo-quadro de cloud inclui diversos **lotes**, conforme definido pela **<ORGANIZAÇÃO>**, para tecnologias de cloud e serviços/produtos de marketplace, serviços de consultoria, serviços profissionais /integração de sistemas/geridos e serviços profissionais de migração, formação e suporte relacionados, como definido pela **<ORGANIZAÇÃO>**, e será utilizado por diversos compradores elegíveis afiliados à **<ORGANIZAÇÃO>**. Isto irá simplificar o processo de aquisição e otimizar economias de escala.*

Uma vez estabelecido, este acordo-quadro permite que uma organização compre as tecnologias de cloud específicas e os serviços de cloud relacionados pretendidos e quando necessário, ao contrário de compras através de aquisições individuais. Essa abordagem reduz os requisitos administrativos e diminui consideravelmente a complexidade da aquisição e a duração do ciclo.

*A duração do acordo-quadro será de, no máximo, **<X>** anos, incluindo quaisquer renovações. O período máximo de um contrato-quadro de call-off é geralmente de **<x>** meses; podendo ser prolongado por **<x>** meses e mais **<x>** meses posteriormente, com as aprovações internas adequadas, se necessário para uma extensão de contrato. Isto será especificado em cada **call-off** específico.*

*O ACORDO-QUADRO está dividido em **3 (três) lotes.***

1. *LOTE 1: TECNOLOGIAS DE CLOUD: gama completa das tecnologias do fornecedor de cloud (diretamente do CISP, do revendedor ou do revendedor com suporte/serviços de valor acrescentado):*
    i. ***Serviços de IaaS e PaaS:** uma lista de tecnologias de cloud, como computação, armazenamento, redes, bases de dados, análises, serviços de aplicações, implementação, gestão, programação, Internet das Coisas (IoT), etc. Inclui pacotes de soluções de tecnologia de cloud, como DR/COOP, arquivo, big data e análise, DevOps, etc.*
2. *LOTE 2: MARKETPLACE: gama completa de serviços/produtos de PaaS e SaaS, como contabilidade, CRM, design, RH, SIG e mapeamento, HPC, BI, gestão de conteúdo, análise de registos, etc.*
3. *LOTE 3: CONSULTORIA DE CLOUD: gama completa de serviços de consultoria (serviços geridos, serviços profissionais, serviços de consultoria, serviços de valor acrescentado, operações financeiras, suporte técnico) relacionados com a utilização de cloud e migração para a cloud. Estes serviços podem incluir: planeamento, design, migração, gestão, suporte, QA, segurança, formação, etc.*

Os fornecedores podem submeter as suas ofertas para diversos lotes.

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

CONCORRÊNCIA NO ACORDO-QUADRO E ADJUDICAÇÃO DE CONTRATOS

CALL-OFFS

Os órgãos do setor público que fazem parte do acordo-quadro podem realizar um pedido ou um call-off dos serviços necessários quando precisam. Efetuar um contrato de call-off sob o acordo-quadro permite aos compradores refinar requisitos com especificações funcionais adicionais para um call-off, mantendo os benefícios oferecidos no acordo-quadro.

Os contratos adjudicados através do acordo-quadro conseguirão demonstrar um registo de auditoria claro em termos dos requisitos utilizados para selecionar o fornecedor em cada lote. Os compradores finais manterão um registo de comunicações com os fornecedores, incluindo quaisquer participações antecipadas no mercado, perguntas de esclarecimento, e-mails ou conversas pessoais ocorridas.

1. REDIGIR REQUISITOS DE CALL-OFF E PEDIR APROVAÇÃO INTERNA PARA REALIZAR A COMPRA

Todos os compradores finais elegíveis para utilizar o acordo-quadro criarão equipas conjuntas de utilizadores finais empresariais, especialistas em compras e especialistas técnicos para preparar uma lista de "itens essenciais" e "itens desejados". Estes requisitos ajudarão a decidir que lotes são aplicáveis e que fornecedor é mais qualificado para cumprir os requisitos. Ao redigir os requisitos, os compradores deverão considerar o seguinte:

- *fundos disponíveis para utilizar o serviço*
- *requisitos técnicos e de aquisição do projeto*
- *critérios nos quais a escolha será baseada*

2. PROCURAR SERVIÇOS

Os compradores presentes no acordo-quadro utilizarão um catálogo online (portal onde os adjudicatários qualificados do acordo-quadro e os seus serviços estarão apresentados) para encontrar produtos/serviços que atendam às suas necessidades identificadas. Irão escolher os lotes apropriados e, depois, procurarão os serviços.

3. REVER E AVALIAR OS SERVIÇOS

Os compradores presentes no acordo-quadro deverão rever as descrições dos serviços para encontrar as que atendem melhor às suas necessidades, com base nos requisitos e também no orçamento. Cada descrição de serviço irá incluir:

- *Documento de definição de serviços ou ligações para definições de serviços*
- *Documento de termos e condições*
- *Documento de preços (as ligações para preços públicos são aceitáveis, partindo do princípio que uma tabela de preços/documento de preços completo estará disponível mediante pedido)*

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, além das ferramentas de cálculo de preços, para saber o preço real do que está a ser comprado e o valor geral oferecido ao comprador (por exemplo, serviços para otimização e redução de custos resultante).

Os compradores ao abrigo do acordo-quadro podem pedir aos fornecedores que expliquem a descrição do serviço, os termos e condições, os preços ou os documentos/modelo de definição de serviços. Será mantido um registo de todas as conversas com os fornecedores.

4. ESCOLHER UM SERVIÇO E ADJUDICAR UM CONTRATO

Fornecedor individual

Se apenas um fornecedor cumprir os requisitos, o contrato poderá ser adjudicado ao mesmo.

Vários fornecedores

Se existirem vários serviços numa lista de pré-seleção, o comprador irá escolher o que tiver a proposta economicamente mais vantajosa (Most Economically Advantageous Tender – MEAT). Veja na tabela seguinte os critérios para a avaliação com base na MEAT. Os compradores podem decidir as características detalhadas a utilizar e como as ponderar.

Tenha em atenção que o comprador pode ter de:

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

A avaliação de fornecedores deve ser sempre justa e transparente. A escolha será baseada na opção mais adequada e os fornecedores/serviços não serão excluídos sem que os requisitos do projeto sejam consultados novamente.

Tabela 2– Avaliação com base na MEAT

Critérios de adjudicação
***Custo para a duração total:** eficiência de custos, 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 de gestão de contas e garantia de fornecimento de uma gama de serviços*
Características não funcionais

MINICONCURSOS

Se for necessário, pode ser efetuado um miniconcurso para identificar o melhor fornecedor para um projeto ou carga de trabalho específica. Com um miniconcurso, o cliente realiza um novo concurso ao abrigo do acordo-quadro, convidando todos os fornecedores num lote a responder a um conjunto de requisitos. O cliente convidará todos os fornecedores aptos do lote a apresentar propostas. Consulte as informações comparativas adicionais nas secções abaixo relativamente a questões técnicas, de segurança e de preço/valor.

CONTRATO

O comprador e o fornecedor assinarão uma cópia do contrato antes de o serviço ser utilizado. O período máximo de um contrato-quadro é geralmente de ***<x>*** *meses; podendo ser prolongado por* ***<x>*** *meses e mais* ***<x>*** *meses posteriormente, com as aprovações internas adequadas, se necessário para uma extensão de contrato.*

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

2.1.5 Requisitos mínimos do concorrente: administrativos

Uma linguagem simples e clara para definir os critérios de qualificação do acordo-quadro ajuda a garantir que não há submissões de fornecedores tradicionais de datacenters ou hardware que tentam vender uma solução tradicional como "cloud". Os participantes do RFP devem demonstrar como respondem aos requisitos administrativos mínimos de concorrente abaixo.

Mais uma vez, tenha em atenção que este documento tem como foco o LOTE 1: TECNOLOGIAS DE CLOUD. No entanto, introduzimos informações adicionais sobre o LOTE 2: MARKETPLACE e o LOTE 3: CONSULTORIA DE CLOUD quando ajudam a fornecer um contexto geral em termos de requisitos e do âmbito do RFP. Por exemplo, é importante incluir critérios de qualificação mínimos para revendedores de CISP/MSP/SI/empresa de consultoria/etc. Isso ajuda a garantir que (1) estão diretamente afiliados ao CISP como revendedores ou parceiros de canal; (2) foram certificados por um CISP para revender o acesso direto às ofertas do CISP a terceiros e (3) possuem certificados do CISP que reconhecem as suas competências e conhecimentos.

Exemplo de linguagem de RFP: requisitos mínimos do licitante (administrativos)

Este acordo-quadro irá adjudicar contratos a diversos fornecedores nas seguintes categorias. Os fornecedores devem ser um CISP comercial, revendedor terceiro de um CISP, distribuidor de serviços de marketplace e/ou fornecedor de serviços para utilização de um CISP (por exemplo, consultoria, serviços de migração, serviços geridos, operações financeiras, etc.). Identifique as funções para as quais está a apresentar proposta:

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 terceiro de CISP (capacidade de conceder acesso direto às ofertas de cloud online dos CISP)

- *Identifique a oferta do CISP para a qual consegue revender o acesso direto: _____*
- *Forneça uma carta do CISP que ateste que é um revendedor autorizado das suas ofertas: _____*

LOTE 2

____ - Fornecedor direto de serviços de marketplace executados num CISP (PaaS e/ou SaaS)

____ - Distribuidor de serviços de marketplace executados num CISP (PaaS e/ou SaaS)

LOTE 3

____ - CISP que presta serviços profissionais

____ - Fornecedor de suporte técnico do CISP

____- Parceiro de CISP que presta serviços para utilizar ou operar num CISP

____- Influenciador/Consultor que presta serviços para utilizar ou operar num CISP

Identifique o tipo de oferta:

- *Serviços geridos de cargas de trabalho num 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: governança de cloud (S/N): _____*
- *Consultoria: operações financeiras (S/N): _____*
- *Consultoria: outro (identifique): _____*

Identifique o ou os CISP para os quais presta serviços: _____
Forneça uma carta do CISP que confirme o seu estatuto de parceiro ao abrigo do modelo do CISP: _____

REQUISITOS MÍNIMOS ADMINISTRATIVOS DO LOTE 1

Fornecedores de serviços de cloud (CISP)
Para se qualificar como CISP, o mesmo tem de estar em conformidade com os requisitos abaixo.

Critérios de qualificação propostos para um CISP	*Motivo*
Informações organizacionais, como nome, estrutura jurídica, número de registo/DUNS, NIF, etc.	
Dimensão da empresa e situação económica e financeira[3].	*O cliente pode determinar a capacidade do CISP de executar o contrato.*
Exemplos de motivos de exclusão: atividades criminais/fraudulentas, etc.	
Casos de estudo/Referências do cliente (especifique o número/tipo de requisito).	*O cliente pode avaliar se o CISP tem a experiência necessária para fornecer os serviços solicitados.*

[3] Tenha em atenção que um RFP de serviços de cloud analisa informações gerais da empresa, em oposição ao número de funcionários da empresa e à estrutura interna de equipas. Com a tecnologia de cloud, não há correlação entre a garantia desempenho do serviço e o número de funcionários. Em vez disso, os RFP de cloud analisam o tamanho geral da empresa para satisfazer os requisitos (escala adequada) e a experiência e o desempenho comprovados.

Responsabilidades sociais corporativas.	*O CISP deve fornecer versões publicamente acessíveis.*
Compromissos e práticas de sustentabilidade publicamente disponíveis.	*O cliente pode avaliar que o CISP se compromete a realizar os seus negócios da forma mais sustentável possível.*
O CISP tem de fornecer um registo comprovado de inovação e lançamento de novos serviços e funcionalidades úteis nos últimos 5 anos, principalmente na área de PaaS, machine learning, análise, big data, serviços geridos e funcionalidades de otimização de utilização de cloud. Para fins de comprovação, podem ser utilizados registos de alterações 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. Isto ajuda os clientes a manter uma infraestrutura de TI de última geração sem ser necessário fazer investimentos de recapitalização.*

Relação do revendedor/parceiro com o CISP

*A **<ORGANIZAÇÃO>** exige que o contratante principal esteja diretamente afiliado ao CISP como revendedor ou parceiro de canal, esteja certificado por um CISP para revender com acesso direto às ofertas do CISP a entidades terceiras e possua certificações do CISP que demonstrem as suas capacidades e conhecimentos. Desta forma, a **<ORGANIZAÇÃO>** não precisa de analisar os termos e serviços associados a uma camada adicional de subcontratação entre o contratante principal do **acordo-quadro** e o CISP. Este requisito também reduz a complexidade que as camadas adicionais de revendedores criam quando (1) a **<ORGANIZAÇÃO>** realiza a devida diligência para garantir que a atribuição clara de responsabilidades referentes aos serviços é fornecida e (2) a **<ORGANIZAÇÃO>** realiza atividades diárias que envolvam o consumo dos serviços de cloud.*

2.2 Requisitos técnicos

Um RFP de serviços de cloud deve elevar o nível de exigência dos CISP ao exigir que forneçam as tecnologias de cloud estandardizadas necessárias para que o cliente desenvolva a sua solução personalizada. Conforme mencionado, esta diferença entre o que é estandardizado e o que é personalizado é muito importante durante a elaboração de um RFP de serviços de cloud. Os CISP oferecem serviços estandardizados a milhões de clientes, por isso, as personalizações num RFP de serviços de cloud focam-se em soluções e resultados ao mais alto nível, em oposição aos métodos, infraestrutura ou hardware subjacentes utilizados para oferecer os serviços de cloud e obter resultados da solução.

2.2.1 Requisitos mínimos

As aquisições de TI tradicionais normalmente contam com requisitos empresariais desenvolvidos através de uma série de sessões de trabalho que documentam como a organização conduz atualmente as suas operações. Fazer com que estes requisitos estejam perfeitamente corretos é um processo difícil na melhor das hipóteses. Quando bem-sucedidas, estas sessões de requisitos documentam o processo empresarial histórico que pode, por si só, estar desatualizado e ser ineficiente. Se esses requisitos fizerem parte do RFP a ser replicado pelo CISP, a única opção poderá ser uma solução personalizada. Este modelo não é compatível com aquisições de cloud.

As organizações do setor público devem conhecer os seus objetivos de negócio e necessidades de desempenho, mas não devem prescrever um RFP de forma a ditar o design e as funcionalidades do sistema. Em vez disso, a organização deve procurar a solução que melhor se adequa ao seu negócio. 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 alcançam ou mesmo superam os objetivos propostos, se respondem às suas necessidades de desempenho e à capacidade de ajustar as regras de negócio através da configuração.

Os RFP de cloud devem fazer as perguntas apropriadas para poder obter as melhores soluções. Considerando que, num modelo de cloud, os ativos físicos não estão a ser comprados, muitos requisitos de aquisição de datacenters tradicionais não são aplicáveis. ***Reciclar perguntas sobre datacenters resultará inevitavelmente em respostas sobre datacenters.*** *Consequentemente, os CISP ficarão impossibilitados de apresentar propostas ou serão criados contratos mal formulados, impedindo que os clientes do setor público obtenham todas as capacidades e benefícios da cloud.*

Um RFP de serviços de cloud foca-se nos principais requisitos exigidos de um CISP e de serviços de cloud, garantindo que os fornecedores qualificáveis para o LOTE 1 cumprem os mais elevados padrões. Os requisitos também devem evitar ser demasiado prescritivos para não limitarem o acesso do setor público a uma vasta gama de CISP qualificados.

Exemplo de linguagem de RFP: capacidades do fornecedor 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 datacenters. Cada cluster deve ser composto por, pelo menos, dois datacenters com ligações de baixa latência para permitir implementações ativo-ativo de alta disponibilidade e implementações de cenários DR-BC. Os datacenters que contêm cada cluster têm de estar fisicamente isolados e ter independência de falhas entre si.	*O CISP tem 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 podem ser replicados pelo CISP fora dessas regiões.	*Os requisitos de residência de dados impõem que o cliente tenha um controlo total sobre onde estão os seus dados.*
O CISP tem de ter a capacidade de fornecer conectividade direta, dedicada e privada entre os datacenters do CISP.	*A conectividade privada é um requisito fundamental para conseguir construir uma infraestrutura híbrida e segura.*
O CISP deve fornecer mecanismos suficientes, que incluem encriptação de dados em trânsito.	*O cliente pode exigir que exista uma capacidade com a qual os dados não podem transitar desencriptados.*
Certificações mínimas do CISP	
O CISP deve ter a certificação ISO 27001.	*A auditoria, certificação e acreditação de terceiros garantem que os clientes podem comparar serviços (e, em particular, a plataforma) para avaliar a qualidade, segurança e fiabilidade. É essencial ter um mínimo de certificações.*

O CISP deve estar em conformidade com o Código de Conduta de Proteção de Dados do CISPE, de forma a fornecer funcionalidades e serviços que possam ser utilizados em conformidade com o RGPD, permitindo que os clientes criem aplicações em conformidade com o RGPD.	*O cliente deve conseguir construir ou executar aplicações em conformidade com o RGPD.*
O CISP tem de disponibilizar relatórios auditados de terceiros, como os relatórios SOC 1 e 2 (que abrangem localizações e serviços utilizados pelo cliente final), para permitir transparência relativamente ao controlo e procedimentos do CISP.	*O CISP deve ser transparente quanto à forma como a aplicação é operada e gerida. Os relatórios SOC são instrumentais para garantir confiança e transparência.*
O CISP tem de aderir ao Climate Neutral Data Centre Pact.	*O Climate Neutral Data Centre Pact compromete o CISP a alcançar a neutralidade carbónica até 2030, permitindo que o utilizador cumpra os seus próprios objetivos de sustentabilidade. São obrigatórios auditores terceiros para fornecedores com mais de 250 funcionários a tempo inteiro (não aplicável a PME).*
O CISP tem de cumprir o Código de Conduta de Portabilidade para IaaS da SWIPO.	*O Código de Conduta de Portabilidade para IaaS da SWIPO garante que os serviços cumprem os requisitos do artigo. 6.º (portabilidade de dados) do Regulamento (UE) relativo a um regime para o livre fluxo de dados não pessoais na União Europeia.*
Características do serviço	
A infraestrutura do CISP tem de ser acessível através de interfaces programáticas (API) e da consola de gestão baseada na Web.	*O acesso self-service e as interfaces programáticas são um critério obrigatório dos fornecedores CISP para eliminar, tanto quanto possível, a utilização de intermediários no acesso dos utilizadores e do fornecedor em si.*
O CISP deve oferecer um conjunto base de serviços que inclua: armazenamento de objetos, base de dados relacional gerida, base de dados não relacional gerida, balanceadores de carga geridos, monitorização e escalabilidade automática integrada.	*A simples oferta de máquinas virtuais não é suficiente para qualificar um fornecedor como fornecedor de cloud. Os fornecedores de cloud devem oferecer um conjunto de serviços PaaS e IaaS para acelerar e melhorar as aplicações dos clientes.*
O CISP tem de permitir que o cliente mude livremente a utilização e configuração dos seus serviços ou que mova os dados dentro e fora do CISP (oferta self-service).	*O acesso self-service aos serviços e dados é um requisito obrigatório que permite que o cliente se torne totalmente independente.*
O CISP tem de permitir a faturação dos seus serviços num regime de "pagamento conforme a utilização".	*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 PoC.*
Segurança de dados e sistemas	
O CISP tem de permitir que o cliente retenha o controlo total dos seus dados, dando-lhe a liberdade de escolher onde os seus dados são armazenados (área urbana da cidade) e a garantia de que os dados não são movidos, a menos que pelo próprio cliente.	*O cliente tem de ter controlo sobre onde os dados são armazenados, como gerir o acesso ao conteúdo e o acesso de utilizador a serviços e recursos.*

As características do CISP têm de conceder ao cliente o controlo total sobre as suas políticas de segurança, incluindo confidencialidade, integridade e disponibilidade de dados e sistemas do cliente.	*O cliente tem de poder definir e implementar os seus padrões de segurança nas suas cargas de trabalho. Confiar no fornecedor para "fazer o que está certo" com os dados do cliente não é suficiente.*
Controlo de custos	
O CISP tem de possuir mecanismos e ferramentas para que o cliente monitorize os gastos ao longo do tempo. As ferramentas têm de permitir a segmentação básica com base em cargas de trabalho, serviços e contas.	
O CISP tem de oferecer ferramentas para alertar o cliente sempre que um limite de gastos for ultrapassado.	
O CISP tem de enviar faturas detalhadas ao cliente. Tem de existir a possibilidade de estruturar a fatura de forma a discriminar o custo por carga de trabalho, ambiente e conta.	

O CISP também deve fornecer respostas às perguntas sobre requisitos técnicos abaixo.

SOLUÇÕES

O CISP deve demonstrar como pode fornecer modelos pré-construídos e soluções de software que estejam alojadas no CISP ou que se integrem nele para as seguintes soluções:

- *Armazenamento*
- *DevOps*
- *Segurança/Conformidade*
- *Big data/Análise*
- *Aplicações empresariais*
- *Telecomunicações e redes*
- *Geoespacial*
- *IoT*
- *(Outras)*

Apresente uma descrição geral sobre como o CISP foi utilizado 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 conteúdo*
- *(Outras)*

2.2.2 Comparação de fornecedores

Além dos requisitos mínimos num RFP de serviços de cloud, é importante mencionar os critérios com os quais se pode comparar as tecnologias do CISP durante uma avaliação competitiva.

Os RFP de serviços de cloud devem solicitar os recursos de cloud necessários para uma organização, com o conhecimento do que o cliente pode utilizar esses recursos para criar a sua solução. As funcionalidades que vão além dos padrões que um CISP pode oferecer (como soluções pré-construídas pelo CISP ou funcionalidades de automatização) podem ser utilizadas para uma análise mais significativa de "opções de valor acrescentado" ou de "melhor valor" num RFP de serviços de cloud.

Normalmente, o setor público exige concorrência entre concorrentes através de critérios de avaliação como o melhor valor, proposta economicamente mais vantajosa (MEAT) ou preço mais baixo. À medida que as entidades do setor público planeiam esta parte do RFP de serviços de cloud, é importante criar uma abordagem que tenha em conta as funcionalidades exclusivas da cloud. Por exemplo, é necessário compreender que comparar apenas os itens de linha entre as ofertas de cloud dos fornecedores (por exemplo, computação ou armazenamento) não é uma forma eficaz de comparar ofertas. Em vez disso, recomendamos ter como foco soluções de nível mais elevado, como as indicadas acima na secção *2.2.1*. As entidades do setor público podem focar-se em requisitos específicos da cloud, como os indicados no *Apêndice A – Requisitos técnicos de comparação entre* os concorrentes.

Os RFP devem apresentar as características essenciais da cloud necessárias para criar a sua solução de cloud. Para isso, as organizações do setor público podem utilizar as características essenciais de cloud do Instituto Nacional de Normas e Tecnologia (NIST), além de utilizar relatórios de analistas terceiros para garantir que o CISP tem oferta mais adequada de "cloud verdadeira" e que opera em grande escala.

Exemplo de linguagem de RFP: comparação de fornecedores

Os CISP devem fornecer respostas a TODAS as perguntas relativas aos requisitos técnicos abaixo no ***Apêndice A****.*

Os inquiridos têm de possuir os seguintes atributos e descrever como as suas ofertas de serviços de cloud satisfazem as cinco características essenciais de computação na cloud[4]*.*

1) ***Self-service a pedido:*** *o inquirido tem de apresentar a capacidade de aprovisionar unilateralmente capacidades de computação, como o tempo de servidor e armazenamento de rede, conforme necessário e de forma automática, sem exigir interação humana com cada fornecedor de serviços. O inquirido deve oferecer a capacidade de aprovisionar unilateralmente serviços ao realizar pedidos (ou seja, sem a análise nem aprovação do fornecedor). Explique como isto funciona com a sua oferta ou com a oferta que representa.*

2) ***Acesso universal à rede:*** *o inquirido tem de fornecer diversas opções de conectividade de rede, sendo uma delas baseada na Internet. Explique como isto funciona com a sua oferta ou com a oferta que representa.*

3) ***Agrupamento de recursos:*** *o CISP do inquirido tem de fornecer recursos de computação agrupados que sirvam os diversos consumidores através um modelo multi-inquilino com diferentes recursos virtuais atribuídos de forma dinâmica e reatribuídos de acordo com a procura do consumidor. O utilizador consegue especificar a localização a um nível mais elevado de abstração (por exemplo, país, região ou localização do datacenter). O inquirido deve suportar a escalabilidade desses recursos em minutos ou horas após o pedido de aprovisionamento. Explique como isto funciona com a sua oferta ou com a oferta que representa.*

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

*4) **Elasticidade rápida:** o CISP do inquirido deve suportar capacidades de aprovisionamento e desaprovisionamento (aumentar e reduzir a escala verticalmente) de serviços, disponibilizando o serviço dentro dos tempos mínimos prescritos (máximo de "x" horas) após o pedido de aprovisionamento. O inquirido deve suportar os ajustes de faturação resultantes destes pedidos de aprovisionamento diariamente, tanto por hora como por dia.*

*5) **Serviço medido:** o inquirido deve oferecer visibilidade quanto à utilização do serviço através de um painel online ou meios eletrónicos semelhantes.*

Além disso, o CISP deve:

- *Ser um líder reconhecido no fornecimento de serviços de cloud, conforme demonstrado pelo Magic Quadrant da Gartner para IaaS[5].*
- *Fornecer relatórios de analistas terceiros reconhecidos no setor que demonstrem a fiabilidade e as capacidades comprovadas do CISP.*

Por fim, os CISP serão comparados através dos cenários apresentados no Apêndice B.

