PROCESSO Nº 8.2019.0211/000052-6

CADERNO DE ESPECIFICAÇÕES TÉCNICAS

1. DEFINIÇÕES GERAIS

1.1. PRINCIPAIS TERMOS EMPREGADOS NA ESPECIFICAÇÃO TÉCNICA

1.1.1. "Bare-metal Server": consiste em servidor físico sem virtualização.

1.1.2. "Cloud Broker ": consiste em corretor de serviços de nuvem que desempenha papel similar a um corretor de imóvel ou de investimento apoiando o cliente na intermediação de serviços especializados. Um "cloud broker" é uma empresa ou pessoa física, especialista em "cloud computing", que vai atuar junto ao provedor, em nome do consumidor. Normalmente esse tipo de empresa possui um certo grau de relacionamento negocial com o provedor de serviços de computação em nuvem, o que supostamente pode reduzir o custo dos serviços contratados, além de oferecer gerenciamento e otimização do ambiente e suporte aos usuários. A grande vantagem desse modelo de contratação reside na "nacionalização" dos serviços contratados, ou seja, a empresa contratada estará encarregada de recolher e pagar todos os impostos e o provedor em moeda estrangeira, desonerando o contratante de tais atividades.

1.1.3. Computação em Nuvem: consiste em modelo de entrega de recursos computacionais que permite acesso ubíquo e sob demanda, através da rede mundial de computadores, a um conjunto compartilhado de recursos computacionais configuráveis (por exemplo: redes, servidores, armazenamento, aplicações e serviços), que podem ser rapidamente provisionados e disponibilizados com o mínimo de esforço de gerenciamento ou de interação com o provedor de serviços.

1.1.4. "Compute Instance" (ou instância computacional): consistem em VM ou "bare-metal server", dependendo dos dispositivos de computação ofertados pelos provedores.

1.1.5. "Container": um *container* (usualmente baseado na plataforma Docker ou equivalente) que roda em um contexto dedicado no ambiente de um sistema operacional.

1.1.6. *Datacenter* Físico: ambiente projetado para abrigar servidores e outros componentes como sistemas de armazenamento de dados (*storages*) e ativos de rede (*switches*, roteadores). Seu objetivo principal é garantir a disponibilidade e a proteção de equipamentos que rodam os sistemas de negócio de uma organização, garantindo a continuidade do negócio e sustentando os ambientes, equipamentos, *softwares* e serviços contratados. O *datacenter* deve prover conexões (*links*) redundantes, mecanismos de segurança (física e lógica), sistemas redundantes de geração de

energia elétrica, sistema de prevenção contra incêndios e refrigeração adequada para operação dos servidores e demais equipamentos.

1.1.7. *Datacenter* Lógico: pode consistir em um único *datacenter* físico, a uma sala dentro de um *datacenter* físico ou um conjunto de *datacenters* físicos dentro da mesma área ou proximidade. As edificações podem compartilhar energia, água, climatização e telecomunicações.

1.1.8. DNS ("Domain Name System"): sistema computacional usado para atribuir nomes a serviços de rede e computadores, organizado de acordo com uma hierarquia de domínios. A atribuição de nomes de DNS é utilizada em redes TCP/IP para localizar computadores e serviços através de nomes amigáveis ao usuário.

1.1.9. Elasticidade: permite aumentar ou reduzir de forma simples e dinâmica, sem interrupções e em tempo de execução, a quantidade de recursos computacionais utilizados, suprindo, desta forma, momentos de picos de demanda.

1.1.10. *Firewall*: dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado conjunto de hosts em operação na rede, podendo ser do tipo filtro de pacotes, *proxy* de aplicações, etc. O *firewall* existe na forma de *software* e de *hardware*, senod que a combinação de ambos normalmente é chamada de "appliance".

1.1.11. Infraestrutura como Serviço (IaaS): é o provisionamento pelo fornecedor de serviços em nuvem de processamento, armazenamento, comunicação de rede e outros recursos fundamentais de computação nos quais o cliente pode instalar e executar *softwares* em geral, incluindo sistemas operacionais e aplicativos. O cliente não gerencia nem controla a infraestrutura subjacente da nuvem, mas tem controle sobre o espaço de armazenamento e aplicativos instalados, e possivelmente um controle limitado de alguns componentes de rede.

1.1.12. IOPS ("Input/Output Operations per Second"): é uma unidade padrão para fins de avaliação de desempenho de discos e outros dispositivos de armazenamento de dados.

1.1.13. IP: identificação de um dispositivo (computador, impressora, etc) em uma rede local ou pública. Cada computador na Internet possui um identificador IP ("Internet Protocol") único, que é o meio pelo qual as máquinas usam para se comunicarem entre si.

1.1.14. Latência: em uma rede de computadores, a latência, também conhecida como atraso, representa a expressão do tempo necessário para um pacote de dados ir de um ponto para outro. Em outras palavras, é a referência a qualquer atraso ou espera que aumente o tempo de resposta real ou percebido além do tempo de resposta desejado. Em alguns casos, a latência é medida enviando-se um pacote, que é devolvido ao remetente e o tempo completo desse percurso é considerado como latência.

1.1.15. Nuvem Híbrida: este tipo de solução em nuvem é uma composição de 2 (duas) infraestruturas de nuvem (privada e pública), interligadas por tecnologias apropriadas que permitem portabilidade de aplicações e de dados entre as nuvens. É possível utilizar essa abordagem para valer-se dos principais benefícios dos modelos público (elasticidade devido ao consumo de recursos compartihados) e privado (desempenho garantido devido ao consumo de recursos dedicados), e ao mesmo tempo, minimizar os riscos e otimizar os custos advindos de cada modelo, sempre que existirem necessidades distintas associadas a determinados tipos de usuários ou de dados.

1.1.16. Nuvem Privada: a infraestrutura de nuvem privada que está alocada para uso exclusivo de um único cliente. Sua utilização, gerenciamento e operação podem ser feitos pelo cliente e/ou terceirizada, em suas dependências e/ou no provedor. Todavia, a nuvem privada tem flexibilidade reduzida.

1.1.17. Nuvem Pública: é uma infraestrutura de nuvem que está disponível para uso público e que reside nas instalações do provedor. Pode ser da própria organização ou operada por terceiros, ou uma combinação. A infraestrutura física é compartilhada. No entanto, há uma separação lógica por cliente. Os recursos computacionais são baseados em virtualização, agrupados e compartilhados entre clientes, e acessados via rede mundial de computadores ou conexão de rede dedicada. O uso dos recursos é monitorado e pago conforme o uso.

1.1.18. Plataforma como Serviço (PaaS): consiste na capacidade fornecida ao cliente para provisionar na infraestrutura de nuvem aplicações adquiridas ou criadas para o cliente, desenvolvidas com linguagens de programação, bibliotecas, serviços e ferramentas suportados pelo provedor de serviços em nuvem. O cliente não gerencia nem controla a infraestrutura de nuvem subjacente incluindo rede, servidores, sistema operacional ou armazenamento, mas tem controle sobre as aplicações instaladas e possivelmente sobre as configurações do ambiente de hospedagem de aplicações.

1.1.19. Portabilidade: capacidade que permite que aplicações e dados operem em qualquer modelo de nuvem, ofertados por fornecedores distintos, sem a necessidade de reescrever códigos de aplicações, converter bancos de dados, alimentar os sistemas com informações dos usuários ou mesmo alterar características das aplicações.

1.1.20. Provedor de Serviços em Nuvem: empresa que possui infraestrutura de tecnologia da informação e comunicação (TIC) destinada ao fornecimento de infraestrutura, plataformas e aplicativos baseados em computação em nuvem.

1.1.21. Rede Privativa: consiste em uma rede virtual que é totalmente isolada e não é externamente roteável. Tal construto usa a RFC 1918 para designar blocos de endereços IP privativos. Um serviço em nuvem que suporta redes privativas deve permitir instâncias computacionais que possuem apenas endereços IP privativos em

uma rede privada se comunicar entre si. Todavia, usualmente provedores de serviços em nuvem suportam o acesso às redes privativas por meio de *gateway* que fornece roteamento seguro para a rede pública.

1.1.22. Região: consiste em um agrupamento de *datacenters* lógicos e físicos localizados dentro de uma área geográfica. Sendo usual uma região consistir de um ou mais *datacenters* físicos.

1.1.23. Software como Serviço (SaaS): são as aplicações do fornecedor executadas em uma infraestrutura de nuvem, disponíveis ao consumidor. As aplicações podem ser acessadas por vários dispositivos clientes, tais como um navegador web ou um software cliente. O consumidor não gerencia nem controla a infraestrutura da nuvem associada ao serviço, incluindo rede, servidores, sistemas operacionais, armazenamento, ou mesmo recursos individuais da aplicação.

1.1.24. "Throughput": é uma unidade padrão que referencia a vazão de dados transferidos em discos, sistemas de armazenamento ou redes de dados e pode ser traduzido como a taxa de transferência efetiva de um sistema.

1.1.25. vCPU ("virtual" CPU): trata-se da CPU ("Central Processing Unit") virtualizada através do processador tendo-se como premissa de que uma vCPU equivale a uma *thread*.

1.1.26. "Virtual Machine" (VM - máquina/servidor virtual): consiste em um servidor convidado que roda em um servidor físico hospedeiro com virtualização baseada em *hypervisor*.

1.1.27. "Virtual Network" (VNet - rede virtual): uma rede virtual é um construto de conectividade definida em software (SDN - "Software-Defined Network") que é entregue como um serviço na qual a topologia de rede é configurada pelo cliente do serviço.

1.1.28. "Virtual Private Network" - VPN - rede privada virtual): extensão segura da rede local por meio de uma rede pública através de um túnel criptografado.

1.1.29. Zona de Disponibilidade (ZD): consiste em um tipo de *datacenter* lógico dentro de uma região. Um provedor com uma arquitetura baseada em ZD possui múltiplas ZD em uma região. Estas zonas de disponibilidade estão frequentemente dentro de uma distância de replicação síncrona (usualmente 100 km). Uma ZD é projetada para ser operacionalmente autônoma.

1.2. **DESCRIÇÃO DO OBJETO**

1.2.1. O objeto é composto pela composição dos seguintes serviços a serem prestados pelas contratadas e provedores de serviços de computação em nuvem ofertados ao contratante:

1.2.1.1. Fornecimento de serviços de computação em nuvem de múltiplos provedores (pelo menos dois) com possibilidade de integração com os serviços em operação nos

datacenters do contratante assegurando a implantação de ambiente do tipo nuvem híbrida.

1.2.1.2. Fornecimento de mão de obra especializada nas atividades de arquitetura e engenharia em serviços de computação em nuvem de múltiplos provedores.

1.2.1.3. Fornecimento de serviços especializados de treinamento nos serviços de computação em nuvem disponibilizados pelos múltiplos provedores ofertados visando assegurar a adequada capacitação bem como a transferência de conhecimento sobre os serviços ofertados à equipe técnica do contratante por meio da realização de treinamento oficial reconhecido pelos respectivos provedores, ou que possua classificação equivalente.

1.2.1.4. Fornecimento de serviços especializados de monitoria, relatórios, manutenção e de suporte técnico nos serviços de computação em nuvem de múltiplos provedores ofertados com acionamento automático dos serviços especializados de cada provedor.

1.2.1.5. Fornecimento de serviços de comunicação de dados para fins de interligação dos *datacenters* do contratante aos *datacenters* dos provedores de serviços de computação em nuvem garantindo a implementação de serviços em ambiente do tipo nuvem híbrida.

1.3. CARACTERÍSTICAS GERAIS DA PRESTAÇÃO DOS SERVIÇOS

1.3.1. De forma a respeitar critérios de soberania nacional, somente poderão ser ofertados serviços de nuvem que tenham como base *datacenters* localizados em território nacional.

1.3.2. A contratada deverá comprovar que realiza a corretagem de serviços de provedores em nuvem pública que possuam serviços ofertados em *datacenter* nacional. A comprovação poderá ser realizada a partir de consulta no síito dos provedor de serviços em nuvem demonstrando a existência de região operando no Brasil, carta do provedor de serviços em nuvem ou por meio de instrumento de prova equivalente.

1.3.3. Os recursos de infraestrutura viabilizados pelos serviços de computação em nuvem deverão ser totalmente definidos em *software*, incluindo recursos computacionais tais como máquinas virtuais, armazenamento e rede.

1.3.4. Os recursos de infraestrutura deverão ser escaláveis permitindo o aumento de capacidade para absorver a demanda oriunda de picos de acesso ou crescimento vegetativo do uso de aplicações disponibilizadas pelo contratante aos seus usuários.

1.3.5. O provisionamento de recursos de infraestrutura deverá ser em tempo real, sob demanda e totalmente automatizado.

1.3.6. Deverá ser possível o acesso direto aos recursos de infraestrutura assegurando seu provisionamento em modalidade de serviço auto-serviço ("self-service").

1.3.7. As interfaces de auto-serviço deverão ser expostas diretamente ao contratante, seja por meio de console de gerenciamento *web*, linha de comando (CLI - "command line interface"), SDK ou REST API.

1.3.8. O pagamento dos recursos de infraestrutura provisionados deverá empregar um modelo de precificação baseado no uso efetivo dos serviços de nuvem ("pay-per-use").

1.3.9. Todos os equipamentos, *software*, infraestrutura e sustentação, necessários à implementação e operacionalização dos serviços de computação em nuvem são de inteira responsabilidade dos provedores de nuvem ofertados pela contratada, os quais deverão executar de forma continuada procedimentos que garantam o pleno funcionamento de todos os recursos de infraestrutura, de forma integral e ininterrupta, ou seja, em modalidade 24 x 7 x 365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano), mantendo em pleno funcionamento os serviços de computação em nuvem contratados.

1.3.10. Os provedores de nuvem ofertados pela contratada deverão fornecer infraestrutura baseada em *datacenter* em plena conformidade com as exigências técnicas descritas expressamente no item 2.1.3 assegurarando a perfeita prestação dos serviços de computação em nuvem, incluindo: mão-de-obra especializada, recursos computacionais, equipamentos, cabos, fios, conectores, acessórios, componentes, estrutura de rede de fibra óptica e metálica, criação de redes virtuais, servidores virtuais, estrutura de *backup*, acesso à rede mundial de computadores, e qualquer outro insumo necessário para prestar os serviços detalhados nessa especificação técnica.

1.3.11. Os provedores de nuvem ofertados pela contratada deverão gerenciar, monitorar, sustentar e operar de forma pró-ativa todos os recursos de infraestrutura disponibilizados ao contratante, de forma a garantir o correto funcionamento de todas as funcionalidades exigidas, a partir de Centro de Gerenciamento de Segurança (SOC) e/ou de Centro de Operações de Rede (NOC), em regime 24x7 (24 horas por dia, 7 dias por semana) designado para a execução de tais atividades.

1.3.12. A partir de requisição do contratante a contratada vencedora do lote 2 deverá assegurar a interconexão entre os serviços de computação em nuvem ofertados no lote 1 e os 2 (dois) "datacenters" em operação do Poder Judiciário Gaúcho, a saber: *datacenter* primário - DC 1 (Rua Manoelito de Ornellas, n° 50, CEP 90110-230, Porto Alegre, RS, Brasil) e *datacenter* secundário - DC 2 (Avenida Borges de Medeiros, n° 1565, CEP 90010-908, Porto Alegre, RS, Brasil).

1.3.13. Deverá ser designado um representante da contratada para atuar como gerente de projeto que centralizará todos os controles e procedimentos decorrentes das atividades de prestação dos serviços. Por sua vez, caberá ao contratante a designação de um gerente de projetos específico para o desenvolvimento das atividades necessárias por parte do contratante. A metodologia de gerência deste projeto será baseada no PMBOK ("Project Management Body of Knowledge") do PMI [1] ("Project Management Institute").

1.3.14. A contratada deverá seguir normas, padrões e regulamentos expressos na política de segurança do contratante. Aos profissionais que executarão os serviços será exigido a assinatura de Termo de Responsabilidade e Sigilo, conforme formulário padrão contido no Anexo I - Termo de Responsabilidade e Sigilo.

1.3.15. Os serviços de computação em nuvem, suporte técnico especializado e de treinamento compõem lote único que será contratado de empresa representante oficial dos provedores de nuvem pública contemplados em sua proposta comercial. Enquanto que os serviços de comunicação de dados compõem lote distinto posto que usualmente são comercializados por empresas especializadas em recursos de telecomunicação se diferenciando do papel especializado de corretagem de serviços de computação em nuvem exigido no lote n° 1.

1.3.16. Poderão ser contratados serviços não descritos no instrumento contratual para atender a eventuais necessidades do contratante que não foram previstas originalmente no escopo inicialmente contratado, ou que decorram de avanços tecnológicos, desde que os custos associados não ultrapassem o valor máximo estipulado pelo contrato.

1.3.17. Todos os itens contemplados na relação de serviços de computação em nuvem a ser fornecida incluindo os dados gerados por tais serviços deverão ser hospedados em território nacional, sendo que a legislação brasileira prevalecerá sobre qualquer outra, independente da origem do provedor de nuvem.

1.3.18. Todos os serviços de computação em nuvem relacionados no edital deverão permitir obrigatoriamente e comprovadamente a apuração individual e mensal do consumo (tempo de execução, tráfego, espaço ocupado, etc).

1.3.19. Todos os serviços de computação em nuvem deverão ser prestados em regime integral, 24 horas por dia, 7 dias por semana, sem interrupção, fora do horário comercial ou em finais de semana e feriados.

1.3.20. A contratada deverá realizar o gerenciamento das assinaturas adquiridas dos provedores de serviços de computação em nuvem contidos em sua proposta comercial conforme segue:

---

[1] http://www.pmi.org

1.3.20.1. Consolidação do consumo e dos custos de utilização dos recursos computacionais.

1.3.20.2. Ativação da subscrição de serviços de computação em nuvem.

1.3.20.3. Controle de acesso, gestão de identidades e segregação dos ambientes (contas e serviços), desde que expressamente gerenciados pela contratada, não se aplicando a cenários no qual o contratante empregue os serviços dos provedores de nuvem em modalidade "self-service", cenário no qual o contratante passa a se responsabilizar por eventuais incidentes de segurança.

1.3.20.4. Administração dos *tickets* técnicos, administrativos e financeiros.

1.3.20.5. Interface com o provedor de serviços em nuvem para assuntos relacionados à assinatura.

2. CARACTERÍSTICAS TÉCNICAS MÍNIMAS DO OBJETO

LOTE 1

2.1. SERVIÇOS DE COMPUTAÇÃO MULTINUVEM

2.1.1. DESCRIÇÃO SINTÉTICA DOS SERVIÇOS

2.1.1.1. Generalidades

2.1.1.1.1. Como será descrita na seção referente à descrição analítica dos serviços de computação multinuvem, a contratada deverá atuar como representante (integrador ou "cloud broker") de pelo menos 2 (dois) provedores de serviços de computação em nuvem.

2.1.1.1.2. Consequentemente, pelo menos um dos provedores de serviços de computação em nuvem do qual a contratada atuará como integrador ou corretor ("cloud broker") deverá atender os requisitos técnicos exigidos na descrição analítica dos serviços de computação multinuvem em sua totalidade (ver seção 2.1.2), incluindo:

2.1.1.1.2.1. Oferecer serviços que sejam melhorados e atualizados de forma contínua com o intuito de trazer benefícios de desempenho e de usabilidade aos usuários.

2.1.1.1.2.2. Fornecer serviços que ofereçam um modelo de consumo sob demanda garantindo o pagamentos pelos recursos computacionais efetivamente consumidos, sem necessidade de compromissos a longo prazo, evitando ao mesmo tempo a ocorrência do fenômeno de aprisionamento tecnológico ("vendor lock in") a um provedor especifico.

2.1.1.1.2.3. Oferecer serviços que possibilitem reduções de custos decorrentes da economia de escala global de operação dos provedores.

2.1.1.1.2.4. Prover serviços que suportem *autoscaling* na qual instâncias são inicializadas ou terminadas baseados em parâmetros de desempenho e/ou capacidade definidos pelo usuário.

2.1.1.1.3. Em suma, a contratada deverá ter disponível no portfólio de fornecedores ofertado pelo menos um provedor de infraestrutura de *datacenter* responsável pela entrega de um conjunto de serviços de computação em nuvem que atenda aos requisitos técnicos enumerados a seguir.

2.1.1.2. **Resiliência**

2.1.1.2.1. Deverão ser providos por *datacenters*/zonas de disponibilidade subordinados a região com escopo de atendimento global que sejam localizados no Brasil visando assegurar a soberania dos dados armazenados.

2.1.1.2.2. Os *datacenters*/zonas de disponibilidade deverão possuir proximidade física assegurando o desempenho de rede para viabilizar a replicação síncrona dos dados.

2.1.1.2.3. Deverão ser providos em múltiplas zonas de disponibilidade localizadas no Brasil para viabilizar a publicação de aplicações com alta disponibilidade.

2.1.1.2.4. Deverá possuir pelo menos 2 (dois) *datacenters* em localidades diferentes no Brasil possibilitando a escolha do local de residência dos dados.

2.1.1.2.5. Deverão ser ofertados serviços que sejam executados em *datacenters* isolados de falhas de outros *datacenters* numa mesma região provendo conectividade de rede com baixa latência.

2.1.1.2.6. Deverá ser disponibilizado serviço de monitoria que colete métricas dos serviços e que dispare alarmes no caso de detecção de eventos relevantes.

2.1.1.2.7. Deverão ser comunicados aos clientes os níveis de dependência entre os serviços e suas respectivas regiões de forma transparente.

2.1.1.2.8. Deverá ser oferecida a opção de utilização de serviços em diversas regiões globais com o intuito de otimizar desempenho e taxas de transmissão.

2.1.1.2.9. Deverão implementar algoritmos de atribuição/alocação que permitam que servidores virtuais rodem em diferentes *datacenters*/zonas de disponibilidade/servidores físicos por meio de regra manual e/ou automática de anti-afinidade reduzindo o impacto em caso de evento falha nos *datacenters*/zonas de disponibilidade/servidores físicos.

2.1.1.2.10. Deverão permitir a manutenção dos servidores físicos do parque de equipamentos, incluindo a execução de atualização de "kernel"/"hypervisor", substituição de

componente de *hardware* e o desligamento dos servidores físicos, sem que se faça necessário a reinicialização das VMs que estejam rodando preservando a disponibilidade das aplicações evitando a disrupção dos serviços aos usuários.

2.1.1.2.11. O serviço de virtualização de instâncias computacionais deverá ser projetado para assegurar a reinicialização automática de VMs em servidor físico plenamente operacional em caso de falha no servidor físico que originalmente estava rodando tais VMs.

2.1.1.2.12. Deverão notificar os clientes em caso de necessidade de realização de operações que potencialmente podem resultar em impacto e/ou disrupção das instâncias computacionais.

2.1.1.3. **Computação**

2.1.1.3.1. Deverá proporcionar serviços na camada de processamento que sejam projetados para evitar descontinuidade ou indisponibilidade durante qualquer tipo de manutenção de *hardware*.

2.1.1.3.2. Deverá oferecer opções de instâncias computacionais que permitam a escolha entre os seguintes tipos:

2.1.1.3.2.1. Proposito geral: otimizadas para aplicações genéricas que oferecem um equilíbrio entre recursos processamento, memória e rede.

2.1.1.3.2.2. Intensivas em memória: otimizadas para uso de aplicações de uso intensivo de memória.

2.1.1.3.2.3. Processamento intensivo: otimizadas para uso em aplicações de processamento intensivo.

2.1.1.3.2.4. *Storage*: otimizada para uso intensivo de *storage* que pode ser traduzido em acessos rápidos em grande quantidade.

2.1.1.3.3. Deverá possuir em catálogo de serviços a oferta de instâncias que possam ser executadas a partir de *hardware* dedicado para um único cliente ou contratante permitindo o provisionamento de "bare-metal servers".

2.1.1.3.4. Deverá suportar a execução de pelo menos duas gerações de versões de sistemas operacionais Windows e Linux.

2.1.1.3.5. Deverá oferecer instâncias que sejam compatíveis com diferentes distribuições Linux.

2.1.1.3.6. Deverá disponibilizar instâncias que possuam dispositivos locais de armazenamento temporário para dados que mudem com frequência.

2.1.1.3.7. Deverá disponibilizar instâncias que permitam o provisionamento *self-service* de instâncias concorrentes.

2.1.1.3.8. Deverá permitir uso de mecanismo de afinidade entre instâncias garantindo seu agrupamento lógico em um mesmo *datacenter* para aplicações que exijam baixa latência e altas taxas de transferência.

2.1.1.3.9. Deverá possibilitar uso de mecanismo de anti-afinidade de instâncias assegurando sua segregação entre diferentes domínios de disponibilidade, tais como distintos domínios de falha, zonas de disponibilidade ou regiões, evitando pontos únicos de falha e descontinuidade dos serviços.

2.1.1.3.10. Deverá prover a capacidade de aumentar ou diminuir o número de instâncias automaticamente durante picos de utilização preservando desempenho ou durante períodos de baixa demanda reduzindo custos.

2.1.1.3.11. Deverá assegurar a escalabilidade horizontal das cargas de trabalho ajustando a quantidade de instâncias computacionais automaticamente baseado em condições específicas.

2.1.1.3.12. Deverá fornecer serviço que possibilite a reinicialização automática de instâncias num *host* operacional caso o *host* físico apresente falha.

2.1.1.3.13. Deverá fornecer serviço que possibilite o agendamento de operações tais como *reboot*, inicialização, desligamento e *retirement*. Dependendo do tipo do evento o usuário poderá ter a possibilidade de controlar o tempo de realização da operação.

2.1.1.3.14. Deverá permitir o provisionamento de VMs com pelo menos 64 (sessenta e quatro) processadores virtuais e 512 (quinhentos e doze) GB de memória.

2.1.1.3.15. Deverá disponilizar serviço de gerenciamento de *containers* escalável que seja compativel com a plataforma Docker ou similar.

2.1.1.3.16. Deverá disponilizar serviço de gerenciamento de *containers em* sistemas operacionais Windows e Linux com atualização manual ou automática da camada de orquestração.