2.2.2.1 Acordos de Nível de Serviço (SLA)

Os CISP fornecem SLA comerciais estandardizados a milhões de clientes e, como tal, não podem oferecer SLA personalizados, como é o caso de um modelo de datacenter on-premises. No entanto, os clientes do CISP (normalmente auxiliados por parceiros) podem arquitetar a sua utilização da cloud para aproveitar os SLA comerciais de um CISP de modo a cumprir e superar os requisitos específicos do cliente e SLA exclusivos.

Os RFP de serviços de cloud devem garantir que os CISP oferecem as capacidades e as orientações necessárias para tirar partido dos seus serviços e SLA comerciais, para que os utilizadores finais individuais possam cumprir os requisitos de desempenho e disponibilidade.

Exemplo de linguagem de RFP: Acordos de Nível de Serviço

Forneça informações e ligações sobre a abordagem dos CISP aos Acordos de Nível de Serviço (SLA).

*A **<ORGANIZAÇÃO>** terá conhecimento sobre os SLA do CISP e implementará cargas de trabalho e aplicações importantes de forma a que continuem a operar no caso de um SLA não ser cumprido.*

*A **<ORGANIZAÇÃO>** será responsável pela manutenção dos SLA adequados associados a qualquer equipamento da **<ORGANIZAÇÃO>** ou serviços operados pela **<ORGANIZAÇÃO>** utilizados com o CISP.*

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

2.2.3 Contratação

Os termos e condições do CISP foram criados para refletir como funciona um modelo de serviço de cloud (os ativos físicos não estão a ser comprados e os CISP operam em grande escala oferecendo serviços estandardizados), portanto é importante que os termos e condições do CISP

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

sejam incorporados e utilizados ao máximo na medida do possível. Consulte a secção *2.5* abaixo para obter mais informações sobre termos e condições e contratação.

2.2.3.1 Serviços novos e em mudança

Os CISP oferecem desempenho através de um serviço. Contrariamente às soluções on-premises tradicionais, que necessitam de atualizações e contratos de manutenção de serviço que têm data de validade, os fornecedores de cloud oferecem apenas o serviço estandardizado. Para que o modelo de cloud atinja economias de escala, as atualizações e alterações à infraestrutura subjacente são implementadas para todos os utilizadores (não apenas para utilizadores específicos) e, em seguida, os clientes podem escolher os serviços que utilizam. O serviço funciona de forma mais integrada do que os tradicionais sistemas on-premises e os fornecedores de cloud estão constantemente a adicionar serviços novos e melhorados para que os clientes os utilizem como pretenderem.

Se não for possível adicionar serviços novos ou melhorados do CISP após o prazo de envio do RFP, as organizações do setor público não poderão utilizar novos serviços ou funcionalidades melhoradas até que a próxima versão de um acordo-quadro seja lançada. Portanto, recomendamos que o aprovisionamento dos serviços descritos no acordo-quadro seja amplo de forma a permitir a adição de novos serviços do CISP após o prazo de envio. A legislação da UE em matéria de aquisições pode restringir a introdução de novos serviços do CISP sensivelmente diferentes no acordo-quadro, mas as atualizações e as novas versões de serviços que não sejam consideradas alterações substanciais poderão ser adicionadas sem qualquer impedimento ao nível de aquisição.

Exemplo de linguagem de RFP: serviços novos e em mudança

O CISP deve fornecer uma solução económica que utilize tecnologias de virtualização comprovadas e estáveis e também tecnologias inovadoras constantemente atualizadas. A ***<ORGANIZAÇÃO>*** *reconhece e concorda que as tecnologias de cloud podem ser fornecidas numa base de serviço partilhado à* ***<ORGANIZAÇÃO>*** *e a outros clientes do CISP de um código base comum e/ou ambiente comum e que o CISP pode, periodicamente: alterar, adicionar ou eliminar as funções, as funcionalidades, o desempenho ou outras características dos serviços de cloud e, se essa alteração, adição ou eliminação for feita, as especificações do serviço de cloud serão adequadamente corrigidas.*

O âmbito deste pedido de entrega inclui todos os serviços do CISP existentes, novos ou melhorados ***AO ABRIGO DO ACORDO-QUADRO****. Os serviços de cloud fornecidos pelo CISP disponíveis para clientes comerciais devem ser disponibilizados à* ***<ORGANIZAÇÃO>****.*

2.2.3.2 Dependência de um fornecedor e reversibilidade

A tecnologia de cloud reduz a dependência de um fornecedor, pois não existe uma compra de ativos físicos e os clientes podem mover os seus dados de um fornecedor de cloud para outro a qualquer momento.

No entanto, é inevitável que exista um determinado nível de dependência de um fornecedor aquando da compra de serviços de cloud, pois nem todas as clouds são iguais. Um CISP pode oferecer serviços e capacidades que outro CISP não oferece, o que acaba por reduzir a capacidade de utilizar esses serviços com outro fornecedor. Uma abordagem prudente é exigir que os CISP ofereçam as funcionalidades e serviços necessários para deixar de utilizar a sua cloud, incluindo documentação sobre como utilizar esses serviços com uma "estratégia de saída" razoável, visto que

é impossível que um CISP conheça a configuração exclusiva da utilização dos seus serviços estandardizados por parte de um cliente e, como tal, que forneça um plano de saída personalizado.

Consulte a secção 2.3.1.2 para obter informações sobre códigos de conduta do setor para abordar a "portabilidade de dados" e a "mudança de fornecedor de serviço de cloud" a fim de cumprir os requisitos do artigo 6.º do Regulamento (UE) relativo a um regime para o livre fluxo de dados não pessoais na União Europeia.

Exemplo de linguagem de RFP: integração e saída

*A **<ORGANIZAÇÃO>** procura propostas que forneçam uma estratégia de saída razoável para evitar a dependência de um fornecedor. A **<ORGANIZAÇÃO>** não está a comprar ativos físicos e o CISP irá oferecer a possibilidade de ampliar e reduzir as pilhas de TI. O CISP irá fornecer serviços e ferramentas de portabilidade para ajudar a migrar de e para a plataforma do CISP, minimizando a dependência de um fornecedor. A documentação detalhada sobre como utilizar as ferramentas e os serviços de portabilidade do CISP servirá de plano de saída razoável.*

*O CISP não deve ter compromissos mínimos **obrigatórios** 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 seja necessário, para dentro ou para fora do armazenamento do CISP. O CISP também deverá permitir que as imagens da máquina virtual sejam descarregadas e transferidas para um novo fornecedor de cloud. A **<ORGANIZAÇÃO>** pode exportar as suas imagens de máquina e utilizá-las on-premises ou noutro fornecedor (sujeito a restrições de licenciamento de software).*

2.3 Segurança

A segurança e conformidade são responsabilidades partilhadas entre o CISP e os clientes de cloud. Neste modelo, os clientes da cloud controlam a forma como arquitetam e protegem as suas aplicações e dados na infraestrutura, enquanto os CISP são responsáveis por fornecer serviços numa plataforma controlada e altamente segura e por fornecer um amplo conjunto de funcionalidades de segurança adicionais. O nível de responsabilidades do CISP e do cliente neste modelo depende do modelo de implementação de cloud (IaaS/PaaS/SaaS). Além disso, deve ser claro para os clientes quais são as suas responsabilidades em cada modelo.

Compreender este modelo de responsabilidade partilhada é crucial para a elaboração de um bom RFP de serviços de cloud. As organizações do setor público devem garantir que sabem de facto quais são as responsabilidades de um CISP, as suas próprias responsabilidades e no que podem ajudar os parceiros de consultoria/ISV e respetivas soluções.

2.3.1 Requisitos mínimos

Quando o assunto é segurança na cloud, a palavra-chave é **capacidade.** As organizações do setor público devem ser exigentes com os CISP e exigir que forneçam as capacidades de segurança necessárias para garantir que os clientes cumprem todas as suas responsabilidades no modelo de responsabilidade partilhada. Conforme indicado na lista de requisitos representativos abaixo, o CISP é incumbido de fornecer uma capacidade estandardizada que o cliente utiliza para proteger o seu ambiente de cloud exclusivo.

- ***Fornecer capacidades** de firewall de rede e firewall de aplicações Web para criar redes privadas e controlar o acesso a instâncias e aplicações.*
- ***Fornecer opções** de conectividade que permitam ligações privadas ou dedicadas do seu escritório ou ambiente on-premises.*
- ***Fornecer** a **capacidade** de implementar uma defesa profunda e impedir ataques de DDoS.*
- ***Capacidades** de encriptação de dados, disponíveis em serviços de armazenamento e bases de dados.*
- ***Fornecer opções** de gestão de chaves flexíveis, permitindo escolher se pretende que o CISP faça a gestão das chaves de encriptação ou deixe que o cliente tenha controlo completo sobre as chaves.*
- ***Fornecer API** para que os clientes integrem a encriptação e proteção de dados com qualquer serviço desenvolvido ou implementado num ambiente do CISP.*
- ***Fornecer ferramentas** de implementação para gerir a criação e desativação de recursos do CISP de acordo com os padrões da organização.*
- ***Fornecer ferramentas** de gestão de inventário e configuração para identificar recursos do CISP e controlar e gerir alterações feitas nesses recursos ao longo do tempo.*
- ***Fornecer ferramentas** e funcionalidades que permitam aos clientes ver exatamente o que acontece no seu ambiente do CISP.*
- ***Permitir uma visibilidade** detalhada das chamadas de API, incluindo de quem, de quê e de onde as chamadas foram feitas.*
- ***Fornecer opções** e agregação de registos, simplificação de investigações e relatórios de conformidade.*
- ***Fornecer** a capacidade de configurar notificações de alerta quando ocorrerem eventos específicos ou os limites forem excedidos.*
- ***Fornecer capacidades** para definir, aplicar e gerir políticas de acesso de utilizador nos serviços do CISP.*
- ***Fornecer** a **capacidade** para definir contas de utilizador individuais com permissões em recursos do CISP.*
- ***Fornecer** a **capacidade** para integrar e federar com diretórios corporativos para reduzir a sobrecarga administrativa e melhorar a experiência do utilizador final.*

Pode encontrar mais requisitos no *Apêndice A – Requisitos técnicos de comparação entre os concorrentes*.

As funcionalidades que vão além do padrão mínimo de segurança podem ser utilizadas para uma análise mais significativa de "opções de valor acrescentado" ou "melhor valor" num RFP. Relativamente à segurança, quanto mais funcionalidades integradas ou automatizadas, melhor. Mais uma vez, consulte o *Apêndice A – Requisitos técnicos de comparação entre os concorrentes* para ver os requisitos para a comparação entre concorrentes.

As organizações do setor público devem recorrer a certificações e avaliações de acreditação de cloud para garantir que os controlos de segurança do CISP são implementados. Por exemplo: pense num 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, aprofunda os controlos específicos aos quais o CISP adere em conformidade com os requisitos da ISO relativamente a aquisição, desenvolvimento e manutenção do sistema. É provável que esses controlos abranjam a maioria, se não todos, os controlos relacionados com aquisição, desenvolvimento e manutenção do sistema que, normalmente, seriam pedidos por uma organização num RFP relacionado com TI. Portanto, faz sentido que uma organização apenas exija que um CISP tenha a certificação ISO 27001, em vez de duplicar os esforços e indicar os requisitos de controlo relativamente a aquisição, desenvolvimento e manutenção do sistema num RFP de serviços de cloud.

Esta abordagem de tirar partido de relatórios de conformidade de terceiros pode ser aplicada a muitos controlos de segurança e conformidade, como o Código de Conduta de RGPD do CISPE, ISO, SOC, entre outros.

Exemplo de linguagem de RFP: segurança

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

O CISP deve indicar as suas funções e responsabilidades em matéria de segurança e conformidade:

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

PROPRIEDADE E CONTROLO DOS CONTEÚDOS DA <ORGANIZAÇÃO>

Descreva como as capacidades do CISP podem proteger a privacidade de dados da <ORGANIZAÇÃO>. Inclua os controlos implementados para gerir a proteção de conteúdos da <ORGANIZAÇÃO>. O CISP tem de oferecer um forte isolamento regional, para que os objetos armazenados numa região nunca deixem a região, a menos que a <ORGANIZAÇÃO> os transfira explicitamente para outra região.

- *A <ORGANIZAÇÃO> irá gerir o acesso aos respetivos conteúdos, serviços e recursos. O CISP deve fornecer um conjunto avançado de funcionalidades de acesso, encriptação e registo para ajudar a <ORGANIZAÇÃO> a fazê-lo de forma eficaz. O CISP não irá aceder nem utilizar conteúdos da <ORGANIZAÇÃO> para quaisquer fins que não sejam os legalmente exigidos e necessários para manter os serviços do CISP e fornecê-los à <ORGANIZAÇÃO> e aos respetivos utilizadores finais.*
- *A <ORGANIZAÇÃO> irá escolher as regiões em que os seus conteúdos serão armazenados. O CISP não irá mover nem replicar os conteúdos da <ORGANIZAÇÃO> para fora das regiões escolhidas pela mesma, exceto quando legalmente exigido e necessário para manter os serviços do CISP e fornecê-los à <ORGANIZAÇÃO> e aos respetivos utilizadores finais.*
- *A <ORGANIZAÇÃO> irá escolher como pretende proteger os seus conteúdos. O CISP deve fornecer uma encriptação sólida para os conteúdos da <ORGANIZAÇÃO>, seja em trânsito ou inativos, e dar a opção para que a <ORGANIZAÇÃO> faça a gestão das suas próprias chaves de encriptação.*
- *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 controlo de segurança do CISP. Estes processos de controlo e proteção de segurança são validados de forma independente por várias avaliações independentes de terceiros.*

As avaliações e certificações de acreditação da cloud fornecem garantias às organizações do setor público de que os CISP têm controlos de segurança físicos e lógicos eficazes em vigor. Quando estas acreditações são utilizadas nos RFP, simplificam o processo de aquisição e ajudam a evitar processos duplicados e demasiado onerosos ou fluxos de trabalho de aprovação que podem não ser exigidos para um ambiente de cloud.

Os RFP de serviços de cloud devem dar aos CISP a oportunidade de comprovar se estão em linha com as acreditações e avaliações de conformidade. Conforme mencionado acima, existe uma sobreposição considerável nos cenários de risco e práticas de gestão de risco nestes esquemas de acreditação. Como os controlos e requisitos são agrupados nessas acreditações, exigir que os CISP as cumpram é a forma mais rápida de abordar a conformidade num RFP, em vez de duplicar o trabalho de indicar esses controlos individuais **(muitos dos quais extraídos de RFP anteriores que estão diretamente em datacenters on-premises e, por isso, podem não ser aplicáveis à computação na cloud)**.

NOTA: também é muito importante compreender como é possível aceder aos relatórios indicados abaixo. Por exemplo, os relatórios SOC 1 e SOC 2 costumam ser documentos sensíveis. Deve compreender os requisitos necessários para aceder aos mesmos (por exemplo, a assinatura de um acordo de confidencialidade [NDA]) e não simplesmente pedir que esses documentos sejam enviados como parte da resposta ao RFP (esses documentos poderiam ser tornados públicos por leis de registos abertos [open records] ou legislação semelhante, o que poderia comprometer a segurança na cloud).

Exemplo de linguagem de RFP: conformidade

A utilização de padrões reconhecidos de segurança, conformidade e operações, derivados das melhores práticas nas operações de serviços de cloud (incluindo o manuseamento de dados, segurança de dados, confidencialidade, disponibilidade, etc.), simplifica a aquisição de tecnologia de cloud.

A **<ORGANIZAÇÃO>** *irá avaliar as ofertas de propostas exclusivas em relação aos padrões aceites de segurança, conformidade e operações, conforme descrito abaixo e no* **Apêndice A***. Ao confiar na certificação de conformidade do fornecedor em relação a cada padrão, a* **<ORGANIZAÇÃO>** *pode utilizar a conformidade mínima com o padrão como referência de avaliação da proposta.*

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

O CISP que está a apresentar a proposta (diretamente ou através de um revendedor) deve ter a capacidade de demonstrar que consegue cumprir os seguintes relatórios, atestações e certificações independentes de terceiros. (Nota: se alguns destes relatórios, atestações e certificações estiverem sob restrições de divulgação por questões de riscos de segurança, a **<Organização>** *trabalhará com o CISP para chegar a um consenso sobre o acesso):*

Certificações/Atestações	*Leis, regulamentos e privacidade*	*Alinhamentos/Enquadramentos*
☐ *C5 (Alemanha)*		☐ *CDSA*
☐ *Código de Conduta de Proteção de Dados do CISPE (RGPD)*		
☐ *CNDCP (*Pacto para a neutralidade climática em datacenters*)*		
☐ *DIACAP*	☐ *Diretiva relativa à proteção de dados da UE*	☐ *CIS*
☐ *DoD SRG, níveis 2 e 4*	☐ *Cláusulas-tipo da UE*	☐ *Criminal Justice Info. Service (CJIS)*
☐ *HDS (França, saúde)*		

☐ *FedRAMP*	☐ *FERPA*	☐ *CSA*
☐ *FIPS 140-2*	☐ *RGPD*	☐ *Escudo de Proteção da Privacidade UE-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 (Singapura)*	☐ *PDPA – 2010 (Malásia)*	☐ *ICREA*
☐ *PCI DSS, nível 1*	☐ *PDPA – 2012 (Singapura)*	☐ *IT Grundschutz (Alemanha)*
☐ *Regra SEC 17-a-4(f)*	☐ *PIPEDA (Canadá)*	☐ *MARS – E*
☐ *SecNumCloud (França)*		
☐ *SOC1/ISAE 3402*	☐ *Lei da Privacidade (Austrália)*	☐ *MITA 3.0*
☐ *SOC2/SOC3*	☐ *Lei da Privacidade (Nova Zelândia)*	☐ *MPAA*
☐ *Código para IaaS da SWIPO*		
	☐ *Autorização da APD de Espanha*	☐ *NIST*
	☐ *DPA do Reino Unido (1988)*	☐ *Níveis do Uptime Institute*
	☐ *VPAT/Secção 508*	☐ *Princípios de segurança na cloud do Reino Unido*

A lista acima serve apenas para fins ilustrativos e não deve ser considerada para todas as certificações e padrões que se podem aplicar aos serviços de cloud.

2.3.1.1 Proteção de dados

Uma consideração essencial a ter aquando da utilização de serviços de cloud é que o tratamento de dados pessoais é realizado em conformidade com a lei relativa à proteção de dados da UE, incluindo o Regulamento Geral sobre a Proteção de Dados (RGPD). O RGPD é um regulamento baseado em princípios e, como tal, não fornece orientações específicas a um setor para ajudar a garantir a conformidade. No entanto, o RGPD incentiva a adoção de ferramentas de conformidade, como códigos de conduta, para fornecer tais orientações. O CISPE, em colaboração com a autoridade de proteção de dados francesa (CNIL), desenvolveu um Código de Conduta para Proteção de Dados (Código do CISPE[6]), aprovado pelo Comité Europeu para a Proteção de Dados com uma aplicabilidade geral na Europa. O objetivo do código é ajudar os CISP a cumprir o RGPD e orientar os clientes a avaliar se os CISP são adequados para o tratamento de dados pessoais que o cliente pretende realizar.

[6] https://cispe.cloud/code-of-conduct/

- O código foca-se exclusivamente no setor de IaaS e aborda as funções e responsabilidades específicas dos fornecedores de IaaS.
- Ajuda a clarificar os aspetos do tratamento justo e transparente e de medidas de segurança adequadas no contexto de serviços de infraestrutura de cloud (RGPD, artigo 40.º [2]).
- Ajuda os clientes a compreender como podem manter a soberania sobre os seus dados ao garantir que permanecem dentro da UE.
- Promove as melhores práticas de proteção de dados que suportam a iniciativa GAIA-X da UE para o desenvolvimento de serviços de dados de cloud europeus.

A conformidade do CISP com códigos de conduta de proteção de dados, como o Código do CISPE, garante que os dados pessoais serão tratados em conformidade rigorosa com o RGPD.

Exemplo de linguagem de RFP: proteção de dados

O CISP que está a apresentar a proposta (quer seja diretamente ou através de um revendedor) deve ser capaz de demonstrar que consegue cumprir um Código de Conduta de Proteção de Dados, como o Código do CISPE. O código de proteção de dados tem de estar alinhado com os requisitos definidos na estrutura do RGPD. O código deve incluir no mínimo: (1) uma clara definição das funções e responsabilidades do CISP; (2) o requisito de que o CISP não irá utilizar os dados dos clientes para efeitos de marketing ou publicidade e (3) a capacidade dos clientes de selecionarem serviços do CISP que permitam que os dados sejam tratados totalmente dentro do Espaço Económico Europeu. A conformidade com o código tem de ser verificada por auditores independentes externos (órgãos de monitorização) acreditados pela Autoridade Europeia para a Proteção de Dados.

2.3.1.2 Mudança de fornecedores de cloud e portabilidade de dados

Os clientes devem ter a liberdade de escolher os serviços de cloud que pretendem utilizar e não estarem dependentes de um CISP ou fornecedor de PaaS/SaaS.

Os serviços de cloud fornecidos por um CISP são estandardizados e oferecidos numa base "um para muitos", com serviços configurados, aprovisionados e controlados pelo cliente. Um benefício da computação na cloud é que os clientes têm a capacidade de escolher quaisquer serviços estandardizados de que precisem para desenvolver as suas soluções e aplicações únicas. Este benefício também permite mudar para serviços novos ou diferentes que melhor se adequem às necessidades particulares do cliente a qualquer altura.

Tal como a proteção de dados, os códigos de conduta podem oferecer garantias e confiança aos clientes ao mudarem de uma infraestrutura on-premises para a cloud ou aquando da mudança de CISP. Juntamente com a EuroCIO (associação europeia de CIO), o CISPE copresidiu o desenvolvimento do Código de Conduta de Portabilidade de Dados e Mudança de Serviços de Cloud para Serviços de Cloud IaaS (Código para IaaS da SWIPO [7,8]). A primeira versão do código foi desenvolvida em conformidade com o Regulamento (UE) relativo a um regime para o livre fluxo de dados não pessoais na União Europeia, entregue à Comissão Europeia em novembro de 2019 sob a presidência finlandesa e publicado pela associação SWIPO AISBL em maio de 2020. Em abril

[7] https://ec.europa.eu/digital-single-market/en/news/cloud-stakeholder-working-groups-start-their-work-cloud-switching-and-cloud-security
[8] https://swipo.eu/

de 2021, a SWIPO AISBL declarou que os primeiros serviços estavam em conformidade com o código e, em maio de 2021, foi anunciado que os primeiros serviços dos membros CISPE estavam em conformidade com o código.

Exemplo de linguagem de RFP: mudança de fornecedores de cloud e portabilidade de dados

O CISP que está a apresentar a proposta (diretamente ou através de um revendedor) deve ser capaz de demonstrar a sua capacidade de cumprir um código de conduta de "mudança e portabilidade de dados", como o Código para IaaS da SWIPO. O código tem de mostrar em detalhe como o CISP garante ao cliente uma transferência de dados empresariais segura, caso pretenda mudar de CISP.

2.3.2 Comparação de fornecedores

Assim como nos critérios técnicos nas secções acima, além dos requisitos mínimos de segurança num RFP de serviços de cloud, é importante fornecer critérios pelos quais as capacidades e serviços de segurança do CISP possam ser comparadas durante uma avaliação competitiva.

Consulte *Apêndice A – Requisitos técnicos de comparação entre os concorrentes* para ver exemplos de requisitos de segurança do CISP. Recomendamos que as capacidades abaixo sejam considerações de segurança essenciais para as entidades do setor público que avaliam os CISP:

Exemplo de linguagem de RFP: principais considerações de segurança

- *O CISP tem de compreender a documentação e o modelo de responsabilidade partilhada para ajudar os clientes a compreender a delineação das responsabilidades de segurança para as funcionalidades e os serviços do CISP (por exemplo, no contexto do RGPD)*
- *Histórico comprovado da segurança da infraestrutura do CISP, com documentação não proprietária publicamente disponível sobre o procedimento de segurança e os controlos físicos/lógicos do CISP*
- *Suporte do CISP específico para segurança na cloud*
- *Serviços que possibilitem aos clientes formalizar o design da conta, automatizar e segurança e os controlos de governança de cloud e simplificar a auditoria*
- *A capacidade de criar, aprovisionar e gerir um conjunto de recursos como num modelo (inclui modelos de segurança padrão de excelência do CISP/parceiro do CISP)*
- *A capacidade de estabelecer operações de controlos fiáveis e repetíveis*
- *Funcionalidades para auditoria contínua e em tempo real*
- *A capacidade de desenvolvimento de scripts de políticas de governança de cloud*
- *A capacidade de criar funções forçadas que não podem ser ignoradas pelos utilizadores que não tenham permissão para alterar essas funções*
- *A capacidade de executar a implementação fiável do que foi anteriormente escrito em políticas, padrões e regulamentos, além de aplicar segurança e conformidade, o que ,por sua vez, cria um modelo de governança de cloud fiável para ambientes de TI*
- *Serviços para proteger contra os ataques distribuídos de negação de serviço (DDoS) comuns e mais frequentes da camada de transporte e rede, juntamente com a capacidade de gravar regras personalizadas para mitigar ataques sofisticados da camada de aplicação*
- *Serviço gerido de deteção de ameaças*

2.3.3 Contratação

Conforme observado anteriormente, os termos e condições do CISP foram criados para refletir como sobre funciona um modelo de serviço de cloud (os ativos físicos não estão a ser comprados e os CISP operam em grande escala, oferecendo serviços estandardizados). Por isso, é importante que os termos e condições do CISP sejam incorporados e utilizados o mais amplamente possível. Consulte a secção *2.5* abaixo para obter mais informações sobre termos e condições e contratação.