2.1.1.3.17. Deverá prover serviço de orquestração de *containers* com escalonamento automático e alta disponibilidade.

2.1.1.3.18. Deverá suportar o serviço de orquestração de *containers* Kubernetes.

2.1.1.3.19. Deverá permitir a importação e exportação de uma VM existente ou a cópia da VM nos formatos de imagem VMDK, OVF, OVA ou VHD.

2.1.1.4. **Armazenamento**

2.1.1.4.1. Deverá permitir o uso de dispositivo ou serviço resistente contra violação com criptografia automática dos dados armazenados durante o transporte e apagamento dos dados ao término permitindo a migração dos dados do ambiente "on-premises" do cliente para o ambiente do provedor.

2.1.1.4.2. Os provedores dos serviços de computação em nuvem deverão ofertar serviços de armazenamento em bloco, em objeto e em arquivo.

2.1.1.4.3. Os serviços de armazenamento em bloco deverão oferecer volumes de armazenamento persistentes para uso em instâncias de computação.

2.1.1.4.4. Os serviços de armazenamento em bloco deverão possibilitar a adição de mais de um volume de armazenamento a uma instância de computação para operações de leitura e escrita.

2.1.1.4.5. Os serviços de armazenamento em bloco deverão possibilitar a parametrização de um nível de IOPS de referência.

2.1.1.4.6. Os serviços de armazenamento em bloco deverão pemitir a montagem de volumes do tipo "nonboot" em qualquer instância computacional com pelo menos 1 TB de capacidade sem que se faça necessário seu reprovisionamento.

2.1.1.4.7. Os serviços de armazenamento em bloco deverão suportar volumes de armazenamento do tipo "solid-state-drive" (SSD).

2.1.1.4.8. Os serviços de armazenamento em bloco deverão permitir que o cliente escolha a capacidade a ser provisionada e os níveis de desempenho (HDD, SSD de uso geral ou SSD otimizados por exemplo) dos volumes de armazenamento.

2.1.1.4.9. Os serviços de armazenamento em bloco deverão possibilitar a criptografia dos volumes de armazenamento baseada no algoritmo AES-256 utilizando chaves gerenciadas pelo cliente.

2.1.1.4.10. Os serviços de armazenamento em bloco deverão suportar a criação de réplicas do tipo "snapshot" dos volumes de armazenamento em determinados momentos no tempo que deverão ser de natureza incremental.

2.1.1.4.11. Deverá ser permitido compartilhar os "snapshots" em diferentes localidades geográficas com o intuito de facilitar expansão regional e eventuais migrações de *datacenters*.

2.1.1.4.12. Os serviços de armazenamento em bloco deverão suportar o apagamento dos dados de forma imediata ou na ocorrência de sua regravação.

2.1.1.4.13. Os serviços de armazenamento em bloco deverão permitir o agendamento da execução de jobs de *backup* e de *restore* do tipo "full" ou incremental dos volumes de armazenamento com política de retenção.

2.1.1.4.14. Os serviços de armazenamento de objetos deverão ser escaláveis e resilientes.

2.1.1.4.15. Os serviços de armazenamento de objeto deverão proporcionar armazenamento durável e seguro.

2.1.1.4.16. Os serviços de armazenamento de objetos deverão possibilitar o gerenciamento do ciclo de vida dos objetos desde sua criação até sua deleção final incluindo o arquivamento dos objetos com menor frequência de uso em serviço de armazenamento de baixo custo.

2.1.1.4.17. Os serviços de armazenamento de objetos deverão oferecer a opção de armazenar objetos em diferentes regiões geográficas.

2.1.1.4.18. Os serviços de armazenamento de objetos deverão permitir a criação de objetos com tamanho superior a 100 GB assegurando que na operação de escrita sejam criadas pelo menos 2 (duas) cópias em zonas de disponibilidade distintas.

2.1.1.4.19. Os serviços de armazenamento de objetos deverão verificar a integridade dos objetos por meio de técnica de "checksum" ou equivalente.

2.1.1.4.20. Os serviços de armazenamento de objetos deverão suportar o versionamento dos objetos permitindo que múltiplas versões do objeto possam ser mantidas num mesmo repositório (ou "bucket") protegendo contra deleções acidentais e regravação.

2.1.1.4.21. Os serviços de armazenamento de objetos deverão suportar a criptografia dos dados nas operações de leitura e escrita via algoritmo AES-256 utilizando chaves gerenciadas pelos clientes.

2.1.1.4.22. Os serviços de armazenamento de objetos deverão suportar a replicação assíncrona entre regiões distintas.

2.1.1.4.23. Os serviços de armazenamento de objetos deverão suportar o uso de políticas de controle de acesso (ACL - "Access Control List").

2.1.1.4.24. Os serviços de armazenamento de objetos deverão possibilitar o *upload* de diferentes partes de um dado objeto de forma independente e em ordem aleatória.

2.1.1.4.25. Os serviços de armazenamento em arquivo deverão permitir a montagem de sistemas de arquivos em qualquer tipo de instância computacional.

2.1.1.4.26. Os serviços de armazenamento em arquivo deverão permitir o crescimento e a redução automática do espaço em disco dos sistemas de arquivos que deverão ser acessíveis remotamente pelas instâncias computacionais por meio dos protocolos NFS ou SMB permitindo a criação de listas de controle de acesso e autenticação baseada em serviço de diretório.

2.1.1.4.27. Os serviços de armazenamento em arquivo deverão suportar a replicação assíncrona dos sistemas de arquivos com pelo menos 2 (duas) cópias em zonas de disponibilidade distintas.

2.1.1.4.28. Os serviços de armazenamento em arquivo deverão suportar o apagamento dos dados de forma imediata ou na ocorrência de sua regravação.

2.1.1.4.29. Os serviços de armazenamento em arquivo deverão permitir o agendamento da execução de jobs de *backup* e de *restore* do tipo "full" ou incremental de um único arquivo ou de todo um sistema de arquivos com política de retenção.

2.1.1.5. **Rede**

2.1.1.5.1. Deverá ser virtualizada e definida em *software* com topologia de rede independentemente dos equipamentos de interligação de conectividade empregados.

2.1.1.5.2. Deverá possibilitar a criação de rede virtual e sub-redes que possam ser atribuídas à endereços IP.

2.1.1.5.3. Deverá possibilitar a criação de uma ou mais sub-rede dentro de uma rede virtual privada com um único bloco de CIDR ("Classless Inter-Domain Routing").

2.1.1.5.4. Deverá permitir a criação de pelo menos 10 (dez) sub-redes por rede virtual.

2.1.1.5.5. Deverá permitir a definição de *gateway* do tráfego de saída para sub-redes com roteamento customizado para cada rede virtual.

2.1.1.5.6. Deverá suportar intervalos de endereços IP tais como os especificados na norma RFC 1918 que deverão ser roteáveis internamente.

2.1.1.5.7. Deverá possibilitar a definição de redes virtuais isoladas não roteáveis baseadas em endereços IP privados conforme RFC 1918.

2.1.1.5.8. Deverá ser fornecido serviço que suporte endereços IP associados a uma conta do cliente e não especificamente a uma instância computacional. Tais endereços IP deverão permanecer associados a uma conta até que sejam expressamente liberados.

2.1.1.5.9. Deverá possibilitar a conexão entre duas sub-redes de uma rede virtual assegurando o envio de tráfico entre ambas por meio de endereços IPs privados.

2.1.1.5.10. Deverá assegurar que o tráfego roteado entre os endereços IP privados das redes virtuais isoladas não trafegue na rede mundial de computadores.

2.1.1.5.11. Todo o tráfego privado entre os *datacenters* do provedor de nuvem deverá empregar endereços IP privados isolando o tráfego da rede mundial de computadores, embora permita-se uso de mecanismo de tunelamento do tráfego para tal fim.

2.1.1.5.12. Todo o tráfego entre as redes virtuais privadas de um cliente deverá empregar endereços IP privados, ainda que residam em *datacenters* lógicos diferentes ou em distintas regiões.

2.1.1.5.13. Todas as instâncias computacionais deverão poder empregar endereços IP privados.

2.1.1.5.14. As instâncias computacionais poderão empregar múltiplas interfaces de rede e múltiplos endereços IP.

2.1.1.5.15. Todas as instâncias computacionais poderão possuir pelo menos 2 (dois) endereços IP, sendo um endereço IP privado e outro público, com roteamento independente para cada endereço IP.

2.1.1.5.16. Deverá permitir que todas as instâncias computacionais do tipo VM possuam múltiplas interfaces de rede virtuais cada uma das quais com um endereço MAC distinto.

2.1.1.5.17. Deverá ser possível a criação de uma interface de rede e sua incorporação e desincorporação a uma dada instância computacional bem com sua incorporação em outra instância computacional.

2.1.1.5.18. Deverá ser permitido a captura de informações sobre o tráfico IP entre interfaces de rede.

2.1.1.5.19. Deverá ser ofertado recurso que possibilite a atribuição automática de endereços IP públicos a diferentes instâncias computacionais.

2.1.1.5.20. Todas as instâncias computacionais deverão possuir suporte para múltiplos protocolos IP v4 tais como TCP, UDP e ICMP.

2.1.1.5.21. Deverá ser oferecido serviço que possibilite conexão de rede dedicada entre o provedor de nuvem e o *datacenter* do cliente em função da demanda de tráfego.

2.1.1.5.22. O serviço de conectividade de rede dedicada deverá permitir a conexão entre as redes privativas em operação no ambiente "on-premises" do cliente e as redes virtuais em funcionamento no ambiente de nuvem pública dos provedores por meio de conectividade Ethernet, VPN, MPLS, BGP ou modalidades equivalentes.

2.1.1.5.23. O serviço de conectividade de rede dedicada interligando o ambiente de *datacenter* do cliente à nuvem prestadora de serviço através de *link* dedicado com comunicação de dados ponto a ponto com suporte a IPv4 deverá ter taxa de transmissão "full duplex" de 1 Gbps ou de 10 Gbps.

2.1.1.5.24. Deverá oferecer um serviço que possibilite conexões VPN do tipo "site-to-site" entre provedor de nuvem e *datacenter* do cliente.

2.1.1.5.25. O serviço VPN do tipo "site-to-site" em operação na rede pública deverá conectar a rede privativa de dados em operação no ambiente "on-premises" de um dado cliente e suas respectivas redes virtuais em funcionamento no ambiente de nuvem pública via rede mundial de computadores, sendo que cada rede virtual deverá possuir pelo menos duas conexões VPN.

2.1.1.5.26. O serviço VPN do tipo "site-to-site" deverá ser baseado nos padrões e IKE ("Internet Key Exchange") e IPSec ("IP Security Protocol").

2.1.1.5.27. O serviço VPN do tipo "site-to-site" deverá implementar criptografia dos pacotes IP de forma transparente e automática.

2.1.1.5.28. Deverá ser fornecido serviço de balanceamento de carga (LB - "Load Balancer") para fins de distribuição do tráfego HTTP e HTTPS de entrada permitindo o emprego de endereços IP públicos e privados assegurando que instâncias computacionais em operação na camada de "back-end" do LB venham a possuir

endereços IP públcos e privados e que essas se comuniquem ao LB através de endereços IP privados.

2.1.1.5.29. O serviço de balanceamento de carga deverá prover mecanismo de detecção de falhas que venham a ocorrer nas instâncias computacionais de "back-end" evitando o encaminhamento de requisições para instâncias computacionais irresponsivas.

2.1.1.5.30. O serviço de balanceamento de carga deverá prover mecanismo de multiplexão das conexões, "keep-alive" das instâncias computacionais e suportar "sticky sessions" assegurando a persistência de sessões ("session affinity") garatindo que uma dada requisição de usuário seja consistentemente encaminhada para a mesma instância computacional de destino.

2.1.1.5.31. O serviço de balanceamento de carga deverá prover mecanismo de aceleração de tráfego SSL ("SSL offload") terminando as conexões SSL por meio do emprego de certificado SSL desonerando as VMs dos clientes que não necessitam executar os algoritmos de criptografia/descriptografia SSL.

2.1.1.5.32. Deverá fornecer serviço de balanceamento de carga em camada 4 para fins de distribuição de tráfego TCP e UDP em direção a portas específicas em operação nas instâncias computacionais de "back-end" permitindo o emprego de endereços IP públicos e privados.

2.1.1.5.33. Deverá ser fornecido serviço de balanceamento de carga em camada 7 para fins de distribuição do tráfego HTTP e HTTPS de entrada entre as instâncias computacionais permitindo o emprego de endereços IP públicos e privados, suportando persistência de sessões ("session affinity") e aceleração de tráfego SSL ("SSL offload").

2.1.1.5.34. O serviço de balanceamento de carga em camada 7 deverá encaminhar requisições em direção às instâncias computacionais de "back-end" baseado em padrões contidos nas URI ("Unified Resource Identifier"), nos cabeçalhos HTTP e nos parâmetros da requisição HTTP.

2.1.1.5.35. Deverá ser provido serviço DNS ("Domain Name System") possibilitando o balanceamento de instâncias computacionais entre diversos *hosts*.