Relativamente a segurança, mais uma vez recomendamos permitir que os CISP atualizem constantemente as suas ofertas ou que os fornecedores possam adicionar produtos após o prazo de envio, desde que estejam em conformidade com os parâmetros originais do RFP. Isto deve-se ao facto de os recursos e serviços de segurança evoluírem rapidamente e de os CISP disponibilizarem serviços focados em segurança frequentemente, que em muitos casos podem ser utilizados gratuitamente. Tenha em atenção que é importante ter um nível de segurança básico (consulte os requisitos mínimos acima) para garantir que as alterações às ofertas de segurança não são prejudiciais.

O modelo de responsabilidade partilhada está, obviamente, no centro da segurança num RFP de serviços de cloud. Cada interveniente tem de compreender claramente as suas responsabilidades de segurança e o CISP deve ser encarregado de documentar as responsabilidades de segurança do CISP e do cliente para as tecnologias de cloud fornecidas pelo CISP, juntamente com a documentação que ajuda os clientes a criar e automatizar as melhores práticas de segurança.

Um acordo-quadro de cloud deve fornecer flexibilidade para remover um fornecedor no caso de este deixar de cumprir os requisitos mínimos de segurança e conformidade, conforme previsto no RFP de serviços de cloud.

2.4 Preços

Para contratar tecnologia de cloud ao considerar flutuações de procura, as organizações do setor público precisam de um contrato que lhes permita pagar pelos serviços conforme são utilizados e com a governança e visibilidade da cloud exigidas relativamente à utilização e despesas.

É importante que os RFP de serviços de cloud considerem o valor e o custo total de propriedade (TCO), em vez de uma simples comparação de preços por unidade. Esta prática tradicional de analisar o menor preço por unidade não é aplicável ao modelo de cloud, pois não basta procurar a proposta mais vantajosa economicamente ou o menor preço total.

Para auxiliar na avaliação de preços do CISP, primeiro deve-se ter a pré-qualificação ou lista de preferências de CISP, com os ***requisitos mínimos relacionados com preços,*** *para que os CISP com menos capacidades possam qualificar-se para o acordo-quadro. No processo de avaliação para call-offs e miniconcursos, pode-se analisar uma seleção de arquiteturas de cloud e* ***cenários de preços*** *típicos de exemplo, que correspondam a algumas cargas de trabalho típicas do setor público, e solicitar aos CISP que definam os preços. Também são recomendadas demonstrações de testes em tempo real para permitir a comparação de desempenho e elasticidade dos serviços de tecnologias de cloud fornecidos pelos CISP. Consulte o Apêndice B para ver um exemplo de guião de teste para tecnologias de cloud.*

2.4.1 Requisitos mínimos

A secção de preços num RFP de serviços de cloud é composta por quatro elementos principais:

1. **Preços de utilitários:** os clientes de cloud estão a incorporar o modelo utilitário de pagamento conforme a utilização, pelo qual, ao final de cada mês, pagam apenas pelo que utilizaram, o que é excelente para as métricas de utilização e recursos.
2. **Preços transparentes:** os preços do CISP devem ser transparentes e estar publicamente disponíveis.
3. **Preços dinâmicos:** inclui a flexibilidade de permitir que os preços da cloud variem com base nos preços do mercado. Esta abordagem tira partido da natureza dinâmica e competitiva dos preços de cloud, além de ajudar na inovação e nas reduções de preços.
4. **Controlo de gastos:** os CISP devem fornecer ferramentas de criação de relatórios, monitorização e previsão que permitam aos clientes: (1) monitorizar a utilização e os gastos em níveis detalhados e resumidos; (2) receber alertas de quando a utilização e os gastos atingem os limites personalizados e (3) estimar a utilização e os gastos para planear futuros orçamentos de cloud.

Exemplo de linguagem de RFP: preços

A <ORGANIZAÇÃO> solicita que os CISP participantes incluam o seu método proposto e modelo de preços para oferecer os seus serviços aos utilizadores finais como uma capacidade de cloud comercial.

O CISP deve fornecer:

- *Documento de definição de serviços ou ligações para definições de serviços*
- *Documento de termos e condições*
- *Documento de preços (as ligações para preços públicos são aceitáveis desde que exista uma tabela de preços ou um documento de preços completo disponível mediante solicitação)*

O preço será o custo da configuração mais comum do serviço. Os CISP devem fornecer opções de descontos com base no volume, além de ferramentas de calculadora de preços para saber o preço real do que está a ser comprado, e o valor geral fornecido ao comprador (por exemplo, serviços para otimização e a redução de custos resultante).

Os compradores ao abrigo do acordo-quadro podem pedir aos fornecedores que expliquem a descrição do serviço, os termos e condições, os preços ou os documentos/modelo de definição de serviços. Será mantido um registo de todas as conversas com os fornecedores.

Requisitos adicionais de preços

- *Forneça um modelo de preços dinâmico para as tecnologias de cloud, que proporcione a máxima flexibilidade empresarial e permita escalabilidade e crescimento.*
- *Os atributos dos preços têm de incluir:*
  - *Os preços são fornecidos num serviço a pedido de estilo utilitário com pagamento conforme a utilização? Explique o seu modelo de preços.*
  - *Garante descontos adicionais se existir um compromisso de utilização e/ou compra em volume? Forneça detalhes sobre como o fará.*

- *Os preços são transparentes e estão disponíveis publicamente? Inclua ligações para os preços disponíveis publicamente.*
- *Os preços são dinâmicos e respondem de forma rápida e eficiente à concorrência no mercado?*
- *Fornece as melhores práticas e recursos para controlar os gastos?*
- *Fornece as melhores práticas e recursos para a otimização de custos?*

Transparência de preços
*Devido à constante tendência decrescente dos preços nas tecnologias de cloud comerciais como consequência da inovação e concorrência, o custo da unidade de serviço medido do CISP pago pela **<ORGANIZAÇÃO>**, ao abrigo do acordo-quadro, nunca deve exceder o preço unitário do fornecedor de cloud publicado no site do fornecedor, que passa a vigorar no momento em que a unidade de serviço é consumida pelo cliente.*

Alertas/relatórios sobre orçamentação e faturação
*Para demonstrar a entrega e utilização das tecnologias de cloud, os CISP devem fornecer à **<ORGANIZAÇÃO>** as ferramentas para gerar relatórios de faturação detalhados que discriminam os custos por hora, dia ou mês, por cada conta numa organização, por produto ou recurso do produto ou por etiquetas definidas pelo cliente. A **<ORGANIZAÇÃO>** reconhece que, como parte do modelo de responsabilidade partilhada de cloud, a **<ORGANIZAÇÃO>** será responsável pela utilização das funcionalidades e ferramentas de orçamentos e faturação fornecidas pelo CISP para dar resposta aos requisitos exclusivos de previsão e relatórios.*

- *Forneça informações sobre como a **<ORGANIZAÇÃO>** pode exibir informações de faturação em níveis detalhados e resumidos, visualizando padrões de gastos com recursos do CISP ao longo do tempo, além da previsão de despesas futuras.*
- *Forneça informações sobre como a **<ORGANIZAÇÃO>** pode filtrar a visualização de utilização/faturação por serviço, por conta associada ou por etiquetas personalizadas aplicadas aos recursos e crie alertas de faturação que enviem notificações quando a utilização dos serviços atingir ou exceder os limites/orçamentos definidos pela **<ORGANIZAÇÃO>**.*
- *Forneça informações sobre como a **<ORGANIZAÇÃO>** pode prever a utilização dos serviços de cloud durante um período de previsão definido, com base em utilização anterior. O CISP deve oferecer uma **estimativa** de quanto irá faturar à **<ORGANIZAÇÃO>** e permitir que a **<ORGANIZAÇÃO>** utilize alarmes e orçamentos para montantes previstos de utilização, de forma a melhorar a gestão de custos e despesas.*

2.4.2 Comparação de fornecedores

As organizações do setor público geralmente exigem que, aquando da competição entre os concorrentes, existam critérios de avaliação, como o melhor valor, a proposta economicamente mais vantajosa (MEAT) ou o menor preço. Durante o planeamento dos preços de call-offs ou miniconcursos do acordo-quadro, é importante criar uma abordagem que tenha em consideração as funcionalidades exclusivas da cloud. Por exemplo, é necessário compreender que comparar apenas os itens de linha entre ofertas de fornecedores de cloud (como computação ou armazenamento) não é uma forma eficiente de comparação, pois não tem em consideração funcionalidades como desempenho, otimização de custos com serviços nativos de cloud e ferramentas de monitorização do CISP ou serviços diferenciados que os CISP possam oferecer gratuitamente. Além disso, o preço de catálogo de um CISP pode ter dezenas de milhares de itens de linha e os modelos de preços são diferentes entre serviços e entre fornecedores.

Analisar o TCO

Recomendamos que se foque no custo total de propriedade (TCO) de casos de utilização definidos, que têm em consideração todos os aspetos de uma solução de cloud (incluindo serviços de parceiros, descontos estandardizados do CISP, funcionalidades técnicas 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 alojamento na Web ou implementação de um sistema de recursos humanos com um x número de utilizadores, etc.) podem incluir variáveis como a velocidade e escala dos recursos, desempenho da aplicação ou solução, tempos 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 o processamento de elevados volumes, por exemplo, na altura da entrega de impostos e notificações de emergência, como avisos de cheias. Os cenários devem ser abrangentes e incluir o âmbito da tecnologia e dos serviços que o cliente pode utilizar durante o projeto. Desta forma, o cliente consegue comparar o custo total estimado do projeto.

Comparar cenários de forma financeira e técnica

Também é importante ter em consideração as vantagens técnicas ao comparar preços entre ofertas de CISP. Por exemplo, um CISP pode permitir que os clientes criem uma topologia de recuperação de desastres (DR) ativo-ativo graças ao seu modelo de datacenters em clusters numa região geográfica. Um CISP que não tenha esse tipo de redundância e configuração de datacenter pode ser x% mais caro, considerando o custo das necessidades de recuperação de desastres. Como exemplo do motivo pelo qual uma abordagem holística aos preços que inclua funcionalidades técnicas adicionais é crucial para avaliar os CISP, considere a alternativa abaixo relativa a uma comparação direta.

Exemplo: um cliente quer comparar o preço do armazenamento de objetos fornecido por CISP qualificados num acordo-quadro. O preço do item da "unidade" de armazenamento do CISP 1 é de 0,023 €/GB. O preço da mesma "unidade" do CISP 2 é de 0,01 €/GB. Numa 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 foi concebido para sustentar a perda de dados simultânea em duas instalações diferentes e mantém diversas cópias dos dados. No caso do CISP 2, não são efetuadas cópias redundantes.
2. Qual é o nível de sustentabilidade dos objetos armazenados? O nível do CISP 1 é de 99,999999999% e o do CISP 2 é de 99%.
3. Tenha em consideração o custo durante o período de vigência da propriedade do projeto ou da carga de trabalho total e a forma como as funcionalidades de otimização de custos podem reduzir os custos quando se trata da forma como os dados são armazenados e utilizados (por exemplo, o aumento da utilização de funções sem servidor de um CISP pode reduzir os custos em x%).

Estas são apenas algumas das muitas outras considerações técnicas que envolvem preços, particularmente relacionadas com segurança e conformidade.

As considerações para cenários de preços incluem:

Taxas base: são basicamente os preços públicos dos CISP. Os CISP devem fornecer estes preços publicamente. No entanto, conforme observado acima, para comparar corretamente os CISP, os clientes podem solicitar os preços para 3 a 5 cenários específicos (ou quantos achar necessário) a todos os fornecedores. Os cenários devem ser abrangentes para incluir uma grande variedade de serviços e tecnologias que o cliente tenha a tendência de utilizar ao longo do projeto. Desta forma, o cliente consegue comparar o custo estimado total do projeto. As comparações feitas ao nível de itens de linha/SKU tendem a ser mais problemáticas do que úteis para clientes e fornecedores (os clientes precisam de comparar dezenas de milhares de itens de linha entre os diversos CISP e os fornecedores precisariam de fornecer esse nível de detalhe e geri-lo quando o preço real é determinado apenas com base na utilização do serviço).

Avaliar o conjunto abrangente de capacidades de um CISP é algo fundamental para os clientes de cloud que procuram obter o melhor valor. Por exemplo, os CISP podem dispor de serviços gratuitos ou praticamente gratuitos e uma avaliação de preços deve considerar esses serviços, visto que outros CISP podem cobrar por funcionalidades semelhantes.

Os critérios de avaliação podem ser redigidos de forma a permitirem que os CISP anunciem as suas funcionalidades "incluídas por predefinição" e como esses serviços têm impacto no custo geral. Os critérios de avaliação podem considerar também os preços com base em volume/camadas do CISP e os descontos disponíveis comercialmente, como instâncias reservadas/instâncias spot. Por exemplo:

- Poupança de x% se os clientes comprarem uma capacidade computacional reservada (1 ano, 3 anos, etc.)
- Desconto de x% no preço por camada/volume
- Poupança de x% com base nas avaliações da arquitetura e na otimização da infraestrutura, como a migração para uma opção de computação mais adequada
- Conforme observado acima, tenha em consideração o custo durante toda a duração e a forma como as funcionalidades de otimização de custos podem reduzir os custos

CENÁRIO DE PREÇOS

Os concorrentes devem fornecer os preços para o cenário abaixo apenas para fins de avaliação. O preço real terá por base a utilização dos serviços, num modelo de pagamento conforme a utilização a pedido.

Abaixo encontram-se os requisitos representativos para a determinação de preços, com o conhecimento explícito de que, durante o período de vigência do contrato, esses requisitos nominais sofrerão alterações. Apresente os preços para um modelo de utilização a pedido de 12 e 36 meses e para um modelo de capacidade reservada de 12 e 36 meses.

Indique:

- *Nome da solução ou soluções propostas:*
- *Melhor preço do concorrente:*

- *Horário de atendimento: 24 x 7 x 365*
- *Disponibilidade do serviço: 99,95%*

Os cenários de preços também podem incluir exemplos de clientes existentes com cargas de trabalho semelhantes que otimizaram as suas despesas no espaço de 1/2/3 anos, através da utilização de ferramentas de monitorização e otimização do CISP, adotando soluções nativas de cloud otimizadas e através de reduções de preços do CISP.

2.5 Termos e condições/Configuração da execução do contrato

As tecnologias de cloud e as operações que o CISP oferece são estandardizadas por predefinição, portanto as condições contratuais também são estandardizadas. Contudo, existe a possibilidade de ajustar ligeiramente estes contratos de forma a que se adaptem aos contextos legislativos e regulamentares locais.

Geralmente, os métodos de aquisição de TI tradicionais incluem regras estritas com as quais os candidatos devem estar em conformidade total ou parcial de forma a não serem rejeitados. Em alternativa, podem incluir um subconjunto estrito de requisitos obrigatórios. Quando este tipo de método de fornecimento é utilizado com tecnologias de cloud, que são, na verdade, um conjunto de ferramentas e componentes estandardizados que ajudam a arquitetar uma solução personalizada, as aquisições tendem a falhar.

2.5.1 Termos e condições

A primeira etapa na contratação de um RFP de serviços de cloud é rever e compreender os termos comerciais existentes do CISP que, em muitos casos, pode encontrar publicamente nos sites do CISP. As entidades do setor público estão cada vez mais confortáveis em aceitar os termos comerciais dos CISP. Parte deste esforço para compreender os termos passa por se reunir com os CISP e os seus parceiros para conhecer aprofundadamente as suas abordagens. A pergunta principal a ser feita é: "Por que é que os CISP operam com termos específicos?" Alguns destes termos podem parecer diferentes dos termos de TI tradicionais, mas existem motivos bem específicos para fazerem parte de um contrato de cloud. Se os termos publicamente disponíveis não forem aceitáveis, os CISP têm normalmente contratos ligeiramente modificáveis para clientes empresariais, que podem ser explorados.

Além de rever os termos e condições do CISP, é importante compreender as políticas, regulamentações e/ou leis existentes (por exemplo, as que envolvem tecnologia, classificação de dados, privacidade, pessoal, etc.). Às vezes, existem políticas/regulamentações/leis elaboradas para a compra e utilização de ofertas de TI tradicionais que podem ir contra o modelo do CISP. Por exemplo, permitir apenas a utilização de tecnologias de cloud que tenham sido incluídas na proposta original do acordo-quadro através do RFP de serviços de cloud. Os CISP estão constantemente a adicionar novos serviços e funcionalidades. Não faz sentido limitar o acesso a novos serviços aos clientes finais simplesmente porque segue uma abordagem de atualização de produtos de TI tradicionais. Se for o caso, é importante conversar abertamente com os CISP e analisar estas políticas/regulamentações e/ou leis.

Vantagens das discussões realizadas antes do RFP

Conforme mencionado acima, antes de elaborar um RFP, aproveite para se encontrar com os CISP e fornecedores relacionados para compreender os respetivos termos e condições e informá-los sobre a abordagem, políticas, regulamentações e leis da sua entidade. A parte mais importante destas discussões é que os dois lados saibam por que motivo os termos relevantes funcionam da forma que funcionam. Por exemplo, os termos e condições de serviços de cloud são diferentes para datacenters tradicionais, serviços geridos, hardware, software pronto a utilizar e termos de integração de sistemas. Como são modelos únicos e envolvem uma inovação constante, os respetivos modelos empresariais exigem que o processo de RFP seja suficientemente flexível para possibilitar negociações ou discussões de esclarecimento.

Ao incluir a capacidade de esclarecer termos e condições nas discussões e negociações, as organizações do setor público obtêm um melhor entendimento dos modelos de cloud e evitam o problema da rejeição de fornecedores que, na verdade, poderiam responder às necessidades da organização. Um processo normal é a identificação prévia por parte da organização de determinados termos que pretenda debater e negociar antes da adjudicação. Ao negociar termos aceitáveis com os concorrentes, a organização consegue a adjudicação 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, regulamentos e leis e ambas as partes podem compreender como a utilização da cloud se enquadra nesses modelos. Por vezes, há formas de trabalhar com as cláusulas existentes. No entanto, se existir uma área problemática, ambas as equipas podem trabalhar em conjuntos para encontrar uma solução (recomenda-se que estes temas sejam bem abordados antes de um RFP e da negociação contratual subsequente).

Flexibilidade na negociação

Para assinar contratos em conformidade com a legislação local, confiando nos termos contratuais estandardizados do CISP, é recomendado que: (1) seja solicitado aos candidatos o seu contrato padrão; (2) que não se peçam condições contratuais inadequadas ao criar o acordo-quadro para o RFP de serviços de cloud e (3) se forneça uma opção de negociação sobre todas as disposições da consulta e das propostas, que resultarão no acordo-quadro (exceto, obviamente, as cláusulas obrigatórias impostas pela lei).

Nota: o âmbito da responsabilidade partilhada é inerente ao modelo de cloud e deve refletir-se nos termos do contrato (por exemplo, o CISP confirma que os clientes são proprietários dos seus dados e onde os mesmos residem e fornece ferramentas para garantir que as localizações dos dados sejam limitadas, MAS é da responsabilidade do cliente ou do parceiro utilizar essas ferramentas.

Tenha em atenção que é importante que existam ***conjuntos distintos de termos e condições*** *do contrato para cada um dos LOTES de um acordo-quadro de cloud. Uma "abordagem única" para a contratação de todos os LOTES cria problemas de viabilidade e compatibilidade técnicas.*

Conforme já observado, os RFP 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 rejeitada. As organizações do setor público devem

considerar atentamente as consequências da utilização de termos obrigatórios, a menos que seja exigido por lei. As organizações devem conhecer a necessidade de um requisito ou termo obrigatório, pois podem comprometer futuras negociações com a sua classificação de obrigatoriedade. A utilização de requisitos ou termos obrigatórios deve ser minimizada para que a organização tenha a flexibilidade necessária para adquirir a melhor tecnologia e solução.

Tenha em atenção que as tecnologias de cloud do CISP são completamente estandardizadas e entregues de forma totalmente automatizada. Portanto, um CISP não consegue fazer alterações aos termos e condições que exijam qualquer personalização de serviço subjacente. Além disso, os preços dos serviços são geralmente públicos e estandardizados para todos os utilizadores, o que significa que um CISP não pode ajustar os preços na tentativa de assumir mais riscos em nome de um cliente em particular.

Compras indiretas

Uma opção alternativa à compra de tecnologias de cloud diretamente de um CISP é fazê-lo através de um revendedor do CISP. Pode encontrar mais informações sobre revendedores de CISP na secção *2.1.3* acima.

Exemplo de linguagem de RFP: termos e condições

Os CISP ou fornecedores representantes têm de fornecer os seus termos e condições disponíveis publicamente e dar feedback sobre os principais termos e condições fornecidos pela <ORGANIZAÇÃO>.

A <ORGANIZAÇÃO> pretende celebrar um contrato escrito com o concorrente vencedor com base nos termos contratuais do concorrente. O concorrente deve fornecer um conjunto de termos contratuais propostos para a <ORGANIZAÇÃO> analisar, o que representa a sua melhor proposta legal e comercial. Os autores da proposta 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*
  - *Gestão do acordo-quadro*
  - *Desempenho do acordo-quadro*
  - *Rescisão do acordo-quadro*
  - *Âmbito do acordo-quadro*
  - *Processo de encomenda*
  - *Disposições em matéria de confidencialidade*
  - *IP e informações específicas de categoria*
  - *Requisitos técnicos mínimos a serem cumpridos pelos CISP (por exemplo, padrões de qualidade, acreditação, segurança e proteção de dados)*
- *Existirão termos diferentes para cada um dos lotes do acordo-quadro.*
- *As especificidades do serviço do CISP serão consideradas e geridas durante o call-off.*
- *Permitir alterações contratuais: os termos não devem inibir os clientes e os fornecedores de concordarem com alterações contratuais, renunciando a novos serviços ou melhorias. A natureza evolutiva dos serviços de cloud é tal que as melhorias do serviço serão disponibilizadas continuamente, ajudando a proporcionar uma maior eficiência aos clientes.*

- *Os Acordos de Nível de Serviço (SLA) não devem ser especificados pelo cliente. Os termos do cliente não devem definir SLA específicos que difiram dos modelos de entrega de serviço padrão dos CISP. Ao permitir SLA padrão dos CISP, os CISP poderão manter os custos baixos e passá-los aos clientes, permitindo-lhes ter a certeza de que o CISP consegue corresponder ao SLA.*
- *Os limites de responsabilidade devem ser proporcionais. A responsabilidade deve ser proporcional aos serviços comprados, não devendo haver limites desproporcionalmente altos. Se os limites forem desproporcionalmente altos, será um desincentivo para os CISP aceitarem projetos de baixo valor. Geralmente, estes projetos são uma boa introdução e funcionam como "teste" para os clientes determinarem se certas soluções de cloud são eficientes para a sua organização.*
- *Os clientes devem ter proprietários dos seus dados. Os clientes devem controlar e ser proprietários dos seus dados e ter capacidade de determinar a localização geográfica em que os mesmos são mantidos. Isto permite que os clientes evitem a dependência de um fornecedor e transfiram os dados para novos fornecedores livremente.*

2.5.2 Termos e condições do software

Apesar de este manual se focar na compra de tecnologias de cloud de laaS e PaaS, como fornecidas pelo CISP, é importante destacar os termos e condições do software que as organizações do setor público podem considerar quando compram software aos fornecedores. Consulte a Figura1 (página 5) para rever como o software é comprado como parte de um RFP de serviço de cloud bem estruturado.

O software desempenha uma função crítica em quase todos os negócios, incluindo no setor público. Incluir obrigações como termos e condições de licenciamento de software num RFP de serviço de cloud ajuda a garantir que as entidades do setor público recebem o melhor valor e que têm liberdade para escolher os fornecedores ao adquirirem software.

Consulte os dez princípios de licenciamento justo de software para clientes que utilizam a cloud[9] para obter mais informação. Os princípios foram desenvolvidos pelo Cigref[10], uma associação das principais empresas e administrações públicas francesas que representam os utilizadores de tecnologia digital, em colaboração com o CISPE e o apoio de outras associações comerciais europeias de CIO e fornecedores, para abordar práticas que ambas as associações consideram prejudiciais à transformação digital de organizações de todos os tamanhos à medida que migram para a cloud.

Exemplo de linguagem de RFP: software

*A <**ORGANIZAÇÃO**> pretende celebrar um contrato escrito com o concorrente vencedor com base nos termos contratuais do concorrente. O concorrente deve fornecer um conjunto de termos contratuais propostos para a <**ORGANIZAÇÃO**> analisar, o que representa a sua melhor proposta legal e comercial. Quer os fornecedores de software quer a <ORGANIZAÇÃO> podem abordar os conjuntos de termos e condições durante a fase de <DISCUSSÃO/NEGOCIAÇÃO>.*

Requisito 1.0. *Os fornecedores de software têm de fornecer termos de licenciamento claros, incluindo uma descrição dos custos em níveis resumidos e detalhados.*

Requisito 1.1. *Todos os custos resultantes de qualquer falha no cumprimento dos termos da licença têm de ser fornecidos em níveis resumidos e detalhados.*

[9] https://www.fairsoftware.cloud/principles/
[10] https://www.cigref.fr/

Requisito 2.0. *As licenças de software têm de fornecer à <Organização> a capacidade de migrar o software licenciado on-premises para a cloud à sua escolha, sem que exista a obrigatoriedade de compra de licenças separadas e duplicadas para o mesmo software.*

Requisito 2.1. *As licenças de software têm de ser livres de restrições de licenciamento e custos acrescidos que limitem a capacidade da <Organização> de utilizar software licenciado numa cloud à sua escolha.*

Requisito 3.0. *As licenças de software têm de permitir que a <Organização> utilize o software licenciado no seu próprio hardware (normalmente denominado por software "on-premises"), bem como na cloud à sua escolha.*

Requisito 4.0. *As licenças de software não podem exigir que o software licenciado seja utilizado apenas em hardware dedicado exclusivamente à <Organização>.*

Requisito 5.0. *Os fornecedores de software não podem penalizar a <Organização> caso o software licenciado do fornecedor seja utilizado na oferta de cloud de outro fornecedor, por exemplo, ao incluir direitos para realizar auditorias de software adicionais ou intrusivas ou impor taxas de licenciamento de software mais altas.*

Requisito 6.0. *O software de diretório tem de suportar padrões transparentes para sincronizar e autenticar a identidade do utilizador de forma não discriminatória com outros serviços de identidade.*

Requisito 7.0. *Os fornecedores de software não podem cobrar diferentes preços pelo mesmo software baseado apenas em quem possui o hardware no qual está instalado.*

Requisito 7.1. *Os preços do software não podem discriminar entre software instalado no próprio datacenter da <Organização>, no datacenter gerido por terceiros, em computadores alugados de terceiros ou num fornecedor de cloud escolhido pela <Organização>.*

Requisito 8.0. *Durante o período de vigência do contrato, os fornecedores de software não podem efetuar alterações substanciais aos prazos de licença que restrinjam a <Organização> de utilizações anteriormente permitidas, a não ser que seja exigido por lei ou devido a preocupações de segurança.*

Requisito 9.0. *Os fornecedores de software não podem induzir em erro a <Organização> ao indicar que as licenças de software irão cobrir a utilização pretendida do software da <Organização>, conforme definido nos <Requisitos da organização>, quando a cobertura dessa utilização possa exigir a compra de licenças adicionais.*

Requisito 10.0. *Se a <Organização> tiver o direito de revender e transferir licenças de software, os fornecedores de software têm de continuar a oferecer suporte e atualizações sob condições justas à <Organização>, que obteve uma licença através de uma revenda legal.*

2.5.3 Como fazer a seleção entre adjudicatários por projeto

Os órgãos do setor público que fazem parte do acordo-quadro podem realizar um pedido ou um "call-off" de serviços necessários quando precisem. Efetuar um contrato de call-off sob um acordo-quadro permite aos compradores refinar requisitos com especificações funcionais adicionais para um call-off, mantendo os benefícios oferecidos no acordo-quadro.

Se for necessário, pode ser efetuado um miniconcurso para identificar o melhor fornecedor para um projeto ou carga de trabalho específica. Com um miniconcurso, o cliente realiza um novo concurso ao abrigo do acordo-quadro, convidando todos os fornecedores num lote a responder a um conjunto de requisitos. O cliente convida todos os fornecedores aptos num mesmo lote

a apresentar propostas, daí a importância dos requisitos mínimos para adjudicatários num RFP de serviços de cloud, já que isso garante um nível elevado de opções em cada lote.

Mais uma vez, tenha em atenção que é importante haver conjuntos distintos de termos e condições do contrato para cada uma das categorias de lote com base no tipo de oferta (por exemplo, IaaS/PaaS pública, IaaS/PaaS comunitária, IaaS/PaaS privada), pois uma "abordagem única" na contratação de cada lote causará problemas de viabilidade e compatibilidade técnicas.

Consulte a secção *2.1.4* para ver exemplos de linguagem de RFP relativamente à seleção de adjudicatários.

2.5.4 Integração e saída

Uma consideração a ter durante a criação do acordo-quadro de cloud é a opção de um sistema de compra dinâmico (Dynamic Purchasing System – DPS). Com um modelo de DPS, todos os fornecedores que cumpram os requisitos mínimos do acordo-quadro são admitidos no acordo-quadro. Não há limites para o número de fornecedores que podem participar no acordo-quadro e, ao contrário do modelo de acordo-quadro tradicional, os fornecedores também se podem candidatar para participar no "acordo-quadro de 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 CISP sem garantir uma concorrência leal. O objetivo é evitar saturar o utilizador final com demasiadas opções, mantendo um padrão elevado de tecnologias de cloud disponíveis.

3.0 Melhores práticas/lições aprendidas

Abaixo, destacamos algumas lições aprendidas sobre como elaborar um bom acordo-quadro de cloud com um RFP de serviços de cloud bem redigido.

3.1 Governança de cloud

A governança na cloud é uma responsabilidade partilhada. Os CISP oferecem funcionalidades e serviços para integrar a governança de cloud em todos os aspetos de um ambiente de cloud, enquanto os clientes trazem os seus padrões existentes de governança e descobrem de que forma a cloud promove tal governança.

Na cloud, os clientes têm a oportunidade de criar o ambiente de TI que pretendem, além de poderem gerir o que já possuem. A cloud permite aos clientes: (1) começar com um inventário completo de todos os ativos de TI; (2) gerir todos estes ativos de forma centralizada e (3) criar alertas relativamente à utilização/faturação/segurança/etc. Todos estes benefícios vitais da cloud ajudam os clientes a ter uma arquitetura otimizada (e, tanto quanto possível, automatizada) sem terem de adquirir e instalar novo hardware continuamente. Isto é feito pelo CISP, permitindo que os clientes mudem o foco da gestão de infraestrutura indiferenciada para o nível de operações essenciais à missão.

Uma forma útil de ver a cloud do CISP é considerá-la uma API de grandes dimensões. Quer esteja a iniciar um novo servidor ou a alterar uma definição de segurança, está apenas a fazer chamadas de API. Cada alteração ao ambiente é registada e gravada (quem, porquê, onde e quando foi

efetuada cada alteração). Isto fornece governança, controlo e visibilidade da cloud, que só são possíveis num ambiente de cloud. Permite que os clientes repensem os seus modelos existentes de governança de TI e determinem como podem ser simplificados e melhorados, face aos benefícios que a cloud oferece.

A governança na cloud também pode significar comunicar e incorporar alterações processuais positivas e novos conjuntos de competências que vêm com a cloud. Por exemplo, os gestores de projeto já estão habituados a meses de espera para implementar um ambiente de TI, por isso, podem calcular em excesso os seus calendários para criar um ambiente de desenvolvimento ou teste na cloud (algo que, com a cloud, demora 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 acordo-quadro de cloud possa continuar a evoluir de maneira a que os requisitos sejam adequados para novos processos e uma maior agilidade.

3.2 Orçamentação de cloud

Quando é necessário estruturar o preço de pagamento conforme a utilização da cloud de forma a se adequar aos requisitos de aquisição e orçamentação do setor público, descobrimos que é útil agrupar serviços do CISP num único item de linha (computação, armazenamento, redes, base de dados, IoT, etc.) de **tecnologias de cloud.** Esta abordagem concede flexibilidade para oferecer todas as novas e atuais tecnologias do CISP aos utilizadores em tempo real, oferecendo acesso rápido aos recursos necessários, quando necessário. Também acomoda a procura variável, resultando numa utilização otimizada e em custos baixos.

As organizações do setor público podem adicionar outros itens de linha para pedidos de outros lotes num acordo-quadro de cloud, caso queiram serviços de consultoria/profissionais ou geridos, software de um marketplace, serviços de suporte de cloud e formação para as ofertas do CISP.

Pode ser oferecida mais flexibilidade contratual através da utilização de itens de linha contratuais opcionais dentro de categorias de recursos adequadas para acomodar o crescimento futuro. Como alternativa, se uma organização quiser incluir tecnologias de cloud com serviços de consultoria/profissionais/geridos num item de linha, isso é possível com um item de linha, como "tecnologias de cloud e trabalhos complementares".

Abaixo encontra-se 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" utilizadas. Todos os meses, os incrementos ao pedido podem ter como base projeções de utilização atuais e previstas.

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

N.º DO ITEM	PRODUTOS/SERVIÇOS	QUANTIDADE	UNIDADE	PREÇO UNITÁRIO	VALOR
1001	Tecnologias de cloud	1000	Cada	1 €	1000 €
1002	Serviços de consultoria	1	Por semana	3000 €	3000 €
1003	Suporte de cloud	1	Por mês	1000 €	1000 €
1004	Formação de cloud	1	Por dia	3,00 €	3000 €
1005	Marketplace de cloud	10	Cada	10 €	100 €

Segue-se um exemplo de como esta estrutura pode funcionar: uma organização do setor público conversa com um CISP para estimar a utilização dos serviços de tecnologia de cloud. A organização concorda com os termos do fornecedor, como os 10 milhões de euros durante 5 anos, o que totaliza 2 milhões de euros por ano. A organização compromete-se com o valor anual inicial de 2 milhões de euros. Todos os meses é emitida uma fatura e o dinheiro é retirado do fundo para pagar a mesma. É realizado um levantamento nessa conta. O fundo restante é monitorizado para fins de controlo de custos com ferramentas de monitorização e previsão do CISP. Se o fundo restante for baixo, a organização solicita mais fundos ao diretor financeiro para que os serviços sejam mantidos.

Exemplo de linguagem de RFP: preços – contratação

PRAZOS DE PAGAMENTO

Os prazos de pagamento devem ser estruturados de forma a pagar somente pelos recursos utilizados pela <ORGANIZAÇÃO>, conforme indicado abaixo:

1. *Pagamento mensal, com base na utilização/consumo real de serviços e conforme os preços dos CISP disponibilizados publicamente.*

GARANTIA MÍNIMA E DESPESA MÁXIMA

Como será impossível para a <ORGANIZAÇÃO> determinar exatamente o volume de recursos de um fornecedor de serviços de cloud específico que será consumido durante um certo período, os pedidos serão especificados como quantidades por unidade de preço fixo de um item de linha de pedido único para "tecnologias de cloud".

Cada unidade de item de linha pedida será igual a <1 €> do valor das tecnologias de cloud pedidas. Serão efetuados pedidos incrementais periodicamente através da modificação deste pedido em diversas quantidades, para que a <ORGANIZAÇÃO> tenha a flexibilidade de pedir previamente diversas quantidades em "euros" de tecnologias de cloud do CISP com base na sua utilização estimada para necessidades de duração variada. As quantidades serão pedidas previamente pela <ORGANIZAÇÃO> de forma periódica em valores suficientes para cobrir o custo estimado das tecnologias de cloud que serão utilizadas para cumprir os diversos requisitos.

N.º do item	Descrição	Quantidade	Unidade	Preço
01	Tecnologias de cloud do CISP	1000	Cada unidade	1000 €

PEDIDO MÍNIMO/PEDIDO INCREMENTAL

Os pedidos serão feitos periodicamente para diversas quantidades de <10 000> unidades de item de linha com base na utilização estimada que a <ORGANIZAÇÃO> faz das tecnologias de cloud. Esta 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" de computação na cloud.

Um incremento inicial de <100 000> unidades pelo custo de <100 000 €> será pedido assim que o call-off for realizado. O número mínimo de unidades de item de linha que pode ser feito num pedido incremental único que utiliza 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 call-off quando combinado com todas as unidades anteriores pedidas. A <ORGANIZAÇÃO> será responsável por garantir que todos os pedidos estejam dentro dos limites especificados nesta secção.

PEDIDO MÁXIMO
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>*** *relativamente ao período de desempenho, mas não é garantido.*

3.3 Compreender o modelo empresarial dos parceiros

As entidades do setor público devem compreender os modelos com os quais os CISP fornecem as suas ofertas e reconhecer que os parceiros que fornecem consultoria, serviços geridos, revenda e muito mais são essenciais para o processo. Muitos clientes precisam de um fornecedor de cloud para a sua infraestrutura e subcontratam o trabalho "prático" de planeamento, migração e gestão para um integrador de sistemas (SI) ou um fornecedor de serviços geridos. Dada esta combinação de "serviços", podem existir requisitos que não são aplicáveis a fornecedores de cloud, como cláusulas transferidas para subcontratados.

Iremos utilizar estas cláusulas transferidas como um exemplo para ilustrar por que é importante compreender como os parceiros e revendedores operam em relação aos CISP. Em alguns tipos de aquisição há cláusulas que exigem que o contratante principal transmita certas cláusulas obrigatórias a todos os seus parceiros/subcontratantes. Normalmente, os CISP não fornecerão nem apresentarão propostas como parceiros de subcontratação formais, pois oferecem um serviço estandardizado em grande escala que não está adaptado para cumprir os requisitos exclusivos de um determinado cliente final (incluindo as necessidades de um cliente do setor público segundo um contrato com o setor público). Num modelo de aquisição indireta (aquisição de serviços de cloud através de um revendedor de CISP), um CISP pode rejeitar estas cláusulas do seu revendedor, por não serem aplicáveis a um fornecedor de serviços comerciais de "2.º nível". Nesse caso, o CISP não está a executar o âmbito de trabalho ao abrigo do contrato, pois o parceiro do CISP está a utilizar a infraestrutura do CISP para tal finalidade. Portanto, o CISP é um fornecedor comercial (não um subcontratado) para as operações de um parceiro. Num modelo de aquisição direta (compra de serviços de cloud diretamente de um CISP), o CISP normalmente rejeitaria estas cláusulas "obrigatórias" adequadas para um subcontratado típico de bens devido à natureza comercial dos serviços contratados e o facto de a maioria dos CISP não exigir que os subcontratados forneçam os seus serviços comerciais.

3.4 Agentes de cloud

O conceito de um agente de cloud para reduzir a possibilidade de depender de um fornecedor pode ser problemático. Embora um agente de cloud possa ser uma boa ideia na teoria, na prática, provavelmente poderá criar mais complexidade e confusão do que o valor esperado.

Tentar criar aplicações que funcionem em várias clouds de forma simultânea ou alternada resulta inevitavelmente em concessões de capacidade (não existe uma pedra de Roseta para a cloud). Esta abordagem acaba por acrescentar uma camada desnecessária de complexidade entre clientes do setor público e os seus serviços de cloud, o que pode comprometer as eficiências e os ganhos de segurança que procuram obter, levando à redução da escalabilidade e agilidade, ao aumento nos custos e à desaceleração da inovação.

3.5 Aprovisionamento e estudo de mercado antes do RFP

À medida que uma entidade do setor público planeia criar um RFP de serviços de cloud, deve incluir intervenientes de todos os aspetos da organização, como liderança, intervenientes de negócios, tecnologia, finanças, aquisição, jurídico e contratos, desde o início do processo. Esta abordagem garante que todos os intervenientes conhecem o modelo de cloud e que, consequentemente, abordam de forma informada a reavaliação dos métodos de aquisição de TI tradicionais.

Quando o assunto é dialogar com o setor, recomendamos que as entidades do setor público tenham conversas detalhadas para recolher feedback sobre o CISP, parceiros de CISP, fornecedores de marketplaces de PaaS/SaaS e especialistas do setor. Por exemplo, esse diálogo pode acontecer durante workshops sobre segurança e aquisição. Outra forma eficiente de obter conhecimentos aprofundados sobre aquisição de cloud é com a publicação de um RFI ou, idealmente, de um documento de rascunho de RFP. Normalmente, incluem possíveis problemas que podem ser identificados, abordados e ajustados antes de o RFP de serviços de cloud final ser publicado.

3.6 Sustentabilidade

A sustentabilidade é inerente à computação na cloud e a mudança para serviços de cloud providencia ganhos de eficiência energética, quando comparados com servidores on-premises ou datacenters empresariais. Identificar um CISP que dá prioridade à sustentabilidade e que se comprometeu publicamente em alcançar objetivos de sustentabilidade oferece uma garantia adicional de que a cloud é sustentável. Os CISP e operadores de datacenters europeus (com o apoio da Comissão Europeia) criaram o Climate Neutral Data Centre Pact[11], uma iniciativa autorreguladora que estabelece critérios de sustentabilidade claros, simples e abrangentes para o setor dos datacenters e garante que os operadores de datacenters e fornecedores de serviços de cloud alcançam a neutralidade climática até 2030. A iniciativa autorreguladora inclui objetivos para eficiência energética, conservação de água, reutilização e reparação de servidores e utilização de energia isenta de carbono para alimentar os datacenters. Os CISP que se inscrevam na iniciativa autorreguladora concordam em alcançar estes objetivos e seguir os critérios para serem considerados operadores com impacto neutro no clima.

Um RFP de serviços de cloud deve perguntar aos CISP se os mesmos se comprometeram com tais critérios, especificamente se estes se inscreveram na autorregulação e quando assumiram tal responsabilidade.

Exemplo de linguagem de RFP: sustentabilidade

Comprometeu-se a operar datacenters climaticamente neutros ao assinar a iniciativa autorreguladora de neutralidade climática em datacenters? Se sim, quando se tornou signatário?

Pode comprovar que recebeu o selo do Climate Neutral Data Centre Pact?

[11] https://www.climateneutraldatacentre.net/self-regulatory-initiative/

Apêndice A – Requisitos técnicos de comparação entre os concorrentes

Abaixo encontra-se uma lista de requisitos genéricos de tecnologia de cloud que podem ser utilizados para a comparação de CISP durante call-offs ou miniconcursos num acordo-quadro de cloud.

1. Perfil do fornecedor de cloud

	Requisito
1.	*EXPERIÊNCIA DE MARKETPLACE:* *Há quantos anos é que o fornecedor de cloud opera no segmento do marketplace de cloud?*
2.	*ABERTURA E PROTEÇÃO DE DADOS:* *O fornecedor de cloud adere a códigos de conduta do setor relativos a proteção ou reversibilidade de dados?* *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 datacenters são agrupados numa rede de baixa latência para oferecer um nível superior de alta disponibilidade e tolerância a falhas?* • *Em caso afirmativo, indique o número de domínios e zonas e o número de datacenters dentro da área geográfica necessária.*
4.	*DISTÂNCIA DOS DOMÍNIOS/ZONAS:* *O fornecedor de cloud cria os respetivos domínios ou zonas com datacenters separados fisicamente para oferecer suporte à redundância, alta disponibilidade e baixa latência?*
5.	*DATACENTERS CONSTRUÍDOS:* *O fornecedor de cloud oferece datacenters concebidos para estarem isolados de falhas noutros datacenters, com alimentação, arrefecimento e redes redundantes?*
6.	*REPLICAÇÃO DE DATACENTERS:* *O fornecedor de cloud oferece replicação de dados entre os datacenters num domínio ou zona com failover automático?*
7.	*REPLICAÇÃO DOS DOMÍNIOS/ZONAS:* *O fornecedor de cloud oferece replicação de dados entre domínios ou zonas numa região?*

3. Infraestrutura

3.1 Computação

	Requisito
1.	*COMPUTAÇÃO – INSTÂNCIA REGULAR – UTILIZAÇÃO GERAL:* *O fornecedor de cloud oferece os seguintes tipos de instância?* • *Utilização geral: otimizada para aplicações genéricas e fornece um equilíbrio de recursos de rede, computação e memória.* o *Em caso afirmativo, qual é a maior instância?*
2.	*COMPUTAÇÃO – INSTÂNCIA REGULAR – OTIMIZADA PARA MEMÓRIA:* *O fornecedor de cloud oferece os seguintes tipos de instância?* • *Otimizada para memória: otimizada para aplicações com utilização intensiva de memória.* o *Em caso afirmativo, qual é a maior instância?*
3.	*COMPUTAÇÃO – INSTÂNCIA REGULAR – OTIMIZADA PARA COMPUTAÇÃO:* *O fornecedor de cloud oferece os seguintes tipos de instância?* • *Otimizada para computação: otimizada para aplicações com utilização intensiva de computação.* o *Em caso afirmativo, qual é a maior instância?*
4.	*COMPUTAÇÃO – INSTÂNCIA REGULAR – OTIMIZADA PARA ARMAZENAMENTO:* *O fornecedor de cloud oferece os seguintes tipos de instância?* • *Otimizada 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 (HDD/SSD) que podem ser aprovisionados e anexados a uma instância?*
5.	*COMPUTAÇÃO – INSTÂNCIA REGULAR – OTIMIZADA PARA GRÁFICOS:* *O fornecedor de cloud oferece os seguintes tipos de instância?* • *Gráficos de baixo custo: oferece aceleração de gráficos de baixo custo para instâncias de computação?* o *Em caso afirmativo, qual é a maior instância?*
6.	*COMPUTAÇÃO – INSTÂNCIA REGULAR – OTIMIZADA PARA GPU:* *O fornecedor de cloud oferece os seguintes tipos de instância?* • *GPU: oferece unidades de processamento gráfico (GPU) de hardware para aplicações com utilização intensiva de gráficos.* o *Em caso afirmativo, quantas GPU e que modelos de GPU pode o fornecedor de cloud oferecer por instância?*
7.	*COMPUTAÇÃO – INSTÂNCIA REGULAR – OTIMIZADA PARA FPGA:* *O fornecedor de cloud oferece os seguintes tipos de instância?* • *FPGA: oferece matrizes de portas programáveis em campo (FPGA) para o desenvolvimento e a implementação da aceleração de hardware personalizado para aplicações.* o *Em caso afirmativo, quantas FPGA pode o fornecedor de cloud 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 referência?* • *Em caso afirmativo, qual é a maior instância com capacidade de intermitência?*
9.	*COMPUTAÇÃO – INSTÂNCIA COM E/S INTENSIVA:* *O fornecedor de cloud oferece instâncias que utilizam unidades de estado sólido (SSD) de memória expressa não volátil (NVMe) otimizadas para baixa latência, desempenho de E/S aleatório muito alto e alta taxa de transferência de leitura sequencial?* • *Em caso afirmativo, 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 suporta o armazenamento local para instâncias de computação a serem utilizadas para armazenamento temporário de informações que mudam com frequência?*
11.	*COMPUTAÇÃO – SUPORTE PARA VÁRIOS NIC:* *O fornecedor de cloud suporta várias placas de interface de rede (NIC) (primárias e adicionais) a serem alocadas para uma determinada instância?* • *Em caso afirmativo, qual é o número máximo de NIC por instância?*
12.	*COMPUTAÇÃO – AFINIDADE DE INSTÂNCIA:* *O fornecedor de cloud oferece aos utilizadores a capacidade de agrupar instâncias de forma lógica no mesmo datacenter?*
13.	*COMPUTAÇÃO – ANTIAFINIDADE DE INSTÂNCIA:* *O fornecedor de cloud oferece aos utilizadores a capacidade de agrupar instâncias de forma lógica e colocá-las em diferentes datacenters de uma região?*
14.	*COMPUTAÇÃO – APROVISIONAMENTO SELF-SERVICE:* *O fornecedor de cloud oferece aprovisionamento self-service de várias instâncias em simultâneo através de uma interface programática, uma consola de gestão ou um portal Web?*
15.	*COMPUTAÇÃO – PERSONALIZAÇÃO:* *O fornecedor de cloud oferece instâncias personalizáveis, ou seja, a capacidade de modificar definições como unidades de processamento central virtual (vCPU) e memória de acesso aleatório (RAM)?*
16.	*COMPUTAÇÃO – LOCAÇÃO:* *O fornecedor de cloud oferece instâncias de inquilino único que são executadas em hardware dedicado a um único utilizador?* • *Em caso afirmativo, qual é a maior instância de inquilino único disponível?*
17.	*COMPUTAÇÃO – AFINIDADE DE ANFITRIÃO:* *O fornecedor de cloud oferece a capacidade de iniciar uma instância e especificar que essa instância é reiniciada sempre no mesmo anfitrião físico?*
18.	*COMPUTAÇÃO – ANTIAFINIDADE DE ANFITRIÃO:* *O fornecedor de cloud oferece a capacidade de dividir e alojar instâncias específicas em diferentes anfitriões físicos?*