2.1.1.5.36. Deverá ser disponibilizado serviço de *gateway* NAT ("Network Address Translation") distribuindo tráfico de instâncias computacionais internas em direção à Internet, permitindo que instâncias computacionais que possuem apenas endereços IP privados se conectem a dispositivos com endereços IP públicos por meio do roteamento do tráfego de saída destinado à rede mundial de computadores.

2.1.1.5.37. Deverá oferecer serviço de entrega de conteúdo ("Content Delivery Network") com baixa latência a partir de diferentes pontos de presença.

2.1.1.6. **Segurança**

2.1.1.6.1. Deverá ser provido serviço de gerenciamento de chaves (KMS - "Key Management Service") responsável pelo ciclo de vida de gerenciamento de chaves criptográficas, permitindo que clientes criem, controlem e auditem o uso de chaves criptográficas, bem como possibilitando a importação de chaves criptográficas criadas no ambiente "on premises".

2.1.1.6.2. Deverá ser disponibilizado serviço de gerenciamento de certificados digitais permitindo a importação, renovação e emissão de certificados SSL, suportando o uso de certificados emitidos por autoridade de certificação (CA - "Certificate Authority") ao invés do uso de certificados do tipo auto-assinados ("self-signed").

2.1.1.6.3. Os provedores de serviços de nuvem deverão prover serviços que atendam as seguintes certificações internacionais ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2 e SOC 3. A comprovação de tais certificações poderá ser realizada por meio eletrônico ou equivalente.

2.1.1.6.4. Os provedores deverão ser auditados conforme padrões SOC1/SOC2/SOC3 e manter a certificação ISO/IEC 27001 em todos seus *datacenters*.

2.1.1.6.5. Deverá ser comprovado por meio de evidência documental que seus procedimentos de sanitização e de descarte de dados são aderentes aos processos defindos pelo NIST ("National Institute of Standards and Technology").

2.1.1.6.6. Deverá fornecer serviço de gerenciamento de acesso e identidades (IAM - "Identity and Access Management") que deverá suportar a federação de identidades entre contas criadas no ambiente "on premises" e contas criadas no ambiente de nuvem, exigindo que seja necessário apenas um *login* ("single sign-on") para habilitar o uso do portal, CLI e API.

2.1.1.6.7. Todos os serviços de nuvem deverão suportar o mecanismo de RBAC ("Role Based Access Control") por meio do uso do serviço de gerenciamento de acesso e identidades do provedor.

2.1.1.6.8. Deverá fornecer serviços que permitam controlar acesso a recursos a partir de condições relacionadas com IPs de origem e horas do dia.

2.1.1.6.9. Deverá fornecer serviços que permitam gerenciar grupos e usuários.

2.1.1.6.10. Deverá fornecer serviços que permitam a ativação de um diretório "stand-alone" na nuvem ou a conexão com uma instância MS Active Directory existente.

2.1.1.6.11. Deverá ser disponibilizado serviço de *firewall* do tipo *stateful* com filtragem de pacotes IP no nível de sub-rede permitindo o controle do tráfego de entrada e de saída (ACL - "Access Control List") baseado em informações da camada de rede e de transporte.

2.1.1.6.12. Deverá ser provido serviço que suporte a adição ou remoção de regras de tráfico de entrada (*inbound/ingress*) em direção às instâncias computacionais.

2.1.1.6.13. Deverá ser fornecido serviço que suporte a adição ou remoção de regras de tráfico de saída (*outbound/egress*) originado nas instâncias computacionais.

2.1.1.6.14. Deverá disponibilizar serviço que ofereça proteção a aplicações *web* contra ataques distribuídos de negação de serviços (DDoS - "Distributed Denial of Service"), como por exemplo TCP SYN *floods*, UDP *floods* ou ataques de reflexão.

2.1.1.6.15. Deverá ser provido serviço para detectar e mitigar automaticamente ataques volumétricos de negação de serviço distribuídos (DDoS) até a camada 4 do modelo OSI.

2.1.1.6.16. Deverá ser provido serviço de proteção sob demanda contra ataques DDoS que deverá mitigar ataques não volumétricos em camada 7, por meio de mecanismo ("traffic-scrubbing"), disponibilizando um time de resposta a incidentes de segurança para auxílio na análise e mitigação de ataques DDoS.

2.1.1.6.17. Deverão permitir que clientes criem registros de *log* relativos ao tráfego de rede que é permitido e bloqueado pelo serviço de *firewall* para fins de análise forense.

2.1.1.6.18. Deverá ser disponibilizado serviço de *firewall* de aplicação *web* que permita bloquear solicitações maliciosas (WAF - "Web Application Firewall") por meio do uso de assinaturas de ataque ou via emprego de técnicas mais aprimoradas de detecção.

2.1.1.6.19. O serviço WAF deverá permitir criar regras para evitar ataques do tipo "SQL Injection" e "Cross-site Scripting".

2.1.1.6.20. O serviço WAF deverá permitir criar regras para bloquear ou liberar determinados endereços IP.

2.1.1.6.21. O serviço WAF deverá permitir criar regras para bloquear ou liberar requisições com base em informações do cabeçalho da requisição HTTP.

2.1.1.6.22. O serviço WAF deverá ser configurado e permitir a mitigação de ataques listados em "Open Web Application Security Project (OWASP) Top 10 Web Application Security Risks", possuindo integração nativa com outros serviços do provedor assegurando proteção contra vulnerabilidades em aplicações *web*.

2.1.1.6.23. O serviço WAF deverá permitir a monitoria de métricas em tempo real.

2.1.1.6.24. Deverá ser provido serviço de detecção de ameaças com monitoria contínua do ambiente de nuvem identificando potenciais ameaças.

2.1.1.6.25. Deverá ser disponibilizado serviço de avaliação de vulnerabilidades em sistemas operacionais visando identificar vulnerabilidades conhecidas bem como detectar desvios com relação às melhores práticas de segurança.

2.1.1.6.26. Deverá ser fornecido serviço de gerenciamento de correções de *software* para sistemas operacionais Windows e Linux baseado na aprovação do cliente com atualização agendada.

2.1.1.6.27. Deverá fornecer serviços de cofre de senhas que ofereçam a possibilidade de utilizar um dispositivo HSM ("Hardware Security Module" - cofre digital) dedicado possibilitando o armazenamento e operação segura de chaves criptográficas.

2.1.1.6.28. Os serviços de cofre de senhas deverão possibilitar a criação e a gestão de chaves criptográficas por meio do emprego de algoritmos de criptografia e de autenticação.

2.1.1.6.29. Os serviços de cofre de senhas deverão prover alta disponibilidade e balanceamento de carga.

2.1.1.6.30. Os serviços de cofre de senhas deverão assegurar durabilidade das chaves armazenadas permitindo que várias cópias sejam realizadas.

2.1.1.6.31. Os serviços de cofre de senhas deverão possibilitar auditorias sobre operações em chaves criptográficas.

2.1.1.6.32. Deverá fornecer serviços que registrem o histórico de chamadas de APIs e eventos relacionados com a atividade de uma determinada conta incluindo a disponibilização dos respectivos registros de *log*.

2.1.1.6.33. Deverá disponibilizar serviços que possibilitem armazenar registros de *log* de acesso em serviço de armazenamento de baixo custo.

2.1.1.7. **Infraestrutura de Software**

2.1.1.7.1. Deverá ser disponibilizado serviço de banco de dados relacional gerenciado ("Relational DBaaS") do tipo "serverless" em modalidade PaaS sem que o tráfego de dados se baseie no uso de endereços públicos na Internet. Alternativamente, deverá permitir o emprego de bancos de dados em modalidade IaaS.

2.1.1.7.2. O serviço de banco de dados relacional gerenciado deverá permitir o emprego de bancos de dados "open-source" tais como MySQL e PostgreSQL, sendo que tal enumeração não é exaustiva. Alternativamente, deverá permitir o emprego de bancos de dados "open-source" em modalidade IaaS.

2.1.1.7.3. O serviço de banco de dados relacional gerenciado deverá permitir o emprego de bancos de dados proprietários disponibilizados pelo provedor de serviços em nuvem.

2.1.1.7.4. O serviço de banco de dados relacional gerenciado deverá ser escalável com alta disponibilidade permitindo o emprego de mais uma instância de banco de dados com réplica de leitura e de pelo menos 2 (dois) tipos de bancos de dados ("open-source" ou proprietário).

2.1.1.7.5. O serviço de banco de dados relacional gerenciado deverá permitir a configuração de *backups* automáticos com politicas de retenção e exportação de *dump* de banco de dados.

2.1.1.7.6. O serviço de banco de dados relacional gerenciado deverá possibilitar a replicação assíncrona de réplicas de leitura de pelo menos 2 (dois) tipos de bancos de dados ("open-source" ou proprietário) que deverão estar espalhadas entre diversos *datacenters* dentro de uma mesma região.

2.1.1.7.7. O serviço de banco de dados relacional gerenciado deverá possibilitar o *failover* manual de uma base primária para uma réplica em *standby*.

2.1.1.7.8. O serviço de banco de dados relacional gerenciado deverá possibilitar a leitura de réplicas assegurando escalabilidade sobrepujando os limites de uma única base num contexto de altas cargas de trabalho de consulta.

2.1.1.7.9. O serviço de banco de dados relacional gerenciado deverá possibilitar a recuperação de uma base de dados num determinado ponto no tempo.

2.1.1.7.10. O serviço de banco de dados relacional gerenciado deverá possibilitar a criação de um *snapshot* de uma base e posterior recuperação.

2.1.1.7.11. O serviço de banco de dados relacional gerenciado deverá possibilitar a criptografia dos dados armazenados ("in rest") utilizando o algoritmo de criptografia AES-256 ou similar.

2.1.1.7.12. Deverá ser disponibilizado serviço de migração de banco de dados gerenciado permitindo a migração dos bancos de dados empregados pelos clientes para bancos de dados relacionais gerenciados suportados pelo provedor.

2.1.1.7.13. Deverá ser disponibilizado serviço de "data warehouse" gerenciado do tipo "serverless" compatível com o padrão ANSI SQL e com drivers ODBC e JDBC.

2.1.1.7.14. O serviço gerenciado de "data warehouse" deverá suportar cargas de trabalho com terabytes de dados.

2.1.1.7.15. O serviço gerenciado de "data warehouse" deverá possibilitar a replicação e *backup* automáticos dos dados.

2.1.1.7.16. O serviço gerenciado de "data warehouse" deverá oferecer diferentes mecanismos de *backup* (incremental, continuo e automático) para dados armazenados.

2.1.1.7.17. O serviço gerenciado de "data warehouse" deverá suportar criptografia de dados no armazenamento ("in rest") e na transferência ("in transit").

2.1.1.7.18. Deverá fornecer serviços gerenciados de processamento em tempo real de grande quantidade de dados a partir de *streams*.

2.1.1.7.19. Deverá fornecer serviços gerenciados que permitam a transmissão de dados entre serviços de processamento e *storage* de forma nativa.

2.1.1.7.20. Deverá ser disponibilizado serviço "functions as a service" gerenciado do tipo "serverless" que permita executar código gerenciando os recursos computacionais consumidos de forma transparente.

2.1.1.7.21. O serviço "functions as a service" gerenciado deverá executar código sob demanda com suporte a pelo menos 3 (três) linguagens de programação em tempo de execução limitado e tarifado somente pelo uso efetivo dos recursos computacionais consumidos.

2.1.1.7.22. O serviço "functions as a service" gerenciado deverá ser escalável tratando aspectos de concorrência e de disponibilidade por meio de mecanismos de tratamento de erros de forma transparente.

2.1.1.7.23. Deverá ser disponibilizado serviço de banco de dados não relacional (NoSQL ou similar) gerenciado para aplicações que necessitem escalabilidade e baixa latência.

2.1.1.7.24. O serviço de banco de dados não relacional gerenciado deverá ser do tipo "serverless" e baseado nos mecanismos de armazenamento chave-valor, documento e colunar suportando *backups* automáticos sem disrupção das operações de banco de dados.

2.1.1.7.25. O serviço de banco de dados não relacional gerenciado deverá permitir o emprego de bancos de dados "open-source" e proprietário.

2.1.1.7.26. O serviço de banco de dados não relacional gerenciado deverá possibilitar a replicação de dados de forma automática entre *datacenters* físicos de uma mesma região geográfica oferecendo alta disponibilidade e durabilidade dos dados.

2.1.1.7.27. O serviço de banco de dados não relacional gerenciado deverá suportar uma estrutura de chave e de valores baseada em chave primária.

2.1.1.7.28. O serviço de banco de dados não relacional gerenciado deverá suportar modelo de dados baseados em JSON ou equivalente através de armazenamento, *queries* e atualizações de tal formato de dados.

2.1.1.7.29. O serviço de banco de dados não relacional gerenciado deverá suportar a execução de códigos que são executados como respostas a modificações nas tabelas.

2.1.1.7.30. O serviço de banco de dados não relacional gerenciado deverá garantir consistência durante operações de leitura, assegurando que usuários acessem os dados mais atualizados.

2.1.1.7.31. Deverá ser disponibilizado serviço de *cache* em memória ("in-memory caching") gerenciado do tipo "serverless" compatível com Redis ou Memcached que permita o armazenamento de dados do tipo chave-valor.