19.	*COMPUTAÇÃO – ESCALABILIDADE AUTOMÁTICA* *O fornecedor de cloud oferece a capacidade de aumentar automaticamente o número de instâncias durante os picos de procura para manter o desempenho (ou seja, aumentar a escala horizontalmente)?*
20.	*COMPUTAÇÃO – MECANISMO DE IMPORTAÇÃO DE IMAGEM:* *O fornecedor de cloud oferece aos utilizadores a capacidade de importar as suas imagens existentes e de guardá-las como novas imagens disponíveis de forma privada que podem ser utilizadas para aprovisionar instâncias no futuro?* • *Em caso afirmativo, quais são os formatos suportados?*
21.	*COMPUTAÇÃO – MECANISMO DE EXPORTAÇÃO DE IMAGEM:* *O fornecedor de cloud oferece a capacidade de exportar uma instância em execução existente ou uma cópia de uma instância para um formato de máquina virtual?* • *Em caso afirmativo, quais são os formatos suportados?*
22.	*COMPUTAÇÃO – INTERRUPÇÃO DE SERVIÇO:* *O fornecedor de cloud oferece mecanismos para evitar interrupções ou períodos de inatividade de instâncias quando o fornecedor executa manutenções de hardware ou serviço ao nível do anfitrião?*
23.	*COMPUTAÇÃO – REINÍCIO DA INSTÂNCIA:* *O fornecedor de cloud oferece mecanismos para reiniciar automaticamente instâncias num anfitrião em bom estado de funcionamento, caso o anfitrião físico original falhe?*
24.	*COMPUTAÇÃO – NOTIFICAÇÕES:* *No caso de um evento resiliente de computação, o fornecedor de cloud consegue notificar o utilizador da existência de tal evento? E o utilizador pode optar por receber ou não receber esta notificação por si mesmo?*
25.	*COMPUTAÇÃO – PROGRAMAÇÃO DE EVENTOS:* *O fornecedor de cloud oferece a capacidade de agendar eventos para as instâncias do utilizador, como reiniciar, interromper, iniciar ou retirar a instância?*
26.	*COMPUTAÇÃO – MECANISMO DE BACKUP E RESTAURO:* *O fornecedor de cloud oferece um mecanismo integrado de backup e recuperação?*
27.	*COMPUTAÇÃO – MECANISMO DE SNAPSHOT:* *O fornecedor de cloud oferece um mecanismo de snapshot manual a pedido?*
28.	*COMPUTAÇÃO – METADADOS:* *O fornecedor de cloud oferece um serviço de metadados de instância que permite aos utilizadores definir pares de valores-chave arbitrários para a instância?*
29.	*COMPUTAÇÃO – CHAMADA DE METADADOS:* *O fornecedor de cloud oferece um serviço de metadados de instância que fornece uma interface de programação de aplicações (API) que a instância possa chamar para obter informações sobre si mesma?*
30.	*COMPUTAÇÃO – MECANISMO DE LICITAÇÃO:* *O fornecedor de cloud oferece um mecanismo de licitação para licitar instâncias de custo mais baixo que podem ser imediatamente instanciadas para alojar cargas de trabalho não críticas?*
31.	*COMPUTAÇÃO – MECANISMO DE PROGRAMAÇÃO:* *O fornecedor de cloud oferece alguma forma de agendar e reservar capacidade computacional adicional de forma recorrente, ou seja, um agendamento diário, semanal ou mensal?*

32.	*COMPUTAÇÃO – MECANISMO DE RESERVA:* *O fornecedor de cloud oferece alguma forma de reservar capacidade computacional adicional para o futuro (ou seja, 1 ano, 2 anos, 3 anos, etc.)?*
33.	*COMPUTAÇÃO – SISTEMA OPERATIVO LINUX:* *O fornecedor de cloud suporta as duas últimas versões suportadas a longo prazo de, pelo menos, uma distribuição Linux empresarial (como Red Hat, SUSE) e uma distribuição Linux gratuita utilizada regularmente (como Ubuntu, CentOS e Debian)?*
34.	*COMPUTAÇÃO – SISTEMA OPERATIVO WINDOWS:* *O fornecedor de cloud suporta as duas principais versões do Windows Server (Windows Server 2017 e Windows Server 2016)?*
35.	*COMPUTAÇÃO – PORTABILIDADE DE LICENÇAS:* *O fornecedor de cloud oferece portabilidade e suporte para licenças?* • *Em caso afirmativo, indique o fornecedor, nomes, edições e versões de software.*
36.	*COMPUTAÇÃO – LIMITES DE SERVIÇO:* *O fornecedor de cloud possui alguma restrição (ou seja, limites de serviço) relativamente à secção de computação acima?* *Exemplo:* *Número máximo de instâncias por conta* *Número máximo de anfitriões dedicados por conta* *Número máximo de endereços IP reservados*

3.2 Redes

	Requisito
1.	*REDES – REDES VIRTUAIS:* *O fornecedor de cloud suporta a capacidade de criar uma rede virtual lógica e isolada que representa a própria rede de uma empresa na cloud?*
2.	*REDES – CONECTIVIDADE NA MESMA REGIÃO:* *O fornecedor de cloud suporta a ligação de duas redes virtuais na mesma região para encaminhar o tráfego entre as mesmas com endereços IP privados?*
3.	*REDES – CONECTIVIDADE EM REGIÕES DIFERENTES:* *O fornecedor de cloud suporta a ligação de duas redes virtuais em regiões diferentes para encaminhar o tráfego entre as mesmas com endereços IP privados?*
4.	*REDES – SUB-REDE PRIVADA:* *O fornecedor de cloud oferece a capacidade de criar redes e sub-redes virtuais totalmente isoladas (privadas) nas quais as instâncias podem ser aprovisionadas sem qualquer endereço IP público ou encaminhamento de Internet?*
5.	*REDES – INTERVALO DE ENDEREÇOS DE REDE VIRTUAL:* *O fornecedor de cloud suporta intervalos de endereços IP especificados no pedido de comentários (RFC) 1918, bem como blocos de encaminhamento CIDR (Classless Inter-Domain Routing) publicamente encaminháveis?*

6.	*REDES – VÁRIOS PROTOCOLOS:* *O fornecedor de cloud suporta vários protocolos, incluindo o protocolo de controlo de transmissão (TCP), protocolo de datagrama do utilizador (UDP) e protocolo de mensagem de controlo da Internet (ICMP)?*
7.	*REDES – ATRIBUIÇÃO AUTOMÁTICA PARA ENDEREÇOS IP:* *O fornecedor de cloud suporta a capacidade de atribuir automaticamente endereços IP públicos a instâncias?*
8.	*REDES – ENDEREÇOS IP ESTÁTICOS RESERVADOS:* *O fornecedor de cloud suporta endereços IP associados a uma conta de utilizador e não a uma instância específica? O endereço IP deve permanecer associado à conta até ser explicitamente libertado.*
9.	*REDES – SUPORTE AO IPV6:* *O fornecedor de cloud suporta a versão 6 do protocolo de Internet (IPv6) ao nível de gateway ou da instância e expõe essa funcionalidade aos utilizadores?*
10.	*REDES – VÁRIOS ENDEREÇOS DE IP POR NIC:* *O fornecedor de cloud suporta a atribuição de um endereço IP primário e secundário a uma placa de interface de rede (NIC) ligada a uma determinada instância?*
11.	*REDES – VÁRIOS NICS:* *O fornecedor de cloud suporta a atribuição de várias placas de interface de rede (NIC) a uma determinada instância?*
12.	*REDES – MOBILIDADE DE NIC E IP:* *O fornecedor de cloud suporta que as placas de interface de rede (NIC) e os endereços do protocolo de Internet (IP) sejam movidos entre instâncias?*
13.	*REDES – SUPORTE AO SR-IOV:* *O fornecedor de cloud suporta capacidades como a virtualização de entrada/saída de raiz única (SR-IOV) para obter um maior desempenho (ou seja, pacotes por segundo – PPS), menor latência e menor instabilidade?*
14.	*REDES – FILTRAGEM DE ENTRADA:* *O fornecedor de cloud suporta a adição ou remoção de regras aplicáveis ao tráfego de entrada para instâncias?*
15.	*REDES – FILTRAGEM DE SAÍDA:* *O fornecedor de cloud suporta a adição ou remoção de regras aplicáveis ao tráfego de saída proveniente de instâncias?*
16.	*REDES – ACL:* *O fornecedor de cloud suporta listas de controlo de acesso (ACL) para controlar o tráfego de entrada e de saída para sub-redes?*
17.	*REDES – SUPORTE AO REGISTO DE FLUXOS:* *O fornecedor de cloud suporta a captura de registos de fluxos de tráfego da rede?*
18.	*REDES – NAT:* *O fornecedor de cloud fornece um serviço gerido de gateway de tradução de endereços de rede (NAT) para permitir que as instâncias numa rede privada se liguem à Internet ou a outros serviços de cloud, mas impede que a Internet inicie uma ligação a essas instâncias?*
19.	*REDES – VERIFICAÇÃO DE ORIGEM/DESTINO:* *O fornecedor de cloud suporta a desativação da verificação de origem/destino em placas de interface de rede (NIC)?*
20.	*REDES – SUPORTE DE VPN:* *O fornecedor de cloud suporta uma ligação de rede privada virtual (VPN) entre o fornecedor de cloud e o datacenter do utilizador?*

21.	*REDES – TÚNEIS DE VPN:* *O fornecedor de cloud suporta várias ligações de rede privada virtual (VPN) por rede virtual?*
22.	*REDES – SUPORTE À VPN DE IPSEC:* *O fornecedor de cloud permite que os utilizadores acedam aos serviços de cloud através de um túnel de rede privada virtual (VPN) de segurança do protocolo de Internet (IPsec) ou de um túnel de rede privada virtual (VPN) de Secure Sockets Layer (SSL) na Internet pública?*
23.	*REDES – SUPORTE DE BGP:* *O fornecedor de cloud aplica o Border Gateway Protocol (BGP) para melhorar o failover em túneis de rede privada virtual (VPN) de segurança do protocolo de Internet (IPsec)?*
24.	*REDES – CONECTIVIDADE DEDICADA PRIVADA:* *O fornecedor de cloud oferece um serviço de ligação direta e privada entre as localizações do fornecedor de cloud e o ambiente de colocalização, escritório ou datacenter do utilizador que permite transferências de dados grandes e rápidas?*
25.	*REDES – BALANCEADOR DE CARGA DE FRONT-END:* *O fornecedor de cloud oferece um serviço de balanceamento de carga de front-end (acessível pela Internet) que recebe pedidos de clientes pela Internet e distribui esses pedidos entre instâncias registadas com o balanceador de carga?*
26.	*REDES – BALANCEADOR DE CARGA DE BACK-END:* *O fornecedor de cloud oferece um serviço de balanceamento de carga de back-end (privado) que encaminha o tráfego para instâncias alojadas em sub-redes privadas?*
27.	*REDES – BALANCEADOR DE CARGA DA CAMADA 7:* *O fornecedor de cloud oferece um serviço de balanceamento de carga da camada 7 (protocolo de transferência de hipertexto – HTTP) capaz de balancear a carga de tráfego de rede em várias instâncias?*
28.	*REDES – BALANCEADOR DE CARGA DA CAMADA 4:* *O fornecedor de cloud oferece um serviço de balanceamento da camada 4 (protocolo de controlo de transmissão – TCP) capaz de balancear a carga de tráfego de rede em várias instâncias?*
29.	*REDES – AFINIDADE DA SESSÃO PARA BALANCEADORES DE CARGA:* *O fornecedor de cloud oferece um serviço de balanceamento de carga que permite a afinidade da sessão?*
30.	*REDES – BALANCEAMENTO DE CARGA BASEADO EM DNS:* *O fornecedor de cloud oferece um serviço de balanceamento de carga capaz de balancear a carga de tráfego para instâncias alojadas em vários anfitriões pertencentes a um único domínio?*
31.	*REDES – REGISTOS DO BALANCEADOR DE CARGA:* *O fornecedor de cloud fornece registos que capturam informações detalhadas sobre todos os pedidos enviados a um balanceador de carga?*
32.	*REDES – DNS:* *O fornecedor de cloud oferece um serviço de sistema de nomes de domínio (DNS) altamente disponível e escalável?*
33.	*REDES – ENCAMINHAMENTO DE DNS BASEADO EM LATÊNCIA:* *O fornecedor de cloud oferece um serviço de sistema de nomes de domínio (DNS) compatível com o encaminhamento baseado em latência (ou seja, o serviço DNS responde a consultas DNS com os recursos que fornecem a melhor latência)?*

34.	*REDES – ENCAMINHAMENTO DE DNS BASEADO EM GEOGRAFIA:* *O fornecedor de cloud oferece um serviço de sistema de nomes de domínio (DNS) compatível com o encaminhamento baseado em geografia (ou seja, o serviço DNS responde a consultas DNS com base na localização geográfica dos utilizadores)?*
35.	*REDES – ENCAMINHAMENTO DE DNS BASEADO EM FAILOVER:* *O fornecedor de cloud oferece um serviço de sistema de nomes de domínio (DNS) compatível com o encaminhamento baseado em failover (ou seja, o serviço DNS encaminha as consultas DNS para o recurso que está ativo, enquanto um segundo recurso aguarda e só fica ativo no caso de uma falha no recurso principal)?*
36.	*REDES – SERVIÇO DE REGISTO DE DOMÍNIO:* *O fornecedor de cloud oferece serviços de registo de nomes de domínio (ou seja, os utilizadores podem pesquisar e registar nomes de domínio disponíveis)?*
37.	*REDES – VERIFICAÇÕES DE INTEGRIDADE DE DNS:* *O fornecedor de cloud oferece um serviço de sistema de nomes de domínio (DNS) que utiliza verificações de integridade para monitorizar a integridade e o desempenho dos recursos?*
38.	*REDES – INTEGRAÇÃO DE DNS E BALANCEADOR DE CARGA:* *O fornecedor de cloud oferece um serviço de sistema de nomes de domínio (DNS) que se integra com o balanceador de carga do fornecedor de cloud?*
39.	*REDE – EDITOR VISUAL:* *O fornecedor de cloud oferece uma ferramenta que permite aos utilizadores criarem políticas para a gestão de tráfego?*
40.	*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.	*REDE – EXPIRAÇÃO DA CACHE DE CDN:* *O fornecedor de cloud oferece um serviço de rede de entrega de conteúdo (CDN) que permite remover um objeto das caches edge antes que expire, incluindo funcionalidades como a invalidação e o controlo de versões de objetos?*
42.	*REDES – ORIGENS EXTERNAS DE CDN:* *O fornecedor de cloud oferece um serviço de rede de entrega de conteúdo (CDN) compatível com uma origem personalizada, ou seja, um servidor de protocolo de transferência de hipertexto (HTTP)?*
43.	*REDES – OTIMIZAÇÃO DE CDN:* *O fornecedor de cloud oferece um serviço de rede de entrega de conteúdo (CDN) com controlo granular para configurar vários servidores de origem e armazenar em cache propriedades para diferentes localizadores uniformes de recursos (URL)?*
44.	*REDES – CDN COM RESTRIÇÃO GEOGRÁFICA:* *O fornecedor de cloud oferece um serviço de rede de entrega de conteúdo (CDN) que suporta restrição geográfica, ou seja, impede que utilizadores em áreas geográficas específicas acedam a conteúdo?*
45.	*REDES – TOKENS DE CDN:* *O fornecedor de cloud oferece um serviço de rede de entrega de conteúdo (CDN) que suporta localizadores uniformes de recursos (URL) assinados que normalmente incluem informações adicionais, como data/hora de validade, para conceder aos utilizadores mais controlo sobre o acesso ao conteúdo?*
46.	*REDES – CERTIFICADOS DE CDN:* *O fornecedor de cloud oferece um serviço de rede de entrega de conteúdo (CDN) que suporta certificados Secure Sockets Layer (SSL) personalizados para fornecer conteúdo de forma segura por HTTPS a partir de localizações edge?*

47.	***REDES – CACHE MULTICAMADAS DE CDN:*** *O fornecedor de cloud oferece um serviço de rede de entrega de conteúdo (CDN) que aplica uma abordagem de cache multicamadas com a utilização de caches edge regionais para reduzir a latência?*
48.	***REDES – COMPRESSÃO DE CDN:*** *O fornecedor de cloud oferece um serviço de rede de entrega de conteúdo (CDN) compatível com a compressão de ficheiros?*
49.	***REDES – CARREGAMENTOS ENCRIPTADOS DE CDN:*** *O fornecedor de cloud oferece uma rede de entrega de conteúdo (CDN) que permite que os utilizadores façam o carregamento dos seus dados sensíveis com segurança, de forma a que essas informações só possam ser visualizadas por determinados componentes e serviços na infraestrutura de origem do utilizador?*
50.	***REDES – PONTOS FINAIS:*** *O serviço de rede do fornecedor de cloud oferece aos utilizadores pontos finais que podem encaminhar o tráfego através da ligação de rede interna do fornecedor (ou seja, ligação 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) relativamente à secção de redes acima?* *Exemplo:* *Número máximo de redes virtuais por conta* *Tamanho máximo de uma rede virtual* *Número máximo de sub-redes por conta* *Número máximo de balanceadores de carga por conta* *Número máximo de entradas da lista de controlo de acesso (ACL)* *Número máximo de túneis de rede privada virtual (VPN)* *Número máximo de origens por distribuição* *Número máximo de certificados por balanceador de carga*

3.3 Armazenamento

	Requisito
1.	***SERVIÇO DE ARMAZENAMENTO EM BLOCO:*** *O fornecedor de cloud oferece volumes de armazenamento em bloco para utilizar com instâncias de computação?*
2.	***ARMAZENAMENTO EM BLOCO – IOPS:*** *O fornecedor de cloud oferece a opção de compra de um nível de desempenho ou um objetivo 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 suporta dispositivos de armazenamento com base em unidades de estado sólido (SSD) que ofereçam latências de milissegundos com um único dígito?* • *Em caso afirmativo, qual é o número máximo de SSD que podem ser anexados por instância?*

4.	*ARMAZENAMENTO EM BLOCO – ESCALABILIDADE:* *O fornecedor de cloud oferece aos utilizadores a capacidade de aumentar o tamanho de um volume de armazenamento em bloco existente sem precisar de aprovisionar um novo volume e copiar/mover os dados?*
5.	*ARMAZENAMENTO EM BLOCO – SNAPSHOTS:* *O fornecedor de cloud tem capacidade de snapshot para o respetivo serviço de armazenamento em bloco?*
6.	*ARMAZENAMENTO EM BLOCO – ELIMINAÇÃO DE DADOS:* *O fornecedor de cloud suporta a eliminação completa de dados, para que não sejam legíveis ou acessíveis por utilizadores não autorizados e/ou terceiros?*
7.	*ARMAZENAMENTO EM BLOCO – ENCRIPTAÇÃO DE DADOS INATIVOS:* *O fornecedor de cloud oferece encriptação de dados inativos no lado do servidor para os dados armazenados em volumes e respetivos snapshots?* • *Em caso afirmativo, qual é o algoritmo criptográfico aplicado?*
8.	*SERVIÇO DE ARMAZENAMENTO DE OBJETOS:* *O fornecedor de cloud oferece armazenamento de objetos seguro, duradouro e altamente escalável para armazenar e obter 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 custo mais baixo destinado a armazenar objetos e ficheiros 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 mais baixo?*
11.	*ARMAZENAMENTO DE OBJETOS – ACESSO MENOS FREQUENTE:* *O fornecedor de cloud oferece um nível para dados acedidos com menos frequência, mas que ainda assim exijam um acesso rápido?*
12.	*ARMAZENAMENTO DE OBJETOS – CAMADAS DE OBJETOS:* *O fornecedor de cloud oferece a capacidade de armazenar objetos por níveis, ou seja, a capacidade de recomendar a transição de um objeto entre classes ou níveis de armazenamento de objetos com base na respetiva frequência de acesso?*
13.	*ARMAZENAMENTO DE OBJETOS – GESTÃO DO CICLO DE VIDA:* *O fornecedor de cloud suporta a gestão do ciclo de vida de um objeto através de uma configuração de ciclo de vida, que define a forma como os objetos são geridos durante a sua vida útil, desde a criação até à eliminação?*
14.	*ARMAZENAMENTO DE OBJETOS – GESTÃO CONTROLADA POR POLÍTICA:* *O fornecedor de cloud oferece a capacidade de criar e utilizar políticas para gerir dados armazenados, o respetivo ciclo de vida e as respetivas definições de níveis?*
15.	*ARMAZENAMENTO DE OBJETOS – POLÍTICAS BASEADAS EM LOCALIZAÇÃO E HORA:* *O fornecedor de cloud oferece aos utilizadores a capacidade de criar políticas que possam restringir o acesso aos dados com base na localização do utilizador e na hora do pedido?*
16.	*ARMAZENAMENTO DE OBJETOS – ALOJAMENTO DE SITES:* *O fornecedor de cloud suporta o alojamento de sites estáticos fora do serviço de armazenamento de objetos?*

17.	*ARMAZENAMENTO DE OBJETOS – ENCRIPTAÇÃO DE DADOS INATIVOS:* *O fornecedor de cloud suporta encriptação do lado do servidor (SSE) de dados inativos, com o fornecedor de cloud a gerir as chaves de encriptação?* • *Em caso afirmativo, qual é o algoritmo criptográfico aplicado?*
18.	*ARMAZENAMENTO DE OBJETOS – ENCRIPTAÇÃO COM CHAVES DO UTILIZADOR:* *O fornecedor de cloud oferece capacidades de encriptação do lado do servidor (SSE) com chaves de encriptação fornecidas pelo cliente?*
19.	*ARMAZENAMENTO DE OBJETOS – SERVIÇO GERIDO POR CHAVE:* *O fornecedor de cloud suporta encriptação do lado do servidor (SSE) com um serviço de gestão de chaves que cria chaves de encriptação, define as políticas que controlam como estas podem ser utilizadas e realiza auditorias de utilização de chaves para comprovar que estão a ser utilizadas corretamente?*
20.	*ARMAZENAMENTO DE OBJETOS – CHAVE MESTRA NO LADO DO CLIENTE:* *O fornecedor de cloud oferece aos utilizadores a opção de reter o controlo das chaves de encriptação e concluir a encriptação/desencriptação de objetos do lado do cliente?*
21.	*ARMAZENAMENTO DE OBJETOS – CONSISTÊNCIA FORTE:* *O fornecedor de cloud oferece uma consistência de leitura após a gravação para operações PUT para novos objetos?*
22.	*ARMAZENAMENTO DE OBJETOS – LOCALIDADE DOS DADOS:* *O fornecedor de cloud oferece um forte isolamento regional, para que os objetos armazenados numa região nunca deixem essa região, a menos que o utilizador os transfira explicitamente para outra região?*
23.	*ARMAZENAMENTO DE OBJETOS – REPLICAÇÃO:* *O fornecedor de cloud oferece uma funcionalidade de replicação entre regiões que replicará automaticamente os objetos nas regiões selecionadas pelo utilizador?*
24.	*ARMAZENAMENTO DE OBJETOS – CONTROLO DE VERSÕES:* *O fornecedor de cloud suporta o controlo de versões, ou seja, a capacidade de armazenar e manter várias versões de um objeto?*
25.	*ARMAZENAMENTO DE OBJETOS – MARCADOR DE ITEM NÃO ELIMINÁVEL:* *O fornecedor de cloud permite que um utilizador marque um item como não eliminável?*
26.	*ARMAZENAMENTO DE OBJETOS – EXCLUSÃO DE MFA:* *O fornecedor de cloud suporta a autenticação multifator (MFA) para operações de eliminação como uma opção de segurança adicional?*
27.	*ARMAZENAMENTO DE OBJETOS – CARREGAMENTO FRACIONADO:* *O fornecedor de cloud permite o carregamento de um objeto como um conjunto de partes, em que cada uma é uma porção contígua dos dados do objeto e o carregamento dessas partes de objetos pode ser feito de forma independente e em qualquer ordem?*
28.	*ARMAZENAMENTO DE OBJETOS – ETIQUETAS:* *O fornecedor de cloud oferece a capacidade de criar e associar etiquetas dinâmicas mutáveis ao nível do objeto?*
29.	*ARMAZENAMENTO DE OBJETOS – NOTIFICAÇÕES:* *O fornecedor de cloud oferece a capacidade de enviar notificações quando determinados eventos ocorrem ao nível do objeto (ou seja, operações de adição/eliminação)?*

30.	*ARMAZENAMENTO DE OBJETOS – REGISTOS:* *O fornecedor de cloud oferece a capacidade de criar registos de auditoria que incluam detalhes sobre um pedido único de acesso, como o requerente, o horário do pedido, a ação do pedido, o estado 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 permitir aos utilizadores visualizar rapidamente objetos e o respetivo estado, permitindo-lhes identificar rapidamente os objetos com acesso público?*
32.	*ARMAZENAMENTO DE OBJETOS – INVENTÁRIO PARA METADADOS:* *O fornecedor de cloud oferece recursos de inventário de objetos para permitir aos utilizadores visualizar rapidamente os metadados dos objetos?*
33.	*ARMAZENAMENTO DE OBJETOS – OTIMIZAÇÃO DE CARREGAMENTOS:* *O fornecedor de cloud oferece a capacidade de encaminhar dados de localizações edge para o serviço de armazenamento através de um caminho de rede otimizado?*
34.	*ARMAZENAMENTO DE OBJETOS – RECURSO DE CONSULTAS:* *O fornecedor de cloud oferece aos utilizadores a capacidade de consultar o seu serviço de armazenamento de objetos através de instruções de linguagem de consulta estruturada (SQL)?*
35.	*ARMAZENAMENTO DE OBJETOS – RECUPERAÇÃO DE SUBCONJUNTOS:* *O fornecedor de cloud oferece aos utilizadores a capacidade de recuperar apenas um subconjunto de dados de um objeto através de expressões simples de linguagem de consulta estruturada (SQL)?*
36.	*SERVIÇO DE ARMAZENAMENTO DE FICHEIROS:* *O fornecedor de cloud oferece um serviço de armazenamento de ficheiros simples e escalável para utilizar com instâncias de computação na cloud?*
37.	*ARMAZENAMENTO DE FICHEIROS – REDUNDÂNCIA:* *O fornecedor de cloud armazena de forma redundante os objetos do sistema de ficheiros (ou seja, diretório, ficheiro e ligação) em vários datacenters ou instalações para alcançar níveis mais altos de disponibilidade e durabilidade?*
38.	*ARMAZENAMENTO DE FICHEIROS – ELIMINAÇÃO DE DADOS:* *O fornecedor de cloud suporta a eliminação completa de dados de armazenamento de ficheiros, para que não sejam legíveis ou acessíveis por utilizadores não autorizados ou terceiros?*
39.	*ARMAZENAMENTO DE FICHEIROS – ALTA DISPONIBILIDADE:* *O sistema de ficheiros geridos do fornecedor de cloud fornece um nível elevado de alta disponibilidade?*
40.	*ARMAZENAMENTO DE FICHEIROS – NFS:* *O fornecedor de cloud suporta o protocolo de sistema de ficheiros de rede (NFS)?*
41.	*ARMAZENAMENTO DE FICHEIROS – SMB:* *O fornecedor de cloud suporta o protocolo de bloco de mensagens de servidor (SMB)?*
42.	*ARMAZENAMENTO DE FICHEIROS – ENCRIPTAÇÃO DE DADOS INATIVOS:* *O serviço de armazenamento de ficheiros do fornecedor de cloud suporta a encriptação de dados inativos?*
43.	*ARMAZENAMENTO DE FICHEIROS – ENCRIPTAÇÃO DE DADOS EM TRÂNSITO:* *O serviço de armazenamento de ficheiros do fornecedor de cloud suporta a encriptação de dados em trânsito?*
44.	*ARMAZENAMENTO DE FICHEIROS – 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 on-premises para o sistema de ficheiros baseado na cloud?*

45.	***SERVIÇO DE ARMAZENAMENTO DE ARQUIVO:*** *O fornecedor de cloud oferece um serviço de armazenamento de custo muito baixo destinado a arquivar objetos e ficheiros acedidos com menos frequência e praticamente imutáveis?*
46.	***ARMAZENAMENTO DE ARQUIVO – TOLERÂNCIA A FALHAS:*** *A arquitetura do fornecedor de cloud fornece tolerância a falhas para o serviço de armazenamento de arquivo?*
47.	***ARMAZENAMENTO DE ARQUIVO – IMUTABILIDADE:*** *O fornecedor de cloud suporta a imutabilidade dos ficheiros e objetos arquivados?*
48.	***ARMAZENAMENTO DE ARQUIVO – WORM:*** *O fornecedor de cloud oferece a capacidade WORM (uma gravação e muitas leituras)?*
49.	***ARMAZENAMENTO DE ARQUIVO – RECUPERAÇÃO DE SUBCONJUNTOS:*** *O fornecedor de cloud oferece aos utilizadores a capacidade de recuperar apenas um subconjunto de dados de um objeto arquivado através de expressões simples de linguagem de consulta estruturada (SQL)?*
50.	***ARMAZENAMENTO DE ARQUIVO – 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 ARQUIVO – ENCRIPTAÇÃO DE DADOS INATIVOS*** *O serviço de armazenamento de arquivo do fornecedor de cloud suporta a encriptação de dados inativos?*
52.	***ARMAZENAMENTO – LIMITES DE SERVIÇO:*** *O fornecedor de cloud possui alguma restrição (ou seja, limites de serviço) relativamente à secção 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 respetiva infraestrutura e recursos?*
2.	***ADMINISTRAÇÃO – REDEFINIÇÃO DA PALAVRA-PASSE:*** *O fornecedor de cloud permite que os utilizadores redefinam as suas próprias palavras-passe de forma self-service?*
3.	***ADMINISTRAÇÃO – PERMISSÕES:*** *O fornecedor de cloud oferece a capacidade de adicionar permissões para utilizadores e grupos ao 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 a utilizadores confiáveis configuradas para durar desde alguns minutos até várias horas?*
6.	***ADMINISTRAÇÃO – CONTROLO DE ACESSO:*** *O fornecedor de cloud oferece controlos de acesso granulares para os respetivos recursos de infraestrutura?* • *Em caso afirmativo, que condições podem ser utilizadas por esses controlos (ou seja, hora do dia, endereço IP de origem, etc.)?*
7.	***ADMINISTRAÇÃO – POLÍTICAS INTEGRADAS:*** *A infraestrutura do fornecedor de cloud contém políticas de controlo de acesso integradas que podem ser anexadas a utilizadores e grupos?*
8.	***ADMINISTRAÇÃO – POLÍTICAS PERSONALIZADAS:*** *A infraestrutura do fornecedor de cloud permite criar e personalizar políticas de controlo de acesso que podem ser anexadas a utilizadores e grupos?*
9.	***ADMINISTRAÇÃO: SIMULADOR DE POLÍTICAS:*** *O fornecedor de cloud oferece um mecanismo para testar os efeitos das políticas de controlo de acesso antes de enviar tais políticas para produção?*
10.	***ADMINISTRAÇÃO – MFA DE CLOUD:*** *O fornecedor de cloud suporta a utilização de autenticação multifator (MFA) como uma camada adicional de controlo de acesso e autenticação para a respetiva infraestrutura?*
11.	***ADMINISTRAÇÃO – LIMITES DE SERVIÇO:*** *O fornecedor de cloud possui alguma restrição (ou seja, limites de serviço) relativamente à secção de administração acima?* *Exemplo:* *Número máximo de utilizadores* *Número máximo de grupos* *Número máximo de políticas geridas*

5. Segurança

	Requisito
1.	***SEGURANÇA – VERIFICAÇÕES DE ANTECEDENTES:*** *Todo o pessoal do fornecedor de cloud com acesso à infraestrutura do serviço (seja física ou não física) é 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 pedido de suporte específico para um problema, pedido de alteração ou autorização formal semelhante?*

3.	*SEGURANÇA – REGISTOS DE ACESSO:* *O fornecedor de cloud regista o acesso do pessoal à infraestrutura, onde tal acesso é sempre registado e os registos são mantidos durante pelo menos 90 dias?*
4.	*SEGURANÇA – INÍCIOS DE SESSÃO DE ANFITRIÕES:* *O fornecedor de cloud impede que o respetivo pessoal inicie sessão em anfitriões computacionais, automatizando todas as tarefas realizadas em anfitriões computacionais onde o conteúdo dessas tarefas automatizadas é registado, com os registos mantidos durante pelo menos 90 dias?*
5.	*SEGURANÇA – CHAVES CRIPTOGRÁFICAS:* *O fornecedor de cloud oferece um serviço para criar e controlar as chaves criptográficas utilizadas para encriptar dados de utilizador?*
6.	*SEGURANÇA – GESTÃO DE CHAVE DE ACESSO:* *O fornecedor de cloud oferece a capacidade de identificar quando uma chave de acesso foi utilizada pela última vez, alternar chaves antigas e remover utilizadores inativos?*
7.	*SEGURANÇA – CHAVES FORNECIDAS PELO CLIENTE:* *O fornecedor de cloud permite que os utilizadores importem chaves a partir das suas próprias infraestruturas de gestão de chaves para o serviço de gestão de chaves do fornecedor do serviço de cloud?*
8.	*SEGURANÇA – INTEGRAÇÃO DO SERVIÇO DE CHAVES CRIPTOGRÁFICAS:* *O serviço de gestão de chaves do fornecedor de cloud está integrado com outros serviços de cloud para fornecer capacidade de encriptação de dados inativos?*
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 criptográficas seguras dentro de um módulo de hardware resistente a adulteração?*
10.	*SEGURANÇA – DURABILIDADE DE CHAVES CRIPTOGRÁFICAS:* *O fornecedor de cloud suporta a 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 autenticação única (SSO) gerido que permita aos utilizadores gerir de forma centralizada o acesso a várias contas e aplicações empresariais?*
12.	*SEGURANÇA – CERTIFICADOS:* *O fornecedor de cloud oferece um serviço gerido para aprovisionar, gerir e implementar 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 DE CARÁTER VARIÁVEL:* *O serviço de gestão de certificados do fornecedor de cloud suporta a utilização de certificados de caráter variável?*
15.	*SEGURANÇA – AUTORIDADE DE CERTIFICAÇÃO:* *O serviço de gestão de certificados do fornecedor de cloud também atua como uma autoridade de certificação (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 suporta a integração com o Active Directory (AD) da Microsoft on-premises?*
18.	*SEGURANÇA – LDAP:* *O serviço gerido de Active Directory (AD) da Microsoft do fornecedor de cloud suporta o Lightweight Directory Access Protocol (LDAP)?*
19.	*SEGURANÇA – ACTIVE DIRECTORY:* *O serviço gerido de Active Directory (AD) da Microsoft do fornecedor de cloud suporta a Security Assertion Markup Language (SAML)?*
20.	*SEGURANÇA – GESTÃO DE CREDENCIAIS:* *O fornecedor de cloud oferece um serviço gerido que ajuda os utilizadores a alternar, gerir e recuperar credenciais, como chaves da interface de programação de aplicações (API), credenciais de bases de dados e outros segredos facilmente?*
21.	*SEGURANÇA – WAF:* *O fornecedor de cloud oferece uma firewall de aplicações Web (WAF) que ajuda a proteger aplicações Web contra ataques 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 na rede e ataques distribuídos de negação de serviço (DDoS) da camada de transporte, juntamente 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 potenciais vulnerabilidades em aplicações e recursos?*
24.	*SEGURANÇA – DETEÇÃO DE AMEAÇAS:* *O fornecedor de cloud oferece um serviço gerido de deteção de ameaças?*
25.	*SEGURANÇA – LIMITES DE SERVIÇO:* *O fornecedor de cloud possui alguma restrição (ou seja, limites de serviço) relativamente à secção de segurança acima?* *Exemplo:* *Número máximo de chaves mestras do cliente* *Número máximo de módulos de segurança de hardware (HSM)*

6. Conformidade

A lista abaixo serve apenas para fins ilustrativos e não deve ser considerada com uma lista completa das certificações e padrões que podem ser aplicados aos serviços de cloud.

Indique o conjunto de padrões de conformidade internacionais e específicos do setor que o fornecedor de cloud cumpre:

Certificações/Atestações	*Leis, regulamentos e privacidade*	*Alinhamentos/Enquadramentos*
☐ C5 [Alemanha]	*☐ Diretiva relativa à proteção de dados da UE*	*☐ CDSA*

☐ *Código de Conduta de Proteção de Dados do CISPE*	☐ *Cláusulas-tipo da UE*	
☐ *CNDCP (Climate Neutral Data Centre Pact)*		
☐ *DIACAP*	☐ *FERPA*	☐ *CIS*
☐ *DoD SRG, níveis 2 e 4*	☐ *RGPD*	☐ *Criminal Justice Info. Service (CJIS)*
☐ *FedRAMP*	☐ *GLBA*	☐ *CSA*
☐ *FIPS 140-2*	☐ *HIPAA*	☐ *Escudo de Proteção da Privacidade UE-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 (Singapura)*	☐ *Lei da Privacidade (Austrália)*	☐ *IT Grundschutz (Alemanha)*
☐ *PCI DSS, nível 1*	☐ *Lei da Privacidade (Nova Zelândia)*	☐ *MARS – E*
☐ *Regra SEC 17-a-4(f)*	☐ *Autorização da APD de Espanha*	☐ *MITA 3.0*
☐ *SOC1/ISAE 3402*	☐ *DPA do Reino Unido (1988)*	☐ *MPAA*
☐ *SOC2/SOC3*	☐ *VPAT/Secção 508*	☐ *NIST*
☐ *Código para IaaS da SWIPO*		
		☐ *Níveis do Uptime Institute*
		☐ *Princípios de segurança na cloud do Reino Unido*

Utilizar 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 operações. Esses relatórios podem mostrar que o CISP, através da sua conformidade, cumpre os controlos de operações de datacenter abaixo, que são exigidos do fornecedor de serviços de cloud pública. Exigir a conformidade com esses relatórios ajuda as entidades do setor público a garantir que os controlos abaixo sejam implementados.

- *Acesso verificado: o CISP deve restringir o acesso físico a pessoas que precisam de estar no local por motivo profissional justificável. Se o acesso for concedido, o mesmo deve ser revogado assim que o trabalho necessário estiver concluído.*

- *Entrada controlada e monitorizada: a entrada na camada de perímetro do datacenter deve ser um processo controlado. O CISP deve ter responsáveis por segurança nos portões de entrada e supervisores para monitorizar os funcionários e visitantes através de câmaras de segurança. Quando for aprovada a permanência de indivíduos no local, os mesmos deverão receber um distintivo que exija autenticação multifator e limite o acesso às áreas pré-aprovadas.*

- *Funcionários do datacenter do CISP: os funcionários do CISP que precisam de acesso diário a um datacenter devem receber as permissões para as áreas relevantes da instalação com base no respetivo cargo, com acesso regularmente verificado. As listas de funcionários devem ser revistas diariamente por um gestor de acesso à área para garantir que a autorização de cada funcionário ainda é necessária. Se um funcionário não tiver de estar num datacenter por motivos profissionais, deverá entrar através do processo de visitantes.*

- *Monitorização de entradas não autorizadas: os CISP devem monitorizar continuamente a entrada não autorizada na propriedade do datacenter, através de vigilância por vídeo, deteção de invasões e sistemas de monitorização de registos de acesso. As entradas devem estar protegidas por dispositivos que acionam alarmes caso uma porta seja arrombada ou mantida aberta.*

- *Segurança global monitorizada pelos centros de operações de segurança do CISP: os centros de operações de segurança do CISP devem estar espalhados pelo mundo e ser responsáveis por monitorizar, fazer a triagem e executar programas de segurança para datacenters do CISP. Devem supervisionar a gestão de acesso físico e a resposta a deteções de invasão e oferecer suporte global 24/7 às equipas de segurança do datacenter no local; realizar atividades de monitorização contínua (por ex.: controlar atividades de acesso e revogar permissões de acesso) e analisar e responder a possíveis incidentes de segurança.*

- *Análise de acesso por camada: o acesso à camada de infraestrutura deve ser restrito com base na necessidade da empresa. Com a implementação da análise de acesso por camada, o direito de aceder a cada camada não é concedido por predefinição. O acesso a uma determinada camada deve ser concedido somente quando há uma necessidade específica.*

- *A manutenção dos equipamentos faz parte das operações regulares: as equipas do CISP devem executar diagnósticos em máquinas, redes e equipamentos de backup para que estejam prontos a funcionar no imediato e em caso de emergência. As verificações de manutenção de rotina nos equipamentos do datacenter devem fazer parte das operações regulares do datacenter do CISP.*

- *Equipamentos de backup disponíveis para emergência: água, energia, telecomunicações e ligação à 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 falha, as unidades de fonte de alimentação ininterrupta estejam prontas para determinadas funções, enquanto os geradores fornecem energia à instalação completa. A temperatura e a humidade devem ser monitorizadas por pessoas e sistemas para evitar o sobreaquecimento, reduzindo possíveis falhas no serviço.*

- *Pessoas e tecnologia a trabalhar em conjunto para que haja mais segurança: devem existir procedimentos obrigatórios para que se obtenha autorização de acesso à camada de dados. Isto inclui a análise e aprovação do pedido de acesso de uma pessoa por parte de indivíduos autorizados. Enquanto isso, os sistemas eletrónicos de deteção de ameaças e invasões devem monitorizar e acionar alarmes automaticamente para ameaças identificadas ou atividades suspeitas. Por exemplo, se uma porta for arrombada ou mantida aberta, será acionado um alarme. O CISP deve implementar câmaras de segurança e guardar as gravações de acordo com os requisitos legais e de conformidade.*

- *Impedir invasões físicas e tecnológicas: os pontos de acesso a salas de servidor devem ser reforçados com dispositivos de controlo eletrónico que exijam autorização multifator. O CISP também deve preparar-se para evitar intrusões tecnológicas. Os servidores do CISP devem ter a capacidade de alertar os funcionários sobre quaisquer tentativas de remoção de dados. No improvável caso de uma infração, o servidor deve ser desativado automaticamente.*

- *Servidores e suportes de dados recebem atenção imediata: os dispositivos de armazenamento utilizados para armazenar dados dos clientes devem ser classificados pelo CISP como críticos e tratados como tal (de alto impacto) durante todo o seu ciclo de vida. O CISP deve aplicar padrões rigorosos sobre como instalar, reparar e até destruir os dispositivos quando deixam de ser úteis. Quando um dispositivo de armazenamento chega ao fim da sua vida útil, o*

CISP deve desativar o suporte de dados com as técnicas dispostas no NIST 800-88. Os suportes de dados que armazenam dados dos clientes não são removidos do controlo do CISP até que sejam desativados de forma segura.

- *Auditores de terceiros verificam os procedimentos e sistemas do CISP: o CISP deve ser auditado por auditores externos para inspecionar datacenters e confirmar se o CISP está a seguir as regras estabelecidas necessárias para obter as suas certificações de segurança. Consoante o programa de conformidade e os respetivos requisitos, os auditores externos podem perguntar aos funcionários do CISP sobre como lidam com e eliminam suportes de dados. Os auditores também podem assistir a gravações das câmaras de segurança e observar entradas e corredores num datacenter. Além disso, podem examinar equipamentos do CISP, como dispositivos de controlo de acesso eletrónico e câmaras de segurança.*

- *Preparado para o inesperado: o CISP deve preparar-se de forma proativa para possíveis ameaças ambientais, como desastres naturais e incêndios. Instalar sensores automáticos e equipamentos de resposta são duas maneiras de o CISP proteger os seus datacenters. Os dispositivos de deteção de água devem ser instalados para alertar os funcionários quanto a problemas, enquanto as bombas automáticas removem líquidos e evitam danos. De forma semelhante, os equipamentos automáticos de deteção e extinção de incêndios reduzem os riscos e podem notificar os funcionários do CISP e bombeiros sobre um problema.*

- *Alta disponibilidade através de várias zonas de disponibilidade: o CISP deve fornecer várias zonas de disponibilidade para ter uma maior tolerância a falhas. Cada zona de disponibilidade deve consistir num ou mais datacenters, estar fisicamente separada da outra e ter energia e rede redundantes. As zonas de disponibilidade devem estar ligadas entre si com rede de fibra ótica rápida e privada para arquitetar aplicações que tenham um failover automático entre as zonas de disponibilidade sem interrupção.*

- *Simular interrupções e medir a resposta: o CISP deve ter um plano de continuidade de negócios, como um guia de processos de operações que descreva como evitar e reduzir interrupções devidas a desastres naturais, com passos detalhados a realizar antes, durante e depois de um evento. Para atenuar e preparar-se para o inesperado, o CISP deve testar regularmente o plano de continuidade de negócios com exercícios que simulem diferentes cenários. O CISP deve documentar os resultados dos respetivos funcionários e processos e, em seguida, resumir as ilações retiradas e as ações corretivas que possam ser necessárias para melhorar a taxa de resposta. Os funcionários do CISP devem estar treinados e prontos para recuperar rapidamente das interrupções, com um processo de recuperação metódico para minimizar mais interrupções devido a erros.*

- *Ajudar a atingir objetivos de eficiência: além de abordar riscos ambientais, o CISP também deve incorporar considerações de sustentabilidade no design dos seus datacenters. O CISP deve fornecer detalhes do seu compromisso para com a utilização de energias renováveis para os seus datacenters e fornecer informações sobre como os seus clientes podem reduzir emissões de carbono por oposição aos seus próprios datacenters.*

- *Seleção de local: antes de escolher um local, o CISP deve realizar avaliações ambientais e geográficas iniciais. Os locais dos datacenters devem ser selecionados com atenção para reduzir riscos ambientais, como inundações, condições meteorológicas extremas e atividade sísmica. As zonas de disponibilidade do CISP devem ser criadas para serem independentes e fisicamente separadas umas das outras.*

- *Redundância: os datacenters devem ser criados para antecipar e tolerar falhas sem deixar de manter os níveis de serviço. Em caso de falha, os processos automatizados devem desviar o tráfego de dados dos clientes da área afetada. As aplicações principais devem ser implementadas numa configuração N+1, para que, na eventualidade de uma falha no datacenter, exista capacidade suficiente para permitir o equilíbrio da carga de tráfego nos restantes locais.*

- *Disponibilidade: o CISP deve identificar componentes críticos do sistema necessários para manter a disponibilidade do seu sistema e recuperar o serviço no caso de indisponibilidade. Dever ser realizado um backup dos componentes críticos do sistema em várias localizações isoladas. Cada localização ou zona de disponibilidade deve ser criada para operar de forma independente com alta fiabilidade. As zonas de disponibilidade devem estar ligadas para que as aplicações tenham um failover automático sem interrupção entre as zonas de disponibilidade. Os sistemas altamente resilientes e, consequentemente, a disponibilidade do serviço, devem ser características consideradas no design do sistema. O design do datacenter com zonas de disponibilidade e replicação de dados deve permitir que os clientes do CISP alcancem 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 monitorizar a utilização do serviço de forma contínua para implementar uma infraestrutura que permita cumprir os compromissos e requisitos de disponibilidade. O CISP deve manter um modelo de planeamento de capacidade que avalie, pelo menos, mensalmente a utilização e as exigências da infraestrutura do CISP. Este modelo deve ajudar no planeamento de futuras exigências e incluir considerações, como processamento de informações, telecomunicações e armazenamento de registos 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 os passos a adotar antes, durante e depois de um evento. O plano de continuidade dos negócios deve ser fundamentado 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 de correção e as lições aprendidas com o intuito de obter melhorias contínuas.*

- ***Resposta em caso de pandemia:*** *o CISP deve incorporar políticas e procedimentos de respostas a pandemias no planeamento de recuperação de desastres para se preparar para responder com rapidez a ameaças de doenças infeciosas. As estratégias de mitigação incluem modelos alternativos de alocação de funcionários para transferir processos críticos para recursos fora da região e a ativação de um plano de gestão de crises para ajudar nas operações empresariais mais importantes. Os planos para pandemias devem fazer referência a agências e regulamentações de saúde internacionais, incluindo pontos de contacto de agências internacionais.*

MONITORIZAÇÃO E REGISTO

- ***Análise de acesso a datacenters:*** *o acesso aos datacenters deve ser sempre analisado. O acesso também é automaticamente revogado quando o registo de um funcionário é cancelado no sistema de recursos humanos do CISP. Além disso, quando o acesso de um funcionário ou subcontratado expira de acordo com a duração do pedido aprovado, o acesso deve ser revogado mesmo que continue a ser funcionário do CISP.*

- ***Registos de acesso a datacenters:*** *o acesso físico aos datacenters do CISP deve ser registado, monitorizado e mantido. O CISP deve correlacionar as informações obtidas dos sistemas de monitorização lógicos e físicos para melhorar a segurança conforme necessário.*

- ***Monitorização de acesso a datacenters:*** *o CISP deve monitorizar os datacenters através de centros de operações de segurança globais, responsáveis por monitorizar, fazer a triagem e executar programas de segurança. Devem fornecer suporte global 24/7 ao gerir e monitorizar atividades de acesso aos datacenters, equipar equipas locais e outras equipas de suporte para responder a incidentes de segurança através da triagem, análise e envio de respostas.*

VIGILÂNCIA E DETEÇÃO

- ***CCTV:*** *os pontos de acesso físico a salas de servidor devem ser gravados por câmaras de televisão em circuito fechado (CCTV). As imagens devem ser mantidas de acordo com os requisitos legais e de conformidade.*

- ***Pontos de entrada do datacenter:*** *o acesso físico deve ser controlado em pontos de entrada do edifício por uma equipa de segurança profissional através de videovigilância, sistemas de deteção de intrusão e outros meios eletrónicos. Os funcionários autorizados devem utilizar mecanismos de autenticação multifator para aceder aos datacenters. As entradas das salas de servidores devem ser protegidas com dispositivos que acionam alarmes para iniciar uma resposta a um incidente caso a porta seja arrombada ou mantida aberta.*

- ***Deteção de intrusão:*** *os sistemas de deteção de intrusão eletrónica devem ser instalados na camada de dados para monitorizar, detetar e alertar automaticamente o pessoal competente acerca de incidentes de segurança. Os pontos de entrada e saída nas salas de servidores devem ser protegidos com dispositivos que obrigam todas as pessoas a efetuar uma autenticação multifator antes de permitir a sua entrada ou saída. Estes dispositivos acionam alarmes se a entrada for forçada sem autenticação ou se a porta ficar aberta. Os dispositivos de alarme nas portas também devem ser configurados para detetar instâncias em que uma pessoa sai ou entra numa camada de dados sem fazer a autenticação multifator. Os alarmes devem notificar de imediato os centros de operações de segurança do CISP (24/7), para registo, análise e resposta imediatos.*

GESTÃO DE DISPOSITIVOS

- ***Gestão de ativos:*** *os ativos do CISP devem ser geridos de forma centralizada através de um sistema de gestão de inventário que armazena e monitoriza informações sobre o proprietário, local, estado, manutenção e descrição. Depois da aquisição, os ativos devem ser analisados e controlados. Os ativos em manutenção devem ser analisados e monitorizados quanto à propriedade, estado e resolução.*

- ***Destruição de suportes de dados:*** *os dispositivos de armazenamento utilizados para armazenar dados dos clientes devem ser classificados pelo CISP como críticos e tratados como tal (de alto impacto) durante todo o seu ciclo de vida. O CISP deve aplicar padrões rigorosos sobre como instalar, reparar e até destruir os dispositivos quando deixam de ser úteis. Quando um dispositivo de armazenamento chega ao fim da sua vida útil, o CISP deve desativar o suporte de dados com as técnicas dispostas no NIST 800-88. Os suportes de dados que armazenam dados dos clientes não devem ser removidos do controlo do CISP até que sejam desativados de forma segura.*