2.1.1.7.32. O serviço de *cache* em memória gerenciado deverá ser escalável e clusterizado para assegurar alta disponibilidade com capacidade de alterar o número de nós assim como os recursos provionados para cada nó.

2.1.1.7.33. Deverá ser disponibilizado serviço de *gateway* de API ("Application Programming Interface") gerenciado do tipo "serverless" escalável e resiliente.

2.1.1.7.34. O serviço de *gateway* de API deverá implementar mecanismo de controle de acesso baseado em políticas atuando como intermediário na invocação de chamadas de API provenientes de aplicações e como "proxy" para APIs remotas.

2.1.1.7.35. O serviço de *gateway* de API deverá suportar pelo menos o padrão OAuth 2.0 e implementar mecanismo de "traffic-shaping".

2.1.1.7.36. O serviço de *gateway* de API deverá permitir que desenvolvedores publiquem documentação referente a uma dada API e a gravação de registro de "log" de requisições de acesso à API.

2.1.1.7.37. Deverá ser disponibilizado serviço de mensageria assíncrona gerenciado do tipo "serverless" escalável e resiliente que implemente mecanismo de fila de mensagens.

2.1.1.7.38. O serviço de mensageria assíncrona deverá permitir o transporte de eventos em modalidade "many-to-many" (n produtores x n consumidores) suportando pelo menos um dos padrões arquiteturais via RESTful API: "queues/topics", "point-to-point", "publish/subscribe".

2.1.1.7.39. O serviço de mensageria assíncrona deverá permitir o emprego de sistemas de mensageria "open-source" ou proprietário.

2.1.1.7.40. Deverá ser disponibilizado serviço de indexação e pesquisa gerenciado do tipo "serverless" escalável com suporte a pilha de pacotes de *software* ELK (Elasticsearch, Logstash and Kibana) ou similar permitindo integração com aplicações.

2.1.1.7.41. Deverá fornecer serviço de notificações gerenciado do tipo "serverless".

2.1.1.7.42. Deverá disponibilizar serviço de *transcoding* de conteúdo de mídias.

2.1.1.7.43. Deverá ser fornecido serviço de entrega de *e-mail* gerenciado do tipo "serverless" escalável baseado em "relay" SMTP que suporte o envio de mensagens via protocolo SMTP ou API.

2.1.1.7.44. Deverá fornecer serviços de suporte para SDKs para diversas plataformas tais como Node.js, .NET, Java, Go, PHP, Python, Ruby.

2.1.1.7.45. Deverá fornecer serviços de versionamento de aplicações.

2.1.1.8. **Aprendizado de Máquina**

2.1.1.8.1. Deverá ser fornecido serviço de aprendizado de máquina (ML - "Machine Learning") gerenciado do tipo "serverless" escalável baseado em instâncias computacionais otimizadas com infraestrutura provisionada de treinamento de máquina.

2.1.1.8.2. O serviço de aprendizado de máquina gerenciado deverá permitir a criação e treinamento de modelos preditivos.

2.1.1.8.3. O serviço de aprendizado de máquina gerenciado deverá possuir integração nativa com outros serviços de armazenamento permitindo o uso de dados existentes.

2.1.1.8.4. O serviço de aprendizado de máquina gerenciado deverá apoiar na análise de desempenho de modelos através de cálculos de métricas de qualidade e da visualização do seu comportamento.

2.1.1.8.5. O serviço de aprendizado de máquina gerenciado deverá oferecer ferramentas de visualização e exploração de dados ajudando na análise de conteúdo e na identificação de padrões.

2.1.1.8.6. O serviço de aprendizado de máquina gerenciado deverá suportar transformações nos dados através de sugestões automáticas.

2.1.1.8.7. O serviço de aprendizado de máquina gerenciado deverá permitir o emprego de instâncias computacionais configuradas especificamente para treinamento e validação estatística de modelos de ML, com aceleração de hardware (NVIDIA GPUs ou similar) suportado por "frameworks" de ML, barramento de alta velocidade (PCIe 3.0, NVIDIA NVLink ou similar) entre CPU e acelerador e entre aceleradores, rede de interconexão com alta vazão (RDMA, InfiniBand ou similar) e armazenamento de dados com alta velocidade (NVME SSD ou similar).

2.1.1.8.8. O serviço de aprendizado de máquina deverá prover infraestrutura de treinamento de ML do tipo "serverless" sem que seja necessário o gerenciamento da infraestrutura do "framework" de ML.

2.1.1.8.9. O serviço de aprendizado de máquina deverá suportar múltiplos "frameworks" de ML contemplando pelo menos TensorFlow, PyTorch, scikit e Apache MXNet.

2.1.1.8.10. O serviço de aprendizado de máquina deverá ser complementado por APIs do tipo "serverless" escaláveis e resilientes que deverão suportar pelo menos as seguintes funcionalidades: tradução de linguagem escrita, conversão da linguagem falada para texto ("speech-to-text"), reconhecimento de imagens, reconhecimento ótico de caracteres (OCR - "optical character recognition") e processamento natural de linguagem incluindo suporte para *chatbot*.

2.1.1.9. **Análise de Dados**

2.1.1.9.1. Deverá ser disponibilizado serviço de análise de dados para operações "Big Data" gerenciado do tipo "serverless" escalável baseado em *clusters* Hadoop com armazenamento HDFS ou via integração com outro serviço para tal fim.

2.1.1.9.2. Deverão ser ofertadas instâncias computacionais otimizadas para transações configuradas especificamente para cargas de trabalho orientadas a transações de

banco de dados e de análise de dados com armazenamento NVME SSD, conectividade de pelo menos 10 Gbps e instâncias computacionais com pelo menos 8 vCPUs e 64 GB de RAM.

2.1.1.9.3. A infraestrutrura de análise de dados deverá permitir o provimento de serviço gerenciado de Hadoop para processamento de quantidades consideráveis de dados por meio do emprego de *framework* "open source" baseado em Java ou equivalente que suporte aplicações distribuídas rodando em *clusters*.

2.1.1.10. **Operações e Governança**

2.1.1.10.1. As interfaces de auto-serviço (portal, CLI e API) deverão suportar todas as funcionalidades providas pelos serviços de computação em nuvem.

2.1.1.10.2. Deverá ser disponibilizada funcionalidade de gerenciamento básico de custos incluindo a bilhetagem do mês corrente e do mês anterior bem como a geração de alertas em caso de consumo superior ao orçamento estimado. Alternativamente, tal requisito poderá ser atendido pelo uso de *scripts* elaborados pela contratada.

2.1.1.10.3. Deverá ser disponibilizada funcionalidade de projeção e de estimativa dos custos futuros mensais baseada em calculadora disponível no portal, em planilha Excel disponível para *download* ou por meio de API que permita a obtenção dos custos programaticamente.

2.1.1.10.4. Deverá ser provido serviço de diretório gerenciado do tipo "serverless" e resiliente compatível com o serviço Microsoft Active Directory System (ADS).

2.1.1.10.5. O serviço de diretório deverá suportar pelo menos a execução das operações "join" em domínio do serviço MS ADS para instâncias computacionais que estejam rodando os sistemas operacionais Windows e Linux, criação de usuários/grupos, atribuição de grupos a usuários, autenticação de usuários e criação/aplicação de "group policies".

2.1.1.10.6. Deverá ser disponibilizado serviço de agendamento de tarefas ("task scheduler") do tipo "serverless" escalável permitindo o agendamento de tarefas em horários com intervalos recorrentes.

2.1.1.10.7. Deverá ser disponibilizado serviço de atualização automática de sistemas operacionais (OS - "operating system") possibilitando a atualização automática e/ou manual do OS que roda nas instâncias computacionais.

2.1.1.10.8. Deverá ser disponibilizado serviço de sincronização de tempo globalmente distribuído baseado no protocolo NTP ("Network Time Protocol").

2.1.1.10.9. Os dispositivos computacionais empregados para entregar os serviços de computação em nuvem deverão sincronizar seus relógios locais por meio do uso do protocolo NTP.

2.1.1.10.10. Deverá ser provido serviço de *batch job* do tipo "serverless" assegurando a execução de cargas computacionais em lote, permitindo sua definição, submissão e execução em um *cluster* de instâncias computacionais, ainda que o cliente venha a ter a responsabilidade de especificar o número de nós do *cluster* bem com seu tipo computacional.

2.1.1.11. **Gerenciamento e Auditoria**

2.1.1.11.1. Deverá ser providenciado "dashboard" de saúde dos serviços de nuvem ofertados permitindo sua visualização com base nos serviços regionalmente disponíveis.

2.1.1.11.2. Deverá ser provida documentação sobre o modelo de responsabilidade compartilhada de operação e segurança entre provedor e cliente, a qual deverá documentar claramente a divisão de responsabilidade entre ambos os atores.

2.1.1.11.3. Deverá ser fornecido serviço de notificação de mudança de versão dos serviços de computação em nuvem com pelo menos 1 (um) ano de antecedência.

2.1.1.11.4. Deverão ser providenciados guias de referência de arquitetura de aplicações documentando as melhores práticas sugeridas pelo provedor em sua plataforma de serviços, incluindo aspectos relativos a disponibilidade, desempenho e segurança.

2.1.1.11.5. Deverá ser comprovada a aderência às certificações de segurança e de privacidade em nuvem por meio de auditoria externa devendo ser mantidas as certificações ISO/IEC 27017 e 27018 em todos os serviços de nuvem por meio do uso dos controles de segurança aplicáveis a cada contexto.

2.1.1.11.6. Deverá entregar serviços que permitam monitorar o inventário de recursos utilizados incluindo o histórico de configurações realizadas com o intuito de aprimorar a segurança e conformidade.

2.1.2. **DESCRIÇÃO ANALÍTICA DOS SERVIÇOS**

2.1.2.1. A contratada deverá atuar como representante/corretor (integrador ou "cloud broker") de pelo menos 2 (dois) provedores de serviços de computação em nuvem (doravante denominado provedor de nuvem).

2.1.2.2. Pelo menos um dos provedores de nuvem ofertados deverá atender aos requisitos descritos na Tabela 1 em sua integralidade.

2.1.2.2.1. Caberá à contratada firmar os contratos associados com os provedores para utilização dos serviços de computação nuvem que venham a ser consumidos pelo contratante.

2.1.2.2.2. Todos os serviços apresentados na Tabela 1 somente serão aceitos se forem parte da lista de serviços de computação em nuvem dos provedores ofertados pela

contratada, devendo ser contabilizados por meio de USNs. Não serão aceitos provisionamento de serviços por meio de instalação de *software* ou máquinas virtuais para a sua prestação, caso tais serviços não integrem o conjunto de soluções oferecidas no catálogo do provedor de nuvem ofertado e não possam ser contabilizados diretamente pelos provedores.

2.1.2.2.3. Consequentemente, serviços providos através de loja *online* ou *marketplace* dos provedores de serviços em nuvem ofertados não serão adquiridos visto não estarem mapeados na Tabela 1.

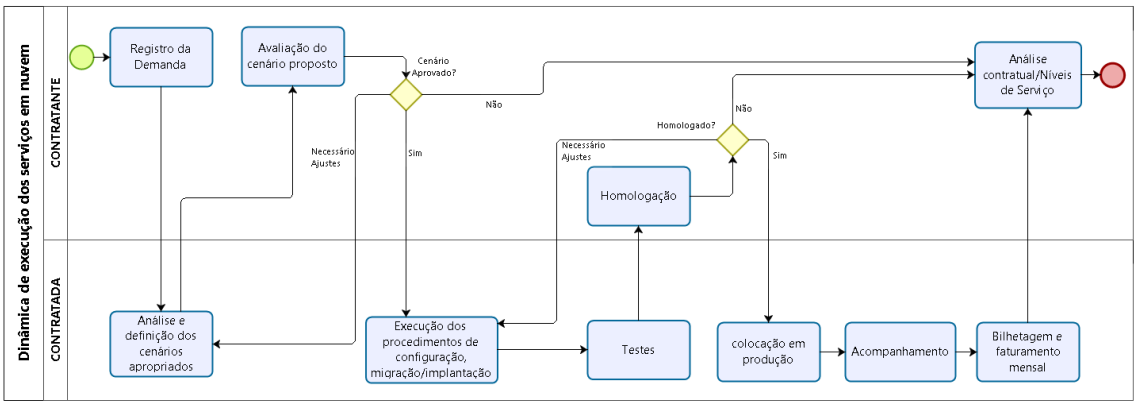
2.1.2.3. A contratada deverá comprovar, no momento da assinatura do contrato, ser empresa autorizada a comercializar os serviços e prestar suporte técnico dos provedores de nuvem ofertados. Esta comprovação deverá ser feita por meio de declaração dos provedores. Por conseguinte, caberá a futura contratada apresentar declaração para habilitação conforme Anexo VI.

2.1.2.4. A contratada deverá disponibilizar uma conta em cada um dos provedores de nuvem ofertados em nome do contratante, por meio da qual poderão provisionados os serviços descritos na Tabela 1.

2.1.2.4.1. Esta conta deverá permitir que o contratante delegue à contratada o acesso aos recursos em nuvem disponíveis para execução dos serviços técnicos especializados descritos na Tabela 3.