SISTEMAS DE SUPORTE OPERACIONAL

- ***Energia****: os sistemas de energia elétrica dos datacenters do CISP devem ser concebidos para serem totalmente redundantes e passíveis de manutenção sem impacto nas operações, 24 horas por dia. O CISP deve garantir que os datacenters estão equipados com uma unidade de alimentação de reserva para garantir que existe energia disponível para carregamentos críticos e essenciais na instalação em caso de falha elétrica.*

- ***Clima e temperatura:*** *os datacenters do CISP devem utilizar mecanismos para controlar o clima e manter uma temperatura de funcionamento apropriada para servidores e outro hardware, impedindo o sobreaquecimento e reduzindo a possibilidade de falhas de serviço. O pessoal e os sistemas devem monitorizar e controlar a temperatura e a humidade.*

- ***Deteção e extinção de incêndios:*** *os datacenters do CISP devem estar equipados com sistemas automáticos de deteção e extinção de incêndios. Os sistemas de deteção de incêndio devem utilizar sensores de deteção de fumo dentro dos espaços de redes, mecânicos e de infraestrutura. Estas áreas devem estar protegidas pelos sistemas de extinção.*

- ***Deteção de fugas:*** *para detetar a presença de uma fuga de água, o CISP deve equipar os datacenters com funcionalidades para detetar a presença de água. Se for detetada água, existem mecanismos preparados para a remover e impedir danos adicionais causados pela mesma.*

MANUTENÇÃO DA INFRAESTRUTURA

- ***Manutenção de equipamentos:*** *o CISP deve monitorizar e fazer a manutenção preventiva de equipamentos elétricos e mecânicos para manter a operacionalidade contínua dos sistemas nos datacenters do CISP. Os procedimentos de manutenção dos equipamentos devem ser realizados por profissionais qualificados e de acordo com um programa de manutenção documentado.*

- ***Gestão do ambiente:*** *o CISP deve monitorizar os sistemas mecânicos e elétricos e equipamentos para possibilitar a identificação imediata de problemas. Isto deve ser realizado através da utilização de ferramentas de auditoria contínua e informações fornecidas por sistemas de gestão técnica centralizada e monitorização elétrica do CISP. A manutenção preventiva deve ser realizada para manter a operacionalidade contínua dos equipamentos.*

GOVERNANÇA E RISCO

- ***Gestão contínua de riscos dos datacenters:*** *o centro de operações de segurança do CISP deve fazer análises regulares de ameaças e vulnerabilidades dos datacenters. A avaliação contínua e a mitigação de potenciais vulnerabilidades devem ser realizadas através de atividades de avaliação de riscos do datacenter. Esta avaliação deve ser realizada como complemento do processo de avaliação de riscos de nível empresarial já utilizado para identificar e gerir riscos para a empresa como um todo. Este processo também deve ter em consideração os riscos ambientais e riscos regulamentares regionais.*

- ***Certificação de segurança de terceiros:*** *os testes aos datacenters do CISP realizados por terceiros, conforme documentado nos relatórios de terceiros, devem garantir que o CISP tem medidas de segurança adequadamente implementadas em alinhamento com as regras estabelecidas necessárias para obter certificações de segurança. Consoante o programa de conformidade e os respetivos requisitos, os auditores externos podem realizar testes de eliminação de suportes de dados, ver gravações das câmaras de segurança, observar entradas e corredores num datacenter, testar dispositivos de controlo de acesso eletrónico e examinar equipamentos do datacenter.*

7. Migrações

	Requisito
1.	*SERVIÇO DE MIGRAÇÕES:* *Quantos serviços de migração de dados diferentes é que o fornecedor de cloud oferece?*
2.	*MIGRAÇÕES – MONITORIZAÇÃO CENTRALIZADA:* *O fornecedor de cloud oferece às organizações um serviço centralizado (ou seja, um único painel), onde podem acompanhar e monitorizar o estado das suas migrações de servidores e aplicações?*
3.	*MIGRAÇÕES – PAINEL:* *A ferramenta de migração do fornecedor de cloud oferece um painel para visualizar rapidamente o estado das migrações, métricas relacionadas e histórico de migrações?*
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?* • *Em caso afirmativo, quais são as ferramentas de migração de terceiros suportadas?*
6.	*MIGRAÇÕES – MIGRAÇÕES EM VÁRIAS REGIÕES:* *A ferramenta de migração do fornecedor de cloud oferece capacidades de acompanhamento e monitorização para migrações de servidores e aplicações que ocorram em diferentes regiões?*
7.	*MIGRAÇÕES – MIGRAÇÃO DE SERVIDORES:* *A ferramenta de migração do fornecedor de cloud oferece uma forma de migrar servidores virtualizados on-premises para a cloud?* • *Em caso afirmativo, quais são os ambientes virtualizados suportados atualmente?*
8.	*MIGRAÇÕES – DETEÇÃO DE SERVIDORES:* *A ferramenta de migração do fornecedor de cloud oferece capacidades de deteção para encontrar automaticamente servidores virtuais on-premises a serem migrados para a cloud?*
9.	*MIGRAÇÕES – DADOS DE DESEMPENHO DO SERVIDOR:* *A ferramenta de migração do fornecedor de cloud consegue recolher e apresentar o desempenho de servidores e/ou máquinas virtuais, como a utilização da unidade de processamento central (CPU) e da memória de acesso aleatório (RAM)?*
10.	*MIGRAÇÕES – BASE DE DADOS DE DETEÇÃO:* *A ferramenta de migração do fornecedor de cloud oferece a capacidade de armazenar todos os dados recolhidos numa base de dados centralizada?* • *Em caso afirmativo, as organizações podem exportar esses dados? Para que formatos?*

11.	*MIGRAÇÕES – ENCRIPTAÇÃO DE DADOS INATIVOS:* *O fornecedor de cloud encripta todas as informações inativas recolhidas e armazenadas na base de dados de deteção?*
12.	*MIGRAÇÕES – REPLICAÇÃO DE SERVIDOR INCREMENTAL:* *A ferramenta de migração do fornecedor de cloud permite uma replicação automatizada e em tempo real do servidor incremental durante a migração do servidor ou da máquina virtual, para garantir que todas as alterações efetuadas no servidor ou na máquina virtual são incluídas na imagem migrada final?* • *Em caso afirmativo, durante quanto tempo é que este serviço pode ser executado?*
13.	*MIGRAÇÕES – VMWARE:* *A ferramenta de migração do fornecedor de cloud suporta migrações de máquinas virtuais VMWare on-premises para a cloud?*
14.	*MIGRAÇÕES – HYPER-V:* *A ferramenta de migração do fornecedor de cloud suporta migrações de máquinas virtuais Hyper-V on-premises para a cloud?*
15.	*MIGRAÇÕES – DETEÇÃO DE APLICAÇÕES:* *A ferramenta de migração do fornecedor de cloud oferece a capacidade de detetar e agrupar aplicações antes de serem migradas?*
16.	*MIGRAÇÕES – MAPEAMENTO DE DEPENDÊNCIAS:* *A ferramenta de migração do fornecedor de cloud oferece a capacidade de detetar dependências entre servidores e aplicações antes de serem migradas?*
17.	*MIGRAÇÕES – MIGRAÇÃO DE BASES DE DADOS:* *A ferramenta de migração do fornecedor de cloud tem a capacidade de migrar bases de dados on-premises para a cloud?*
18.	*MIGRAÇÕES – TEMPO DE INATIVIDADE DA MIGRAÇÃO DE BASE DE DADOS:* *A ferramenta de migração do fornecedor de cloud tem a capacidade de realizar uma migração de base de dados para a cloud com um tempo de inatividade mínimo, ou seja, uma migração em que a base de dados de origem deva permanecer totalmente operacional durante o processo?*
19.	*MIGRAÇÕES – BASE DE DADOS DE ORIGEM:* *A ferramenta de migração do fornecedor de cloud suporta a migração de diferentes bases de dados de origem, como Oracle, SQL Server, etc.?* • *Em caso afirmativo, enumere todas as bases de dados de origem suportadas que podem ser migradas para a cloud.*
20.	*MIGRAÇÕES – MIGRAÇÕES HETEROGÉNEAS:* *A ferramenta de migração do fornecedor de cloud permite a realização de migrações de bases de dados heterogéneas, ou seja, de uma base de dados de origem para uma base de dados de destino diferente, como de Oracle para SQL Server?* • *Em caso afirmativo, enumere todas as combinações de migração de bases de dados heterogéneas 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 utiliza dispositivos seguros para transferir grandes quantidades de dados para dentro e 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 EMPRESARIAIS:* *O fornecedor de cloud oferece um serviço para integrar perfeitamente o datacenter de um cliente com serviços de armazenamento na cloud que permitirão transferir e armazenar dados no serviço de armazenamento do fornecedor de cloud?*
24.	*MIGRAÇÕES – BACKUPS EMPRESARIAIS – ARMAZENAMENTO DE OBJETOS:* *O serviço de backup empresarial do fornecedor de cloud oferece a integração com o serviço de armazenamento de objetos na cloud do fornecedor?*
25.	*MIGRAÇÕES – BACKUPS EMPRESARIAIS– ACESSO A FICHEIROS:* *O serviço de backup empresarial do fornecedor de cloud permite que os utilizadores armazenem e recuperem objetos através de protocolos de ficheiros, como o protocolo do sistema de ficheiros de rede (NFS)?*
26.	*MIGRAÇÕES – BACKUPS EMPRESARIAIS – ACESSO A BLOCOS:* *O serviço de backup empresarial do fornecedor de cloud permite que os utilizadores armazenem e recuperem objetos através de protocolos de blocos, como o protocolo de interface de sistemas de computadores pequenos de Internet (iSCSI)?*
27.	*MIGRAÇÕES – BACKUPS EMPRESARIAIS – ACESSO A BANDAS:* *O serviço de backup empresarial do fornecedor de cloud permite que os utilizadores façam backup dos seus dados através de uma biblioteca de bandas virtuais e que armazenem esses backups em banda na cloud do fornecedor?*
28.	*MIGRAÇÕES – BACKUPS EMPRESARIAIS – ENCRIPTAÇÃO:* *O serviço de backup empresarial do fornecedor de cloud oferece encriptação de dados inativos e em trânsito?*
29.	*MIGRAÇÕES – BACKUPS EMPRESARIAIS – INTEGRAÇÃO DE SOFTWARE DE TERCEIROS:* *O serviço de backup empresarial do fornecedor de cloud integra-se com o software de backup de terceiros utilizado normalmente?*
30.	*MIGRAÇÕES – LIMITES DE SERVIÇO:* *O fornecedor de cloud possui alguma restrição (ou seja, limites de serviço) relativamente à secção de migrações acima?* *Exemplo:* *Número máximo de migrações simultâneas de máquinas virtuais* *Número máximo de solicitações de soluções de transporte de dados*

8. Faturação

	Requisito
1.	*FATURAÇÃO – CONTROLO E RELATÓRIOS:* *O fornecedor de cloud oferece um serviço de acompanhamento e relatórios de faturação para ajudar os utilizadores a gerir e monitorizar a utilização das ofertas de cloud?*
2.	*FATURAÇÃO – ALARMES E NOTIFICAÇÕES:* *O fornecedor de cloud oferece aos utilizadores um mecanismo de configuração de alarmes com notificações para os alertar quando os seus gastos ultrapassarem um limite específico?*
3.	*FATURAÇÃO – GESTÃO DE CUSTOS:* *O fornecedor de cloud oferece um mecanismo para criar e exibir gráficos que resumam 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 numa única conta pagante principal?*
6.	*FATURAÇÃO – LIMITES DE SERVIÇO:* *O fornecedor de cloud possui alguma restrição (ou seja, limites de serviço) relativamente à secção de faturação acima?* *Exemplo:* *Número máximo de contas que podem ser agrupadas* *Número máximo de alarmes que podem ser criados* *Número máximo de orçamentos que podem ser geridos*

9. Gestão

	Requisito
1.	*GESTÃO – SERVIÇO DE MONITORIZAÇÃO:* *O fornecedor de cloud oferece um serviço de monitorização para gerir as aplicações e os recursos de cloud que recolhe, monitoriza e cria um relatório com métricas pré-definidas?*
2.	*GESTÃO – ALARMES:* *O serviço de monitorização do fornecedor de cloud permite que os utilizadores definam alarmes?*
3.	*GESTÃO – MÉTRICAS PERSONALIZADAS:* *O serviço de monitorização do fornecedor de cloud permite que os utilizadores criem e monitorizem métricas personalizadas?*
4.	*GESTÃO – GRANULARIDADE DA MONITORIZAÇÃO:* *O serviço de monitorização do fornecedor de cloud oferece vários níveis de granularidade de monitorização até ao nível de 1 minuto?*
5.	*GESTÃO – SERVIÇO DE CONTROLO DE API:* *O fornecedor de cloud oferece um serviço que regista, monitoriza e armazena atividades em recursos de cloud, tanto ao nível da consola como ao nível da interface de programação da aplicação (API) para uma melhor visibilidade?* • *Em caso afirmativo, quais são os serviços do fornecedor de cloud que se integram com esse serviço de controlo?*
6.	*GESTÃO – NOTIFICAÇÃO:* *O fornecedor de cloud permite a ativação da capacidade de envio de notificações com base nos níveis de atividade da interface de programação da aplicação (API)?*
7.	*GESTÃO – COMPRESSÃO:* *O fornecedor de cloud oferece um mecanismo para comprimir os registos gerados pelo sistema de acompanhamento da interface de programação da aplicação (API), com o objetivo de ajudar os utilizadores a reduzir os custos de armazenamento associados a esse serviço?*
8.	*GESTÃO – AGREGAÇÃO DE REGIÕES:* *O fornecedor de cloud oferece a capacidade de registar a atividade da interface de programação da aplicação (API) da conta em todas as regiões e apresentar essas informações de forma agregada para uma utilização mais fácil?*

9.	*GESTÃO – INVENTÁRIO DE RECURSOS:* *O fornecedor de cloud oferece um serviço para avaliar, auditar e analisar as configurações dos recursos implementados por um utilizador?*
10.	*GESTÃO – ALTERAÇÕES DE CONFIGURAÇÃO:* *O fornecedor de cloud regista automaticamente uma alteração à configuração de um recurso quando a mesma ocorre?*
11.	*GESTÃO – HISTÓRICO DE CONFIGURAÇÕES:* *O fornecedor de cloud oferece a capacidade de analisar a configuração de recursos em qualquer momento exclusivo no passado?*
12.	*GESTÃO – REGRAS DE CONFIGURAÇÃO:* *O fornecedor de cloud oferece diretrizes e recomendações para aprovisionar, configurar e monitorizar continuamente a conformidade?*
13.	*GESTÃO – MODELOS DE RECURSOS:* *O fornecedor de cloud oferece aos utilizadores a capacidade de criar, aprovisionar e gerir um conjunto de recursos através de modelos?*
14.	*GESTÃO – REPLICAÇÃO DE MODELOS DE RECURSOS:* *O fornecedor de cloud oferece a capacidade de replicar rapidamente esses modelos de recursos em diferentes regiões para serem potencialmente utilizados em situações de recuperação de desastres (DR)?*
15.	*GESTÃO – DESIGNER DE MODELOS:* *O fornecedor de cloud oferece uma ferramenta gráfica fácil de utilizar, com funcionalidade de 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, ou seja, servidores, máquinas virtuais, software, bases 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 monitorização dos serviços de cloud?*
18.	*GESTÃO – ACESSO À CLI:* *O fornecedor de cloud oferece uma ferramenta unificada para gerir e configurar vários serviços de cloud a partir da interface da linha de comandos (CLI) e permitir a automatização de tarefas de gestão através da utilização de scripts?*
19.	*GESTÃO – ACESSO MÓVEL:* *O fornecedor de cloud oferece uma aplicação para smartphone para permitir que os utilizadores se liguem ao serviço de cloud e façam a gestão dos seus recursos?* • *Em caso afirmativo, 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 a utilização da cloud em relação às melhores práticas?*

21.	***GESTÃO – LIMITES DE SERVIÇO:*** *O fornecedor de cloud possui alguma restrição (ou seja, limites de serviço) relativamente à secção de gestão acima?* *Exemplo:* *Número máximo de regras de configuração por conta* *Número máximo de alarmes que podem ser criados* *Número máximo de registos 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 a si próprios os recursos/serviços consumidos em diferentes níveis de suporte com base na classificação granular, não forçando os utilizadores a manter contas de cloud separadas para alcançar e receber diferentes níveis de suporte?*
4.	***SUPORTE – FÓRUNS:*** *O fornecedor de cloud oferece fóruns de suporte públicos para que os clientes debatam sobre os seus problemas?*
5.	***SUPORTE – PAINEL DE ESTADO DE INTEGRIDADE DOS SERVIÇOS:*** *O fornecedor de cloud oferece um painel de estado de integridade dos serviços que apresenta as informações mais recentes sobre a disponibilidade dos serviços em várias regiões?*
6.	***SUPORTE – PAINEL PERSONALIZADO:*** *O fornecedor de cloud oferece um painel que apresenta 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 um histórico de 365 dias do painel de estado de integridade do serviço?*
8.	***SUPORTE – CONSULTOR DE CLOUD:*** *O fornecedor de cloud oferece um serviço que atua como um especialista de cloud personalizado e ajuda a comparar a utilização dos recursos em relação às melhores práticas?*
9.	***SUPORTE – TAM:*** *O fornecedor de cloud oferece um Technical Account Manager (gestor de conta técnico – TAM) que fornece conhecimentos técnicos sobre a gama completa de serviços de cloud?*
10.	***SUPORTE – SUPORTE A APLICAÇÕES DE TERCEIROS:*** *O fornecedor de cloud oferece suporte para sistemas operativos comuns e componentes de aplicações comuns em pilha?*
11.	***SUPORTE – API PÚBLICA:*** *O fornecedor de cloud oferece uma interface de programação da aplicação (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 documentação técnica de qualidade e publicamente visível para todos os seus serviços, incluindo, entre outros, guias de utilizador, tutoriais, perguntas frequentes (FAQ) e notas de lançamento?*
13.	*SUPORTE – DOCUMENTAÇÃO DA CLI:* *O fornecedor de cloud oferece documentação técnica de qualidade e publicamente visível sobre a sua interface da linha de comandos (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 de cloud do fornecedor de cloud?*
15.	*SUPORTE – IMPLEMENTAÇÕES DE REFERÊNCIA:* *O fornecedor de cloud oferece um conjunto de documentos online gratuitos com 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.) nas suas ofertas de cloud?*

Apêndice B – Avaliação técnica em tempo real

Ao selecionar um CISP, é importante avaliar as capacidades da plataforma de cloud "em tempo real" com a infraestrutura e os serviços publicamente disponíveis do CISP. Recomendamos pelo menos um dia inteiro de avaliação técnica por CISP pré-selecionado. Durante a avaliação, pode: 1) realizar uma avaliação aprofundada para determinar se as capacidades demonstradas estão alinhadas com os requisitos do seu RFP e as respostas escritas do CISP; 2) fornecer uma plataforma para que os seus especialistas investiguem o CISP de modo a garantirem o alinhamento e o enquadramento com as suas necessidades técnicas e organizacionais específicas e 3) ganhar confiança nos serviços do CISP e na capacidade do CISP de escalar, operar com segurança, operar de forma resiliente e continuar a inovar para satisfazer necessidades futuras.

Quando os CISP respondem aos requisitos de um RFP de serviços de cloud, podem declarar a conformidade com base numa interpretação geral dos requisitos, que não possui o contexto completo das necessidades do ambiente operacional/aplicação de uma organização. Recomendamos a utilização de um painel de avaliação técnica em tempo real com os melhores especialistas técnicos, operacionais, de segurança e de aplicações. Os avaliadores devem pôr à prova o CISP ao longo da avaliação e, como melhor prática, devem pontuar os CISP de forma independente, classificando os cenários numa escala definida, como de 0 a 4 (0 = inaceitável, 1 = mínimo, 2 = aceitável, 3 = bom, 4 = excelente). Posteriormente, as pontuações de demonstração podem ser consolidadas, com a pontuação média para cada cenário de avaliação acumulada na avaliação geral do CISP. Os cenários com um elevado desvio padrão devem ser analisados por uma equipa de avaliação antes da sua finalização. Quando as pontuações forem consolidadas, pode ser feita uma avaliação com base na criticidade dos cenários.

Em termos do âmbito de demonstração, recomendamos que tenha uma visão holística da plataforma do CISP e, em seguida, que a aprofunde para avaliar cargas de trabalho específicas em execução na plataforma. Abaixo encontra-se um resumo de exemplo de uma avaliação de plataforma e carga de trabalho. As organizações podem criar esta base de referência ou personalizá-la para garantir que o CISP selecionado corresponde aos seus requisitos funcionais e não funcionais específicos. Como melhor prática, os fornecedores apresentados com a lista de cenários e requisitos podem propor uma agenda para a avaliação em tempo real que maximize a cobertura e inclua 20% de tempo para perguntas e respostas.

Avaliação da plataforma: vários CISP adotaram o termo "Well Architected" (bem estruturado) para se referirem a uma abordagem de cloud que oferece o valor ideal e minimiza riscos. Os cenários Well Architected numa demonstração técnica em tempo real podem incluir:

1. **Segurança:** identidade, governança centralizada, deteção automatizada de ameaças, proteção de dados, preparação para eventos
2. **Eficácia do desempenho:** dimensionamento correto, escalabilidade/elasticidade, sem servidor
3. **Fiabilidade:** alta disponibilidade (resiliência a falhas), redução do risco de mudança, recuperação de desastres, backup
4. **Gestão de custos:** operações financeiras, otimização comercial, orçamentos e alocação de custos
5. **Excelência operacional:** automatização, monitorização, suporte, gestão e recursos necessários para migrar e operar na cloud

Avaliação das cargas de trabalho: um conjunto comum de tipos de aplicações que podem ser demonstrados e incluem:

- **Aplicação Web:** alojamento público de um site dinâmico, incluindo a base de dados de back-end e armazenamento de objetos estáticos.

- **Análise de dados:** uma arquitetura de data lake ou lake house que permite a consolidação de dados de vários fornecedores e a capacidade de lidar com um alto volume (TB/PB de dados), variedade (estruturado, não estruturado, formatos diferentes, etc.) e velocidade (taxa de produção de dados, alterações e padrões de consulta).
- **Plataforma de ciência de dados:** uma plataforma que permite o desenvolvimento, implementação e utilização de recursos baseados em IA/ML em toda a sua organização.
- **Aplicação IoT:** uma plataforma/capacidade de IoT que abrange a cloud, uma capacidade de rede e os dispositivos.

Para cada carga de trabalho representativa que seja importante para a sua organização, pode definir os cenários a serem demonstrados pelo CISP. Os cenários devem demonstrar as capacidades gerais que permitem a implementação da carga de trabalho de forma bem estruturada. As páginas seguintes incluem exemplos de critérios de avaliação técnica em tempo real para: 1) a plataforma do CISP e 2) um exemplo de carga de trabalho de aplicação Web.

Plataforma: exemplo de avaliação técnica em tempo real

ID do cenário	Nome do cenário	Criticidade (1 = baixo, 4 = crítico)	Requisitos de demonstração	Considerações sobre a pontuação
Plat.Sec.1	Federação de identidades	4	Demonstrar a capacidade de federar de um armazenamento de identidades para um serviço de cloud.	• Suporte para protocolos padrão, como o SAML. • Suporte para a replicação de identidade baseada em SCIM. • Capacidade de definir diferentes níveis de acesso no armazenamento de identidades empresarial e aplicá-los no fornecedor da cloud. • Capacidade de limitar equipas/indivíduos específicos para contas/cargas/projetos específicos. • Capacidade de suportar o controlo de acesso baseado em atributos (ABAC) e utilizar esses atributos no sistema de Identity and Access Management (IAM) do fornecedor de cloud para aceder aos recursos de cloud.
Plat.Sec.2	Governança central	4	Demonstrar a capacidade de definir centralmente políticas e requisitos a um nível organizacional (políticas globais) e a um nível de unidade e projeto.	• A política deve incluir: ativar/desativar serviços, aplicar restrições geográficas (limitar regiões). • As políticas também devem restringir utilizadores, incluindo administradores, de desativar quaisquer controlos de auditoria/governança.
Plat.Sec.3	Limitação da permissão do utilizador	3	Demonstrar as recomendações automáticas para restringir permissões de utilizadores.	• Capacidade de comparar as permissões atuais com as permissões exigidas. • Geração automática de políticas para promover privilégios mínimos.

ID do cenário	Nome do cenário	Criticidade (1 = baixo, 4 = crítico)	Requisitos de demonstração	Considerações sobre a pontuação
Plat.Sec.4	Registo de auditoria	4	Demonstrar o registo de auditoria da atividade na cloud, incluindo ações permitidas e proibidas.	• Registos centralizados para toda a organização. • Registos específicos para uma conta ou um projeto para suportar controlos e responsabilidade básicos. • Ferramentas para permitir a consulta de registos. • Ferramentas que permitem o acionamento de ações baseadas em entradas de registos/eventos específicos. • Capacidade de ver a atividade de suporte do fornecedor. • Capacidade de prevenir a eliminação de registos, mesmo por administradores.
Plat.Sec.5	Isolamento da rede	4	Demonstrar e provar quando possível o isolamento de diferentes inquilinos na cloud. Demonstrar a configuração de sub-redes isoladas (sem conectividade), privadas (sem Internet) e públicas (com acesso à Internet).	• Separação de inquilinos, incluindo em serviços de VPN e ligação cruzada. • Capacidade de controlar o fluxo de tráfego da infraestrutura de cloud (no local) fora e dentro da mesma e para a Internet. • Como a separação é aplicável ao utilizar serviços partilhados, como alojamento de contentores ou função como serviço.
Plat.Sec.6	Encriptação de dados inativos	4	Demonstrar a capacidade de encriptar dados inativos, incluindo as opções para BYOK e encriptação do lado do cliente.	• Capacidade de solicitar encriptação para dados sensíveis. • Capacidade de utilizar chaves geridas do fornecedor ou chaves geridas do cliente. • Aderência ao FIPS 140-2. • Capacidade de alertar e registar o incumprimento dos requisitos de encriptação. • Custo de impacto adicional. • Impacto no desempenho. • Suporte para tamanhos de chave e algoritmos com segurança quântica.
Plat.Sec.7	Encriptação de dados em trânsito	4	Demonstrar a capacidade de encriptar dados em trânsito.	• Encriptação por predefinição para API de serviço. • Capacidade de ativar a encriptação em trânsito (TLS) em balanceadores de carga e API geridas. • Suporte para a autenticação mútua (cliente e servidor).