2.1.2.5. A dinâmica de execução do objeto inclui etapas de registro da demanda, análise e definição dos cenários apropriados, aprovação pelo contratante, execução dos procedimentos de configuração, migração/implantação, testes, homologação, colocação em produção, acompanhamento, bilhetagem e faturamento dos serviços mensalmente, conforme fluxograma apresentado na Figura 1.

Figura 1 - Fluxo de Execução dos Serviços em Nuvem



2.1.2.6. Os serviços de computação em nuvem serão adquiridos por meio de Unidades de Serviço em Nuvem (USN), que servirá como base para aquisição de serviços do provedor.

2.1.2.6.1. A métrica de USN consiste em método padronizado para obtenção de uma quantidade objetivamente definida a ser cobrada pelos serviços de computação em nuvem.

2.1.2.6.2. Tal métrica expressa-se no estabelecimento de um valor de referência específico para cada serviço de computação em nuvem listado na Tabela 1.

2.1.2.6.3. A estimativa do valor de referência da USN individual de cada serviço enumerado na Tabela 1 se baseou na média aritmética dos valores praticados em dólar por diferentes provedores na Região América do Sul (São Paulo).

2.1.2.6.4. Para determinar o valor dos serviços em USN descritos na Tabela 1 deverá ser adotado o seguinte procedimento visando minimizar a ocorrência de discrepâncias nos valores ofertados:

2.1.2.6.4.1. Determinar o valor do serviço em dólar (VALOR1), cobrado pelo provedor de nuvem, para cada serviço da Tabela 1, na localidade solicitada pelo contratante. O preço determinado neste item deverá considerar os custos com a prestação do serviço de suporte técnico de que trata o item 2.4.3.

2.1.2.6.4.2. Aplicar a cotação do dólar comercial do Banco Central do Brasil, do dia da realização do pregão, ao valor obtido no item anterior para obter o valor inicial do serviço em real (VALOR2 = VALOR1 * cotação do dólar comercial). A cotação do dólar se manterá fixa, ao longo de todo o contrato, de acordo com a cotação do dólar comercial do dia da realização do pregão.

2.1.2.6.4.3. Calcular a soma dos percentuais de todos os impostos, contribuições e demais tributos que incidam sobre o serviço prestado, incluindo os descritos no Ato Declaratório Interpretativo da Receita Federal Brasileira nº 7, de 15 de agosto de 2014 (ADI-RFB nº 7/2014 [2]), se for o caso (IMPOSTOS = ∑ PERCENTUAL DE IMPOSTOS + CONTRIBUIÇÕES + TAXAS). A empresa deverá indicar em sua proposta, no momento da licitação, o percentual total relativo a este item, conforme modelo constante do Anexo VIII (Modelo de Proposta de Preços - Lote 1). A empresa também deverá indicar na proposta o seu regime de tributação (EIRELI, EPP, Lucro real, Lucro presumido, etc.).

---

[2] Acessível em http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=55186. Tal ato determina que sobre os valores pagos pela disponibilização de infraestrutura para armazenamento e processamento de dados para acesso remoto (*data center*) devem incidir o Imposto sobre a Renda Retido na Fonte (IRRF), a Contribuição de Intervenção no Domínio Econômico destinada a financiar o Programa de Estímulo à Interação Universidade-Empresa para o Apoio à Inovação (Cide-Royalties), a Contribuição para o PIS/Pasep-Importação e a Cofins-Importação.

2.1.2.6.4.4. Determinar a soma dos percentuais de despesas da contratada, que deverá englobar despesas afetas à garantia, bem como qualquer outra despesa da contratada, incluindo a redução de riscos baseada na estratégia de taxa "hedge" [3] (DESPESAS = ∑ PERCENTUAL DE DESPESAS). Tal percentual deverá ser fixo durante todo o contrato, e deverá ser aplicado linearmente a todo e qualquer serviço do provedor de nuvem ofertado. A empresa deverá indicar em sua proposta, no momento da licitação, o percentual total relativo a este item, bem como os percentuais individuais que compõem o percentual total, conforme modelo constante do Anexo VIII (Modelo de Proposta de Preços - Lote 1).

2.1.2.6.4.5. Determinar o percentual de lucro da contratada (LUCRO). Tal percentual deverá ser fixo durante todo o contrato, e deverá ser aplicado linearmente a todo e qualquer serviço do provedor de nuvem ofertado. A empresa deverá indicar em sua proposta, no momento da licitação, o percentual total relativo a este item, conforme modelo constante do Anexo VIII (Modelo de Proposta de Preços - Lote 1).

2.1.2.6.4.6. Aplicar os índices IMPOSTOS, DESPESAS e LUCRO, calculados nos itens 2.1.2.6.4.3, 2.1.2.6.4.4 e 2.1.2.6.4.5, ao valor VALOR2 obtido no item 2.1.2.6.4.2, para obter o preço final do serviço em real (VALORFINAL = VALOR2 + (VALOR2 * (∑ PERCENTUAL DE IMPOSTOS + DESPESAS + LUCRO))).

2.1.2.6.4.7. Dividir o somatorio de VALORFINAL para cada serviço da Tabela 1 pelo valor do volume anual estimado de USNs para obter o preço do serviço em USNs.

2.1.2.6.5. A contratada será responsável pela obtenção dos serviços com melhor relação custo/benefício dos provedores de nuvem ofertados após análise e mensuração dos preços ofertados levando em conta a quantidade de USNs a serem consumidas pelo contratante.

2.1.2.6.6. Os serviços ou recursos, condições, bem como suas faixas e franquias, declarados como gratuitos na política de preços praticada pelo provedor de serviços em nuvem, integrantes ou não da Tabela 1, deverão ser disponibilizados sem ônus ao contratante.

2.1.2.7. O contratante fará uso e efetuará o pagamento apenas das USNs relativas aos serviços efetivamente solicitados à contratada até o limite máximo das USNs

[3] Presume-se que a licitante poderá se beneficiar de operação de "hedge" visando evitar perdas em função da variação dos preços do dólar comprando contratos futuros de dólar com o preço da moeda predeterminado para uma data futura, por exemplo.

estimadas. O contratante não realizará compra prévia de USNs. Consequentemente, não serão contratados serviços com reserva de capacidade.

2.1.2.8. Conforme mencionado, pelo menos um dos provedores de serviços de computação em nuvem que componha a oferta do integrador deverá atender integralmente (100%) todos os serviços relacionados na Tabela 1, os quais deverão expressamente constar no catálogo de serviços do provedor. Consequentemente, não será aceito a combinação de provedores distintos para tal finalidade.

2.1.2.9. Pelo menos um dos provedores de serviços de computação em nuvem que componha a oferta do integrador deverá permitir que todos os serviços listados na Tabela 1 e que todos os dados pertencentes ao contratante residam em *datacenter* instalado fisicamente em território nacional, incluindo replicação e cópias de segurança, de modo que o contratante disponha de todas as garantias da legislação brasileira enquanto tomadora do serviço e responsável pela guarda das informações armazenadas em nuvem.

2.1.2.10. Deverá ser disponibilizado pela contratada um portal contendo informações sobre:

2.1.2.10.1. Planilha de preços: valores praticados pela contratada com os preços de todos os serviços (em USN), informando também quais serviços dos provedores são gratuitos.

2.1.2.10.2. Relatório de faturamento: relatórios com consumo de serviços dos provedores.

2.1.2.10.3. Informações sobre o contrato: detalhamento do contrato, tipos de serviços.

2.1.2.10.4. Os relatórios deverão ser disponibilizados pelo portal, com periodicidade mensal, estando dentro das responsabilidades da contratada, não sendo cobrado como serviço adicional.

2.1.2.11. Todas as ferramentas, soluções, *software* e scripts fornecidos pela contratada deverão ser executados em infraestrutura do contratante ou nos próprios provedores de nuvem.

2.1.2.11.1. Sob nenhuma hipótese o contratante arcará com custos relacionados ao direito de uso das ferramentas.

2.1.2.11.2. O contratante não ficará responsável pela instalação, manutenção e suporte continuado de tais ferramentas, nem emitirá ordens de serviço para esses fins, devendo essa ser uma das responsabilidades da contratada.

2.1.2.12. A contratada e/ou provedor de nuvem deverá oferecer calculadora ou simulador público de preços para cada item da Tabela 1.

2.1.2.13. Todos os serviços solicitados pelo contratante para a contratada e operacionalizados nos provedores de nuvem serão de propriedade apenas do contratante, a quem deverá ser assegurado acesso de leitura irrestrito a qualquer momento do contrato. Todas as contas e senhas utilizadas pela contratada para operacionalizar serviços dos

provedores de nuvem serão criadas para uso exclusivo do contratante, e não poderão ser utilizadas para gerência de qualquer outro cliente da contratada.

2.1.2.14. Todos os dados produzidos pelos serviços solicitados pelo contratante para a contratada e operacionalizados no provedor serão de propriedade apenas do contratante, a quem deverá ser assegurado acesso irrestrito a qualquer momento do contrato.

2.1.2.15. A contratada deverá fornecer, mediante solicitação do contratante, *backup* das aplicações incluindo código fonte, dados e *scripts* de configuração que estiverem disponíveis em nuvem, o que inclui as imagens das máquinas virtuais de aplicação, cópias dos dados armazenados em dispositivos de armazenamento em nuvem, cópias dos bancos de dados que fazem parte das topologias das aplicações do contratante provisionadas em nuvem ou que fazem parte de topologias híbridas de aplicações e do banco de dados da ferramenta de gestão de nuvem.

2.1.2.16. Os serviços prestados pela contratada deverão ser prestados de modo que as aplicações do contratante provisionadas no ambiente de nuvem sejam portáveis para outros provedores, visando minimizar a possibilidade de aprisionamento tecnológico ("vendor lock-in").

2.1.2.16.1. Consequentemente, não deverão ser utilizados serviços, protocolos ou ferramentas nativos de apenas um provedor (proprietários), salvo quando justificável tecnicamente ou por decisão de projeto/operação e autorizados formalmente pelo contratante.

2.1.2.16.2. Caso seja tomada a decisão de utilizar qualquer serviço, protocolo ou ferramenta que torne uma ou mais aplicações do contratante não portáveis para outros provedores de nuvem, nos planos de saída correspondente deverão ser considerados os riscos inerentes a esta decisão e também indicadas alternativas para que estas aplicações possam, em caso de necessidade, serem reprovisionadas em outros provedores de serviços em nuvem e/ou infraestruturas.

2.1.2.16.3. Caso a arquitetura da aplicação tenha sido definida pela contratada, será de sua responsabilidade garantir a portabilidade das aplicações para outros provedores, incluindo a definição de mecanismos, padrões e protocolos, desde que autorizados formalmente pelo contratante.

2.1.2.17. Ao término do contrato, a contratada repassará ao contratante todas as informações necessárias à continuidade da operação dos serviços em nuvem incluindo, no mínimo, o seguinte:

2.1.2.17.1. Todos os artefatos, incluindo, mas não limitados, a dados, serviços, *workflows*, *scripts*, catálogos de serviço, códigos fontes e arquivos de configuração.

2.1.2.17.2. Listagem de todas as contas, senhas e permissões utilizadas.

2.1.2.18. O pagamento da última fatura do contrato será condicionado à apresentação de todas as informações que trata o item anterior.

2.1.2.19. O foro da contratação será nacional, e a legislação brasileira prevalecerá sobre qualquer outra, independente da origem dos provedores de nuvem, de acordo com os termos do art. 11 da Lei 12.965/2014.

2.1.2.20. A contratada deverá comprovar, no momento da assinatura do contrato, ser empresa autorizada a comercializar os serviços e prestar suporte técnico dos provedores de serviços de computação em nuvem ofertados. Essa comprovação deverá ser feita por meio de declaração dos provedores e/ou através de informações disponibilizadas no *site* oficial do provedor.

2.1.2.21. A contratada não poderá ofertar provedor de serviços em nuvem que pertença a seu mesmo grupo econômico. Esse requisito visa evitar direcionamento e conflitos da contratada entre os papéis de prestador de serviços técnicos e de provedor de serviços em nuvem, além de viabilizar a supremacia do interesse do contratante no consumo das melhores opções do ambiente multinuvem.

2.1.2.22. A relação dos serviços de computação em nuvem a serem contratados consta da Tabela 1. Tais serviços não são exaustivos, e indicam essencialmente componentes básicos de infraestrutura e plataformas de serviços a serem ofertados.

2.1.2.23. Poderão ser contratados recursos e serviços descritos ou não no contrato para atender a eventuais necessidades do contratante não previstas originalmente, ou que decorram de avanços tecnológicos, desde que os custos decorrentes não sejam superiores ao valor máximo prescrito no instrumento contratual. Todavia, a inclusão de serviços que não correspondam exatamente àqueles relacionados nas especificações técnicas dependerá de aditivo contratual, respeitadas as disposições da legislação aplicável.

2.1.2.24. No caso de serviços que não correspondam exatamente à descrição dos serviços relacionados taxativamente na Tabela 1, porém oferecidos pelos provedores de nuvem, a quantidade de USNs poderá ser negociada por meio de ordem de serviço (OS), de acordo com a estimativa de consumo de tais serviços.

Tabela 1 - Serviços de Computação em Nuvem

Item	Descrição do Serviço	Unidade	Valor de Referência em Dólares - USN - Valores Médios - Região América do Sul (São Paulo) [4]

[4] Ou região US East quando o serviço não estiver disponível no Brasil.

1	Máquina Virtual Linux - provisionado com 1 vCPU e 2 GB de memória RAM, por demanda	Instância/hora	0,0417
2	Máquina Virtual Linux - provisionado com 2 vCPU e 4 GB de memória RAM, por demanda	Instância/hora	0,0757
3	Máquina Virtual Linux - provisionado com 4 vCPU e 16 GB de memória RAM, por demanda	Instância/hora	0,2008
4	Máquina Virtual Windows - provisionado com 1 vCPU e 2 GB de memória RAM, por demanda	Instância/hora	0,0708
5	Máquina Virtual Windows - provisionado com 2 vCPU e 4 GB de memória RAM, por demanda	Instância/hora	0,1266
6	Máquina Virtual Windows - provisionado com 2 vCPU e 4 GB de memória RAM, por demanda	Instância/hora	0,3012
7	Serviços de Registro de Containers	Gigabyte/mês	0,18
8	Serviços de Orquestração de Containers	Unidade de vCPU/hora	0,0772
9	Serviço Gerenciado de Publicação de Aplicações Web	Unidade de vCPU/hora	0,0507
10	Serviço de Armazenamento de Blocos (SSD)	Gigabyte/mês	0,2067
11	Serviço de Armazenamento de Blocos (HDD)	Gigabyte/mês	0,0437
12	Serviço de Armazenamento de Objetos - dados com maior frequência de uso	Gigabyte/mês	0,8905
13	Serviço de Armazenamento de Objetos - dados com menor frequência de uso	Gigabyte/mês	0,2585
14	Serviço de Armazenamento de Arquivos	Gigabyte/mês	0,3353
15	Tráfego de Saída da Rede	Gigabyte/mês	0,0808
16	Tráfego de Conexão Intra-região - serviços fornecidos em múltiplas regiões	Gigabyte/mês	0,0404
17	Porta de Conexão de Fibra Ótica 1 Gbps	Unidade/hora	1,45
18	Porta de Conexão de Fibra Ótica 10 Gbps	Unidade/hora	2,25
19	Serviço de DNS - Hospedagem de Zonas	Zona/mês	0,1
20	Serviço de DNS - Consultas	Por operação (a cada 1.000.000)/mês	0,4
21	Serviço de Balanceamento de Carga	Unidade/hora	0,025
22	Serviço de Rede de Entrega de Conteúdo	Gigabyte/mês	0,1175
23	IP Público	Unidade/Mês	0,0017
24	Serviços de Rede Privada Virtual	Gigabyte/mês	0,02
25	Serviço de VPN Gateway	Hora de Conexão	0,995
26	Serviço de Gateway NAT	Hora de Conexão	0,093
27	Serviço de Backup	Instância/mês	10
28	Serviço de Armazenamento de Backup	Gigabyte/mês	0,0114
29	Serviço de Gateway de Armazenamento	Gigabyte/mês	0,01
30	Serviço de Diretório Gerenciado Integrado com o Microsoft Active Directory	Unidade/hora	0,783
31	Serviço de Auditoria e Análise de Logs	Gigabyte/Mês	0,5
32	Serviço de Análise Preditiva e Criação de Modelo para Aprendizado de Máquina	Unidade/hora	2,98
33	Serviço Gerenciado de Execução de Funções	Por operação (a cada 100)/mês	0,004
34	Serviço de Execução de Cargas de Trabalho de Computação em Lote	Unidade/hora	0,9486
35	Serviço de Cofre de Chaves	Por operação (a cada 10.000)/mês	0,6567
36	Serviço Gerenciado de Certificados Digitais	Por operação/mês	0,75
37	Serviço de Gerenciamento de Segredos para Aplicações e APIs	Por operação (a cada 10.000)/mês	0,05
38	Serviço de Gerenciamento de Chaves	Por operação (a cada 10.000)/mês	0,03
39	Serviço Web Aplication Firewall	Por operação (a cada 1.000.000)/mês	1,0085
40	Serviço de Proteção contra Ataques DDoS	Valor mensal	2972
41	Serviço de Avaliação de Vulnerabilidades	Por operação/mês	0,0017
42	Serviço de Banco de Dados Relacional Gerenciado	Unidade/hora	1,6103
43	Serviço Gerenciado de "Data Warehouse"	Unidade/hora	9,84
44	Serviço de Banco de Dados não Relacional Gerenciado	Por operação (a cada 1.000.000)/mês	2,025
45	Serviço de Migração de Banco de Dados	Unidade/hora	1,58
46	Serviço de Análise de Dados	Unidade/hora	2,2664
47	Serviço de Importação e Exportação de Dados	Unidade	283,33
48	Serviço de Indexação e Pesquisa de Documentos	Gigabyte/Mês	1,1219
49	Serviço de Cache em Memória	Unidade de vCPU/hora	0,5848
50	Serviço de Gateway de API	Por operação (a cada	2,4467

		1.000.000)/mês	
51	Serviço de Mensageria Assíncrona	Por operação (a cada 1.000.000)/mês	0,55
52	Serviço de Entrega de Mensagem Eletrônica	Por operação (a cada 1.000)/mês	0,2
53	Serviço de Codificação de Vídeo	Por operação/minuto	0,045
54	Serviço de Visualização de Mapas	Por operação (a cada 1.000)/mês	7
55	Serviço de Identificação de Robôs	Por operação (a cada 1.000)/mês	1
56	Serviço de Transmissão de Vídeos	Gigabyte/mês	0,1
57	Serviço de Compartilhamento de Arquivos	Por usuário/mês	5,08

2.1.2.25. Segue abaixo descrição detalhada de cada serviço listado na Tabela 1.

2.1.2.25.1. **Máquina Virtual Linux e Windows (requisitos aplicáveis a todos os subtipos enumerados na Tabela 1 - itens 1 ... 6)**

2.1.2.25.1.1. As máquinas virtuais serão provisionadas na modalidade por demanda, na qual os serviços são alocados sem um período pré-determinado e com faturamento periódico, de acordo com a respectiva ordem de serviço.

2.1.2.25.1.2. As máquinas virtuais, cujo propósito é de uso geral, deverão ser demandadas respeitando a seguinte relação vCPU e memória RAM: 1 x 2; 2 x 4 e 4 x 8.

2.1.2.25.1.3. As máquinas virtuais serão ofertadas com os seguintes sistemas operacionais instalados: Linux (CentOS 7 ou superior; Ubuntu Server 16.04.2 ou superior), Windows (Windows Server 2016 ou superior).

2.1.2.25.1.4. As vCPUs das máquinas virtuais deverão utilizar pelo menos as seguintes famílias de processadores: Intel Xeon família E5, Xeon Scalable Processor, Xeon Platinum, AMD EPYC, Arm Neoverse ou Arm Zeus. Logo, poderão ser utilizados processadores x86 e/ou ARM. Todavia, poderão ser utilizadas máquinas virtuais cujo *baseline* de capacidade seja inferior a capacidade máxima nominal do processador.

2.1.2.25.1.5. Os sistemas operacionais deverão estar devidamente licenciados e aptos para uso.

2.1.2.25.1.6. As máquinas virtuais deverão ser fornecidas com disco destinado ao *boot* e hospedagem do sistema operacional. A capacidade de espaço em disco deverá ser suficiente para atender aos requisitos de sistema operacional e seus processos de gerência dos recursos computacionais. Entretanto, deve ser enfatizado que não deverá ser somado ao preço da máquina virtual o custo de armazenamento no caso de discos do tipo "nonboot" posto que este será computado com base nos itens 10 ou 11 da Tabela 1.

2.1.2.25.1.7. Deverá permitir que as máquinas virtuais possuam múltiplas interfaces de rede e múltiplos endereços IP incluindo um endereço IP privado e outro público com roteamento independente para cada endereço IP.

2.1.2.25.1.8. Os recursos de CPU e de memória alocados para as máquinas virtuais hospedadas no mesmo servidor físico deverão ser isolados como se cada máquina virtual fosse um servidor físico distinto.

2.1.2.25.1.9. O serviço gerenciado de computação deverá permitir o uso dos serviços de armazenamento de blocos, objetos e arquivos.

2.1.2.25.1.10. Deverá suportar o uso de grupos de segurança ("security groups") controlando o acesso aos recursos de rede providos pela máquina virtual via pilha de protocolo IP v4 (ICMP, UDP e TCP).

2.1.2.25.1.11. O serviço gerenciado deverá suportar criptografia no armazenamento ("in rest") e na transferência ("in transit").

2.1.2.25.1.12. Deverá suportar o monitoramento do uso de CPU, RAM, disco e tráfego de rede.

2.1.2.25.2. **Serviços de Registro de Containers**

2.1.2.25.2.1. Deverá ser durável, escalável e seguro.

2.1.2.25.2.2. Deverá prover serviço gerenciado de registro permitindo o gerenciamento de repositórios e de imagens de serviços de *container* padrões de mercado suportando pelo menos o *container* Docker.

2.1.2.25.3. **Serviços de Orquestração de Containers**

2.1.2.25.3.1. Deverá ser durável, escalável e seguro.

2.1.2.25.3.2. Deverá possibilitar a criação e o gerenciamento de *clusters* de *containers* permitindo provisionar, configurar ou dimensionar *clusters* de máquinas virtuais para executar contêineres. Alternativamente, deverá permitir a execução de contêineres sem a necessidade de dimensionar e gerenciar servidores ou *clusters* de máquinas virtuais.

2.1.2.25.3.3. Deverá ser integrável aos serviços de registro de *containers*.

2.1.2.25.3.4. Deverá permitir a criação de imagens de *containers* assegurando seu armazenamento em serviço gerenciado de registro seguro.

2.1.2.25.3.5. Deverá ser integrável ao serviço de balanceamento de carga.

2.1.2.25.3.6. Deverá ser integrável ao serviço conectividade de rede permitindo o emprego de sub-redes públicas e privadas em pelo menos duas zonas de disponibilidade distintas.

2.1.2.25.3.7. Deverá permitir a configuração dos *containers* via CLI ou REST API.

2.1.2.25.4. **Serviço Gerenciado de Publicação de Aplicações Web**

2.1.2.25.4.1. Deverá ser gerenciado do tipo "serverless" e escalável permitindo a implantação e o gerenciamento de aplicações *web* no ambiente do provedor de nuvem em modalidade PaaS. Alternativamente, deverá ser provido em modalidade IaaS.

2.1.2.25.4.2. Deverá possibilitar a publicação de aplicações *web* via *upload* de versão do aplicativo na forma de um pacote de origem (por exemplo, arquivo Java .war)

ou similar iniciando automaticamente o ambiente de execução, criando e configurando os recursos e serviços em nuvem necessários para executar o código que foi publicado, incluindo mecanismos de rede privada virtual, resolução de nomes, balanceamento de carga, "auto scaling", certificados digitais, grupos de segurança, serviço de banco de dados e área de armazenamento do código fonte e executável.

2.1.2.25.4.3. Deverá provisionar automaticamente instâncias computacionais necessárias para rodar as aplicações publicadas.

2.1.2.25.4.4. Deverá suportar a alteração do tamanho do conjunto de instâncias computacionais empregadas pelas aplicações publicadas.

2.1.2.25.4.5. Deverá possibilitar o versionamento das aplicações publicadas.

2.1.2.25.4.6. Deverá viabilizar a criação de novos ambientes permitindo criar e gerenciar ambientes separados para uso em desenvolvimento, teste e produção.

2.1.2.25.4.7. Deverá suportar o desenvolvimento de aplicações nas linguagens de programação Go, Java, .NET, Node.js, PHP, Python e Ruby.

2.1.2.25.4.8. Deverá garantir a implantação de aplicativos a partir de contêineres Docker.

2.1.2.25.5. **Serviço de Armazenamento de Blocos (SSD)**

2.1.2.25.5.1. Serviço para utilização de volumes de armazenamento "block-level".

2.1.2.25.5.2. Deverá possibilitar que o volume criado seja anexado às instâncias computacionais e reconhecido pelo sistema operacional como um dispositivo físico e local.

2.1.2.25.5.3. Deverá ser baseado em discos de estado sólido (SSD).

2.1.2.25.5.4. Deverá permitir informar o desempenho mínimo, em IOPS e MiB/s, para o volume provisionado.

2.1.2.25.5.5. Deverá suportar criptografia dos volumes no armazenamento ("in rest").

2.1.2.25.6. **Serviço de Armazenamento de Blocos (HDD)**

2.1.2.25.6.1. Serviço para utilização de volumes de armazenamento "block-level".

2.1.2.25.6.2. Deverá possibilitar que o volume criado seja anexado às instâncias computacionais e reconhecido pelo sistema operacional como um dispositivo físico e local.