ID do cenário	Nome do cenário	Criticidade (1 = baixo, 4 = crítico)	Requisitos de demonstração	Considerações sobre a pontuação
Plat.Sec.8	Gestão de chaves	4	Demonstrar a sua capacidade de gestão de chaves. Incluir o ciclo de vida de chaves completo. Incluir a integração com serviços de cloud.	• Registo da criação, utilização, rotação e destruição de chaves.
Plat.Sec.9	Gestão de configuração	3	Demonstrar a sua capacidade de gestão de configuração da plataforma de cloud.	• Manter um CMDB preciso. • Verificar a conformidade. • Ativar automaticamente ações baseadas no incumprimento. • Capacidade de avaliar alterações de configuração relativamente às melhores práticas ou regras personalizadas.
Plat.Sec.10	Segurança de rede	3	Demonstrar a capacidade da firewall e firewall de aplicações Web, incluindo a integração com conjuntos de regras de terceiros/firewalls e a proteção contra ataques volumétricos.	• Capacidades de WAF (firewall de aplicações Web): escalabilidade. • Suporte de redes privadas e públicas. • Capacidade de cumprir o conjunto de regras do setor/fornecedor. • Acionar automaticamente ações dentro da infraestrutura em função dos eventos de WAF. • Capacidades de firewall, escalabilidade. • Firewalls baseadas em anfitriões e redes. • Capacidade de referenciar objetos ou grupos lógicos, bem como a capacidade de especificar bloqueios de IP CIDR. • Número de regras suportadas em cada nível/componente. • Capacidade de suportar um modelo operacional distribuído (equipa de rede + equipa de programadores) através de configurações de políticas e redes.

ID do cenário	Nome do cenário	Criticidade (1 = baixo, 4 = crítico)	Requisitos de demonstração	Considerações sobre a pontuação
Plat.Sec.11	Conectividade de rede	3	Demonstrar a capacidade de ligar a redes no local, bem como pontos finais/clientes, a redes privadas na cloud.	• Conectividade privada (grande largura de banda > 10 GB). • Capacidade de controlar políticas de encaminhamento e firewall por toda a organização. • Conectividade de VPN (site a site e baseada no cliente). • Suporte de IPV6.
Plat.Sec.12	Gestão de instâncias	3	Demonstrar as capacidades de gestão de instâncias.	• Capacidade de monitorizar e gerir o estado dos patches de um grande volume de instâncias. • Suporte para a gestão de patches dos sistemas operativos Linux e Windows. • Capacidade de executar comandos numa frota de servidores sem a necessidade de SSH. • Capacidade de controlar e auditar o acesso remoto a máquinas virtuais de forma centralizada. • Capacidade de alterar o tamanho de uma instância, anexar volumes adicionas, alterar configurações de rede, etc. através da consola, CLI e API.
Plat.Sec.13	Aplicação de políticas	3	Demonstrar a capacidade de configurar serviços para impedir acessos a partir da rede pública.	• Capacidade de isolar tráfego em redes privadas para serviços que possam conter dados críticos/confidenciais. • Capacidade de definir políticas que controlem o acesso a dados baseados na rede de origem. • Aplicação destas restrições de acesso a todos os utilizadores, incluindo utilizadores com credenciais de alto nível.
Plat.Sec.14	Análise de vulnerabilidades	2	Demonstrar a capacidade de analisar imagens (contentor ou máquina virtual) relativamente a vulnerabilidades.	• Capacidade de examinar contentores num registo. • Capacidade de examinar máquinas virtuais relativamente a vulnerabilidades conhecidas. • Capacidade de efetuar uma análise de rede.

ID do cenário	Nome do cenário	Criticidade (1 = baixo, 4 = crítico)	Requisitos de demonstração	Considerações sobre a pontuação
Plat.Sec.15	Inspeção de rede	2	Demonstrar a capacidade de capturar/espelhar tráfego de rede (NetFlow e pacotes completos) do ambiente de um cliente.	• Capacidade de espelhar algum/todo o tráfego na infraestrutura do fornecedor de cloud (da perspetiva do inquilino cliente), incluindo a captura de pacotes completos. • Capacidade de simplesmente selecionar o tráfego que pretende capturar. • Capacidade de escalar para volumes de tráfego muito elevados (>50 GBps).
Plat.Sec.16	Deteção de ameaças	3	Demonstrar a capacidade de deteção de intrusões na sua plataforma, incluindo ameaças de uma rede, utilização de credenciais e análise de padrões de utilização por exemplo.	• Capacidade de detetar atividades suspeitas como "mining". • Capacidade de detetar ataques de autenticação de força bruta, como início de sessão SSH. • Capacidade de detetar fugas ou abusos de credenciais. • Aplicação de ML, com a análise de grandes números de eventos e apresentação de eventos priorizados. • Esforço para ativar/configurar (quanto mais simples melhor). • Capacidade de integração com serviços externos e acionamento de notificações. • Capacidade de configurar o IDS a um nível global para todos os projetos/contas.
Plat.Perf.1	Otimização de computação	2	Demonstrar recomendações automáticas para a otimização de custos da máquina virtual e função como serviço.	• Recomendações baseadas na utilização atual e padrões de cargas de trabalho. • As recomendações incluem poupanças estimadas e informações acerca do nível de carga previsto e implicações técnicas. • As otimizações devem incluir tanto as poupanças como o "risco de desempenho", por exemplo, quando as máquinas virtuais podem ser demasiado pequenas.
Plat.Perf.2	Otimização do ambiente	2	Demonstrar recomendações automáticas para outros componentes de cloud, como balanceadores de carga, redes, bases de dados, armazenamento, etc.	• As recomendações identificam poupanças e potenciais oportunidades de eficiência de otimização noutros componentes para lá da computação de base.

ID do cenário	Nome do cenário	Criticidade (1 = baixo, 4 = crítico)	Requisitos de demonstração	Considerações sobre a pontuação
Plat.Perf.3	Escalabilidade automática de computação	4	Demonstrar as capacidades de escalabilidade automática de uma aplicação implementada atrás de um balanceador de carga num ambiente de computação virtual. Demonstrar as diferentes opções/abordagens e a capacidade de acionar outras ações (opcionais) antes/depois de eventos de escalabilidade, como uma notificação.	• Diferentes opções para escalar abordagens, baseadas em acionadores, baseadas em tempo, manuais ou mais inteligentes que aplicam machine learning para prever a capacidade necessária. • Escalabilidade totalmente automática, incluindo registo com um balanceador de carga e verificações de integridade. • A capacidade de executar uma porção de código aleatório em pontos específicos do ciclo de vida de escalabilidade.
Plat.Perf.4	Escalabilidade online de armazenamento	3	Demonstrar a capacidade de escalar tanto a capacidade como a produtividade de um armazenamento em bloco sem interrupções para a carga de trabalho.	• Capacidade de transferir armazenamento em bloco entre diferentes tipos de armazenamento sem precisar de reconstruir serviços totalmente. • Capacidade de aumentar o tamanho dos volumes apresentados às máquinas virtuais.
Plat.Perf.5	Serviços geridos de escalabilidade automática	3	Demonstrar a capacidade da base de dados NoSQL, depósito de objetos, API Gateway e plataforma FaaS para escalar de alguns utilizadores (dezenas) para muitos (milhares).	• Escalabilidade automática fluída e idealmente sem intervenção do administrador. • Desempenho consistente durante um período contínuo de aumento de escala vertical que se alinha com os requisitos de escalabilidade de produção. • Para alguns componentes, como FaaS, devem analisar-se as opções de preparação e gestão de limites de execução simultânea se necessário.
Plat.Perf.6	Cargas de trabalho baseadas em contentores	3	Demonstrar a capacidade de alojar cargas de trabalho baseadas em contentores.	• Opções para plataformas de alojamento de contentores. • Integração com outros componentes IaaS, como balanceadores de carga. • Disponibilidade para uma solução mesh de serviço. • Opções não proprietárias para alojamento de contentores, como Kubernetes. • Suporte nativo para alta disponibilidade dentro do plano de controlo de contentores. • Capacidade de gerir anfitriões de contentores no local.

ID do cenário	Nome do cenário	Criticidade (1 = baixo, 4 = crítico)	Requisitos de demonstração	Considerações sobre a pontuação
Plat.Rel.1	Resiliência regional	4	Demonstrar o failover automático de uma instância de base de dados relacional numa região quando uma falha localizada geograficamente (como uma falha energética) é simulada.	• Failover automatizado. • Zonas de falha isoladas numa região de cloud. • Delimitação clara e arquitetura simples para oferecer uma alta disponibilidade.
Plat.Rel.2	Recuperação automática de instâncias	2	Demonstrar a autorrecuperação de uma instância/conjunto de instâncias no seguimento de uma verificação de integridade falhada.	• Verificações de integridade configuráveis. • Recuperação/reaprovisionamento de instâncias completamente automático.
Plat.Rel.3	Conhecimento da integridade do balanceador de carga	3	Demonstrar como um balanceador de carga automático deteta uma instância defeituosa e encaminha o tráfego para outros anfitriões em bom estado.	• Verificações de integridade configuráveis. • Encaminhamento automático de tráfego para anfitriões em bom estado.
Plat.Rel.4	Failover regional	3	Demonstrar uma arquitetura multirregional, incluindo uma mudança de tráfego automática para uma região secundária.	• Verificações de integridade conhecidas a nível global. • Opções de encaminhamento automatizado: latência, ponderação e transferência. • Suporte para cargas de trabalho de máquina virtual, bem como serviços geridos como um serviço de base de dados NoSQL/depósito de objetos.
Plat.Rel.5	Backup e recuperação	4	Demonstrar as opções de backup e recuperação para: máquinas virtuais, bases de dados e serviços geridos.	• Nível de automatização. • Capacidade de restaurar para a mesma/outra região de cloud. • Capacidade de copiar backups para outra região de cloud.

ID do cenário	Nome do cenário	Criticidade (1 = baixo, 4 = crítico)	Requisitos de demonstração	Considerações sobre a pontuação
Plat.Cost.1	Orçamentos	3	Demonstrar uma capacidade de gestão de orçamentos, incluindo como os estruturar para subcontas e projetos.	• Considerar a capacidade de implementar controlos orçamentais e de monitorização a diferentes níveis na sua organização. • Verificar a flexibilidade, por exemplo a capacidade de agrupar componentes (através de etiquetas), definir orçamentos para serviços de cloud específicos e configurar limites de alerta/monitorização.
Plat.Cost.2	Alocação do orçamento	1	Demonstrar o aprovisionamento de um novo ambiente de projeto (conta), incluindo o processo de alocação de orçamento para o projeto. O aprovisionamento deve incluir passos de aprovação manual para: 1) avaliação técnica/TI e 2) avaliação comercial/financeira.	• A capacidade de aprovisionamento de forma autónoma, com as aprovações necessárias. • Automatização da configuração de definição orçamental, notificações ou políticas de orçamentação apropriadas para a sua organização.
Plat.Cost.3	Relatórios de orçamentos	2	Demonstrar a capacidade de informar toda a organização sobre relatórios de orçamentos. Elaborar relatórios para um departamento específico vs. toda a organização (em função de quem precisa de ser informado) Os relatórios devem incluir valores de despesa "reais" e estimados.	• A capacidade de fornecer visibilidade a diferentes níveis da organização, obtendo conhecimento e transparência, mas em função de quem precisa de ser informado. • As previsões devem ser baseadas em tendências atuais e anteriores e devem fornecer um pré-aviso no caso de os orçamentos poderem ser excedidos.
Plat.Cost.4	Controlos orçamentais	1	Demonstrar a capacidade de tomar medidas quando o limite orçamental for atingido. As ações devem incluir notificações, aplicação de limites ou intervenção ativa para impedir que os orçamentos sejam excedidos.	• A capacidade de definir ações para diferentes projetos de forma simples. • A capacidade de as ações variarem de um projeto para o outro, por exemplo, considerando implicações de desenvolvimento vs. de produção. • A capacidade de definir várias ações e limites para o mesmo orçamento/projeto. • A capacidade de definir ações personalizadas para além das capacidades padrão.

ID do cenário	Nome do cenário	Criticidade (1 = baixo, 4 = crítico)	Requisitos de demonstração	Considerações sobre a pontuação
Plat.Cost.5	Periodicidade do orçamento	1	Demonstrar a capacidade de aplicar orçamentos para diferentes períodos de tempo: diariamente/mensalmente/ anualmente, etc. Para orçamentos anuais: demonstrar a capacidade de aplicar uma distribuição variável de despesas previstas durante o ano.	• Capacidade de definir orçamentos para diferentes períodos de tempo. • Capacidade de configurar a distribuição de despesas ao longo de todo o ano para orçamentos anuais. Isto é principalmente importante para cargas de trabalho sazonais/altamente elásticas, como a declaração de impostos anual.
Plat.Cost.6	Mercado de terceiros	3	Demonstrar a capacidade de adquirir e implementar produtos de terceiros. Demonstrar como definir um orçamento para um conjunto de produtos de terceiros disponíveis num marketplace e também a capacidade de restringir determinados produtos.	• Capacidade de definir um orçamento para um produto específico, um orçamento global, um orçamento para um conjunto de projetos/contas. • Capacidade de apresentar apenas um subconjunto do marketplace mais amplo aos utilizadores de cloud.
Plat.Cost.7	Modelos de preços de computação	3	Demonstrar os diferentes modelos de preços/comerciais que podem ser aplicados a máquinas virtuais.	• As capacidades devem incluir preços a pedido, detalhados (por minuto/hora) e sem necessidade de compromisso a longo prazo. • Compromissos a longo prazo opcionais em troca de um desconto. • Capacidade de adquirir instâncias com um desconto se estiverem dispostos a que existam interrupções. • Além disso, deve ser possível combinar estes modelos dentro do mesmo projeto/contas e partilhar os benefícios em diferentes contas.
Plat.Cost.8	Recomendações de otimização comercial	3	Demonstrar a capacidade de receber recomendações de otimização comercial para otimizar gastos (sem precisar de fazer nenhuma alteração técnica).	• Recomendações holísticas para múltiplos serviços, incluindo máquinas virtuais e bases de dados geridas. • Capacidade de recomendar ações simples e compreender as poupanças/benefícios projetados.
Plat.Cost.9	Anfitriões dedicados	4	Demonstrar a capacidade de aprovisionar um anfitrião dedicado para permitir a utilização de licenças on-premises que estejam associadas a um anfitrião específico.	• Facilidade de aprovisionamento. • Capacidade de gerir a utilização do anfitrião. • Capacidade de partilhar o anfitrião em diferentes projetos/locações.

ID do cenário	Nome do cenário	Criticidade (1 = baixo, 4 = crítico)	Requisitos de demonstração	Considerações sobre a pontuação
Plat.Ops.1	Migração de máquinas virtuais	3	Demonstrar a importação de uma máquina virtual on-premises para um serviço de máquina virtual baseado na cloud.	• Capacidade de importar sistemas operativos baseados em Windows e Linux. • Capacidade de importar várias máquinas em simultâneo. • Capacidade de manter uma sessão de replicação para permitir um rápido failover para a cloud.
Plat.Ops.2	Capacidades de DevOps e automatização	4	Demonstrar as suas capacidades de DevOps/automatização, incluindo como os ambientes estão definidos em código, suporte de implementações totalmente automáticas, testes automáticos e reversões.	• Capacidade de definir todos os componentes de sistema em código, incluindo a rede, máquinas virtuais, armazenamento e bases de dados. • Capacidade de criar um pipeline. • Capacidade de criar um repositório de código. • Capacidade de automatizar versões. • Capacidade de efetuar implementações azuis/verdes. • Capacidade de criar múltiplos ambientes e ter várias etapas de implementação. • Reversão automática para implementações falhadas.
Plat.Ops.3	Alojamento de aplicações	2	Demonstrar o alojamento de uma simples aplicação de 2.º nível num serviço de plataforma que necessite de poucos conhecimentos de código. Incluir uma base de dados relacional e escalabilidade automática para o nível de aplicação/Web.	• Configuração simples através da interface de utilizador. • Inclusão de verificações de integridade, escalabilidade e alta disponibilidade. Suporte de plataforma, Windows e Linux.
Plat.Ops.4	Integração de segurança	2	Demonstrar as capacidades de integração da sua plataforma de uma perspetiva de incidentes de segurança e gestão de eventos.	• Capacidade de facilmente integrar e consumir registos relacionados com segurança do fornecedor de cloud + API para integração.
Plat.Ops.5	Integração de ITSM	3	Demonstrar as capacidades de integração da sua plataforma de uma perspetiva de ITSM (serviço de gestão de TI).	• Capacidade de criar, monitorizar e atualizar um caso de suporte através de uma API. • Capacidade de aprovisionar serviços ou conjuntos de serviços como “produtos” através de uma API.

ID do cenário	Nome do cenário	Criticidade (1 = baixo, 4 = crítico)	Requisitos de demonstração	Considerações sobre a pontuação
Plat.Ops.6	Suporte	4	Demonstrar a sua oferta de suporte.	• Diferentes níveis de suporte para diferentes tipos de carga de trabalho. • Capacidade de suportar também o sistema operativo/motor de base de dados, etc., conforme apropriado, para um determinado serviço. • Capacidade de oferecer uma oferta diferenciada com líderes de suporte designados para cargas de trabalho críticas. • Capacidade de oferecer um processo estruturado de preparação de eventos e revisão da arquitetura. • Informações sobre o plano de desenvolvimento do fornecedor.
Plat.Ops.7	Auditabilidade	4	Demonstrar as ferramentas que tem para suportar as auditorias de conformidade.	• Capacidade de obter detalhes das auditorias de conformidade através da consola. • Capacidade de gerir e automatizar auditorias de ambiente.
Plat.Ops.8	Máquina virtual para contentor	1	Demonstrar a conversão de uma aplicação numa máquina virtual para um contentor e entregá-la com a plataforma de contentores do fornecedor da cloud.	• Utilização simples da conversão. • Tempo para converter. • Suporte de plataforma, .Net e Java.

Carga de trabalho: aplicação Web – exemplo de avaliação técnica em tempo real

A secção seguinte fornece um exemplo de folha de avaliação de carga de trabalho para uma carga de trabalho "aplicação Web" específica. Ao desenvolver uma folha de avaliação para uma determinada aplicação, é vivamente recomendado que sejam envolvidos os utilizadores, programadores e administradores da aplicação, porque estes terão uma melhor compreensão dos requisitos, desafios atuais e entraves.

ID do cenário	Nome do cenário	Criticidade (1 = baixo, 4 = crítico)	Requisitos de demonstração	Considerações sobre a pontuação
Web.Sec.1	Segurança: proteção da aplicação	3	Demonstrar a sua capacidade de bloquear tentativas maliciosas de explorar a aplicação através de uma injeção SQL, ataque de scripts XSS e outros ataques.	• Capacidade de proteger contra ataques comuns "criativos" com regras/capacidades padrão. • Capacidade de criar verificações/regras/funções personalizadas.
Web.Sec.2	Segurança: proteção baseada em avaliação	3	Demonstrar a sua capacidade de bloquear/proteger contra ataques que envolvam um grande número de pedidos ou volumes de dados direcionados a uma aplicação.	• Capacidade de configurar limites e restringir taxas de pedidos a partir de um endereço IP ou lista de endereços específicos.
Web.Sec.3	Segurança: proteção baseada na fonte	3	Demonstrar a capacidade de restringir o acesso com base numa origem de rede/geográfica.	• Capacidade de restringir por bloco de rede ou lista de blocos de rede. • Capacidade de restringir por país de origem (sem ter de gerir listas de IP).
Web.Sec.4	Segurança: segmentação de rede	4	Demonstrar a capacidade de isolar/proteger componentes (servidor Web, servidor da aplicação/ servidor DB) para proteger contra uma propagação norte-sul e este-oeste na infraestrutura.	• Capacidade de implementar componentes em diferentes sub-redes e controlar o fluxo de tráfego entre diferentes sub-redes. • Capacidade de controlar o fluxo de tráfego a um nível de interface de rede. • Capacidade de referenciar grupos lógicos e blocos CIDR.
Web.Sec.5	Segurança: suporte TLS e gestão de certificados	4	Demonstrar a capacidade de fornecer um ponto final protegido por TLS e gerir automaticamente os componentes de suporte para o poder fornecer, por exemplo, a rotação automática de certificados.	• Suporte para os protocolos TLS mais recentes e capacidade de desativar versões herdades se necessário. • Criação, gestão e rotação simples de certificados (idealmente completamente automática).

ID do cenário	Nome do cenário	Criticidade (1 = baixo, 4 = crítico)	Requisitos de demonstração	Considerações sobre a pontuação
Web.Perf.1	Desempenho: escalabilidade	4	Demonstrar a sua capacidade de escalar de 10 para 100 000 utilizadores simultâneos numa aplicação Web através de escalabilidade automática dinâmica.	• Capacidade de definir regras de escalabilidade baseadas em tempo e acionadores. • Escalabilidade fluída para o utilizador final e administrador. Aumentar a escala horizontalmente quando a carga aumenta e reduzir a escala horizontalmente quando a carga diminui de forma automática. • Assegurar que a escalabilidade existe em cada camada da aplicação Web (balanceador de carga, camada de Web, camada de dados, etc.). • A disponibilidade de colocar serviços em cache em diferentes camadas da aplicação conforme adequado.
Web.Perf.2	Desempenho: entrega global	3	Demonstrar a sua capacidade de CDN, incluindo a demonstração da latência desde diferentes pontos do mundo, incluindo: Austrália, Ásia, África, Médio Oriente, América do Norte, América do Sul e Europa.	• Capacidade de criar e configurar um CDN através de uma consola de CISP/API. • Regras de distribuição configuráveis para diferentes áreas geográficas. • Colocação em cache configurável para diferentes casos de utilização/aplicações.
Web.Rel.1	Fiabilidade: resiliência de região única	4	Demonstrar a capacidade de tolerar um evento localizado, como uma perda de conectividade de rede ao datacenter do CISP.	• Failover automático e uma alta disponibilidade numa região cloud (cidade).
Web.Rel.2	Fiabilidade: implementação multirregião	3	Demonstrar uma implementação multirregião de uma aplicação Web incluindo uma base de dados globalmente replicada.	• Capacidade de implementar uma aplicação multirregião de forma programática. • Replicação entre regiões para o armazenamento de dados. • Encaminhamento automático de utilizadores para a sua melhor região.
Web.Rel.3	Fiabilidade: transferência multirregião	3	Demonstrar o failover automático de uma aplicação Web no caso de ocorrer um problema de serviço que afete toda a região.	• Failover automático e alta disponibilidade em várias regiões de cloud.

ID do cenário	Nome do cenário	Criticidade (1 = baixo, 4 = crítico)	Requisitos de demonstração	Considerações sobre a pontuação
Web.Cost.1	Custo: visibilidade	2	Demonstrar a capacidade controlar o custo por aplicação.	• Capacidade de observar o histórico de custos para uma aplicação específica, incluindo quando escala verticalmente/horizontalmente.
Web.Cost.2	Custo: orçamentos	2	Demonstrar a capacidade de definir orçamentos e alertas relacionados por aplicação.	• Orçamentos configurados por aplicação e a capacidade de acionar alertas/ações com base nos limites configurados.
Web.Ops.1	Operações: janelas de manutenção	3	Demonstrar a capacidade de configurar janelas de manutenção para alinhar com requisitos empresariais, principalmente quando a manutenção pode afetar a disponibilidade da aplicação.	• Janelas de manutenção configuráveis para componentes como um serviço de base de dados relacional.
Web.Ops.2	Operações: registos	3	Demonstrar a capacidade de centralizar os registos para uma aplicação com múltiplos componentes, incluindo persistência de registos após o fim ou falha das máquinas virtuais.	• Capacidade de configurar um serviço de registo centralizado que ser escalado com os requisitos da aplicação. • Capacidade de definir regras/filtros para acionar alertas ou ações com base em eventos de registo específicos.
Web.Ops.3	Operações: monitorização	3	Demonstrar a monitorização da aplicação, incluindo desempenho, disponibilidade, tempo de resposta, contagens de erros, entre outros, e da funcionalidade para tomar medidas/acionar notificações com base em limites de diferentes métricas.	• Uma coleção de métricas padrão disponíveis, como E/S de disco, CPU, métricas de bases de dados, rede, balanceador de carga, etc. • Capacidade de definir métricas e limites personalizados. • Capacidade de criar um painel personalizado para representar as métricas mais importantes e partilhar esses painéis com os utilizadores relevantes.