2.1.2.25.6.3. Deverá ser baseado em discos magnéticos (HDD).

2.1.2.25.6.4. Deverá permitir informar o desempenho mínimo, em IOPS e MiB/s, para o volume provisionado.

2.1.2.25.6.5. Deverá suportar criptografia dos volumes no armazenamento ("in rest").

2.1.2.25.7. **Serviço de Armazenamento de Objetos - dados com maior frequência de uso**

2.1.2.25.7.1. Serviço para utilização de volumes de armazenamento de objetos que exigem menor tempo de acesso.

2.1.2.25.7.2. Deverá ser durável, escalável e seguro.

2.1.2.25.7.3. Deverá permitir a criação/exclusão de *containers* de objetos ("buckets" ou estrutura similar).

2.1.2.25.7.4. Deverá permitir a interação com as funcionalidades do serviço gerenciado via CLI, API e/ou SDK.

2.1.2.25.7.5. Deverá permitir a criação/exclusão de objetos com tamanho superior a 100 GB organizados em "buckets" ou estrutura similar.

2.1.2.25.7.6. Deverá possuir recurso de versionamento dos objetos.

2.1.2.25.7.7. Deverá possibilitar a criação de listas de controle de acesso (ACL - "Access Control List") vinculadas aos objetos concedendo autorização de uso de operações de leitura e de gravação.

2.1.2.25.7.8. Deverá possuir interface *web* para inclusão de objetos e consultas de informações.

2.1.2.25.7.9. Deverá implementar API e/ou SDK que permita executar as operações de "upload", "download" e exclusão de objetos.

2.1.2.25.7.10. Deverá suportar criptografia dos objetos no armazenamento ("in rest") e na transferência ("in transit").

2.1.2.25.7.11. Deverá possibilitar a replicação entre regiões assegurando a cópia automática assíncrona de objetos pertencentes a "buckets" ou estrutura similar entre diferentes zonas de disponibilidade e/ou regiões.

2.1.2.25.8. **Serviço de Armazenamento de Objetos - dados com menor frequência de uso**

2.1.2.25.8.1. Serviço gerenciado de armazenamento otimizado para dados com baixa frequência de uso ("dados frios") e menor custo oferecendo capacidade para arquivamento de dados e *backup*.

2.1.2.25.8.2. Deverá ser durável, escalável e seguro.

2.1.2.25.8.3. Deverá permitir a criação/exclusão de *containers* de objetos ("buckets" ou estrutura similar).

2.1.2.25.8.4. Deverá permitir a interação com as funcionalidades do serviço gerenciado via CLI, API e/ou SDK.

2.1.2.25.8.5. Deverá implementar API e/ou SDK que permita executar as operações de "upload", "download" e exclusão de objetos.

2.1.2.25.8.6. Deverá suportar integração com o serviço de armazenamento de objetos para dados com maior frequência de uso com acesso em tempo real (item 12 da Tabela 1).

2.1.2.25.9. **Serviço de Armazenamento de Arquivos**

2.1.2.25.9.1. Serviço para utilização de volumes de armazenamento de arquivos.

2.1.2.25.9.2. Deverá ser durável, escalável e seguro.

2.1.2.25.9.3. Deverá permitir a criação de sistemas de arquivos

2.1.2.25.9.4. Deverá suportar a publicação dos sistemas de arquivos via protocolos CIFS ou NFS.

2.1.2.25.9.4.1. No caso de sistemas de arquivos publicados via protocolos CIFS deverá permitir sua integração com o serviço de diretórios MS Active Directory.

2.1.2.25.9.5. Os sistemas de arquivos publicados via CFS ou NFS deverão ser acessíveis por instâncias computacionais em funcionamento em diferentes redes virtuais e sub-redes.

2.1.2.25.9.6. Deverá possibilitar a criação de listas de controle de acesso (ACL - "Access Control List") vinculadas aos sistemas de arquivos concedendo autorização de uso de operações de leitura, gravação e execução de processos.

2.1.2.25.9.7. Deverá suportar criptografia de dados no armazenamento ("in rest") e na transferência ("in transit").

2.1.2.25.9.8. Deverá possibilitar a replicação e *backup* manual e/ou automáticos dos arquivos.

2.1.2.25.10. **Tráfego de Saída da Rede**

2.1.2.25.10.1. Deverá permitir a transmissão do tráfego de dados de saída originado de redes privadas virtuais do contratante em direção à rede mundial de computadores.

2.1.2.25.10.2. Nenhum tráfego de entrada em direção às redes privadas virtuais do contratante deverá ser tarifado.

2.1.2.25.11. **Tráfego de Conexão Intra-região - serviços fornecidos em múltiplas regiões**

2.1.2.25.11.1. O serviço gerenciado consiste na possibilidade de transmitir dados bidirecionalmente entre serviços de nuvem que foram configurados para operar em topologia com múltiplas regiões de disponibilidades em cenários de alta disponibilidade (replicação síncrona e/ou assíncrona) ou outros cenários que necessitem de tal funcionalidade.

2.1.2.25.12. **Porta de Conexão de Fibra Ótica de 1 Gbps ou 10 Gbps**

2.1.2.25.12.1. Serviço de conexão de fibra dedicada entre a infraestrutura de rede local do contratante (*datacenter* "on-premises") e uma porta de conexão do provedor de serviços em nuvem sem encaminhamento do tráfego pela Internet.

2.1.2.25.12.2. A porta de conexão deverá estar localizada em território nacional e prover no mínimo 1 Gbps ou 10 Gbps.

2.1.2.25.12.3. Deverá ser compatível com o protocolo de comunicação IPv4 e suportar quadros Ethernet de 1.500 ou 9.000 bytes na camada de enlace com encapsulamento VLAN 802.1Q.

2.1.2.25.12.4. Todos os custos de conexão do *datacenter* do contratante até a porta de conexão do provedor de serviços em nuvem serão de responsabilidade do

contratante. Tais custos serão contemplados pelos serviços descritos no item 2.8.

2.1.2.25.13. **Serviço de DNS - Hospedagem de Zonas**

2.1.2.25.13.1. Serviço gerenciado que permite criar, editar, alterar e excluir entradas no DNS em domínios registrados.

2.1.2.25.13.2. Deverá garantir a resolução de consultas de DNS para aplicações hospedadas em redes privadas virtuais.

2.1.2.25.13.3. Deverá permitir o monitoramento e o registro em *log*.

2.1.2.25.14. **Serviço de DNS - Consultas**

2.1.2.25.14.1. Serviço gerenciado que permite realizar consultas DNS que representam a ação de um *host* buscar um registro específico que está exposto em uma zona DNS publicada.

2.1.2.25.14.2. Deverá ser possível realizar buscas nos registros de recursos disponíveis, quais sejam do tipo A, AAAA, CNAME, MX, PTR, NS, SOA, SRV e TXT, sendo cada um específico para cada finalidade.

2.1.2.25.15. **Serviço de Balanceamento de Carga**

2.1.2.25.15.1. Serviço de balanceamento de carga resiliente que assegura a distribuição automática do tráfego de rede de entrada para aplicações em múltiplos destinos, tais como instâncias computacionais, contêineres e endereços IP, em várias zonas de disponibilidade, aumentando a disponibilidade e a tolerância a falhas de tais aplicações.

2.1.2.25.15.2. Deverá ser escalável, de maneira a crescer ou diminuir seu poder de processamento em função do fluxo de dados que por ele trafegar, permitindo adicionar e remover recursos computacionais de acordo com as necessidades das cargas de trabalho sem perturbar o fluxo geral de encaminhamento de requisições em direção as aplicações balanceadas.

2.1.2.25.15.3. Deverá permitir a configuração do protocolo e/ou número de porta para conexões de clientes que serão encaminhadas para os destinos.

2.1.2.25.15.4. Deverá possibilitar a utilização dos protocolos HTTP, HTTPS e TCP para efetuar o balanceamento de carga incluindo a realização de *health check* nas aplicações.

2.1.2.25.15.5. Deverá suportar os protocolos HTTP/1.0 e HTTP/1.1 em conexões "front-end" (cliente para balanceador de carga) e em conexões "back-end" (balanceador de carga para aplicação destino).

2.1.2.25.15.6. Deverá permitir uso de mecanismo de fidelização por *cookies* (*sticky session*) assegurando a afinidade entre clientes e aplicações.

2.1.2.25.15.7. Deverá possibilitar o uso de endereços IP públicos que deverão estar acessíveis via serviço DNS na camada de "front-end" enquanto que as conexões "back-end" poderão empregar endereços IP privados.

2.1.2.25.15.8. Deverá assegurar o balanceamento de carga de aplicações entre diversas zonas de disponibilidade.

2.1.2.25.16. **Serviço de Rede de Entrega de Conteúdo**

2.1.2.25.16.1. O serviço de rede de entrega de conteúdo (CDN - "Content Delivery Network") deverá ser gerenciado do tipo "serverless" escalável e resiliente acelerando a entrega de conteúdo *web* estático e dinâmico.

2.1.2.25.16.2. Deverá distribuir conteúdo por meio de uma rede global de *datacenters* denominados pontos de presença, acelerando a distribuição de conteúdo via encaminhamento de cada requisição ao ponto de presença com capacidade de entrega mais rápida ao visualizador do usuário.

2.1.2.25.16.3. Deverá prover alta confiabilidade e disponibilidade garantindo que cópias de arquivos sejam mantidos em *cache* em vários pontos de presença.

2.1.2.25.16.4. Deverá assegurar que na solicitação de conteúdo o usuário seja roteado para o ponto de presença com a menor latência para que o conteúdo seja fornecido com melhor desempenho e com maiores taxas de transferência de dados.

2.1.2.25.16.5. Deverá permitir a especificação dos servidores de origem que armazenam a versão original e definitiva dos arquivos que serão distribuídos nos pontos de presença.

2.1.2.25.16.6. Deverá possibilitar o "upload" dos arquivos nos servidores de origem.

2.1.2.25.16.7. Deverá permitir a criação de um ponto de distribuição composto por um conjunto de servidores de origem dos quais serão obtidos os arquivos.

2.1.2.25.16.8. Deverá replicar a configuração do ponto de distribuição para todos os pontos de presença em *datacenters* geograficamente nos quais são armazenadas cópias dos arquivos.

2.1.2.25.16.9. Deverá restringir a distribuição geográfica de conteúdo impedindo que usuários de algumas localizações acessem o conteúdo entregue em um ponto de distribuição

2.1.2.25.16.10. Deverá armazenar conteúdo em *cache* com base nos cabeçalhos de solicitação.

2.1.2.25.16.11. Deverá gerenciar o tempo de permanência (expiração) do conteúdo em *cache*.

2.1.2.25.16.12. Deverá assegurar a veiculação de vídeo sob demanda ou *streaming* de vídeo ao vivo usando qualquer origem de HTTP.

2.1.2.25.16.13. Deverá adicionar, remover ou substituir conteúdo a ser distribuído via uso do protocolo HTTPS ou similar.

2.1.2.25.16.14. Deverá permitir o monitoramento e o registro em *log*.

2.1.2.25.17. **IP Público**

2.1.2.25.17.1. Serviço de atribuição de endereço IP v4 público (estático ou dinâmico) dedicado, até que seja liberado a pedido do contratante, ou no caso de ser dinâmico, até que o recurso seja desligado.

2.1.2.25.18. **Serviços de Rede Privada Virtual**

2.1.2.25.18.1. Deverá permitir a criação e a exclusão de redes privadas virtuais.

2.1.2.25.18.2. Deverá permitir a criação e a exclusão de sub-redes CIDR IPv4.

2.1.2.25.18.3. Deverá permitir a associação e a desassociação de blocos CIDR IPv4 com endereços privados especificados na RFC 1918 a uma rede privada virtual.

2.1.2.25.18.4. Deverá possibilitar a associação e a desassociação de blocos CIDR IPv4 com endereços privados especificados na RFC 1918 secundários a uma rede privada virtual.

2.1.2.25.18.5. Deverá permitir a atribuição de endereços IPv4 privados a sub-redes e instâncias computacionais.

2.1.2.25.18.6. Deverá suportar a criação de tabela de roteamento especificando as rotas permitidas para o tráfego de saída originado de uma sub-rede.

2.1.2.25.18.7. Deverá permitir a exclusão de uma tabela de roteamento.

2.1.2.25.18.8. Deverá permitir a adição e a remoção de rotas da tabela de roteamento.

2.1.2.25.18.9. Deverá permitir acesso a rede mundial de computadores atuando como *gateway* redundante e resiliente para instâncias computacionais em uma sub-rede de uma rede privada virtual, fornecendo um destino nas tabelas de rotas da rede privada virtual para o tráfego roteável na Internet e executando tradução de endereços de rede (NAT - "Network Address Translation") para instâncias designadas por meio do uso de endereços IPv4 públicos.

2.1.2.25.18.10. Deverá suportar a criação de lista de controle de acesso de rede ("Network ACL") funcionando como *firewall* para controlar o tráfego de entrada e de saída de uma ou mais sub-redes.

2.1.2.25.18.11. Deverá possibilitar a associação e a desassociação de listas de controle de acesso de rede a uma ou mais sub-redes.

2.1.2.25.18.12. Deverá suportar a criação e a exclusão de regras de entrada e de saída em uma lista de controle de acesso de rede permitindo ou bloqueando o tráfego.

2.1.2.25.19. **Serviço de VPN Gateway**

2.1.2.25.19.1. Serviço para uso de rede privada virtual ("Virtual Private Network" - VPN) que deverá permitir que instâncias computacionais executadas no ambiente de nuvem pública possam se comunicar com instâncias computacionais em operação no ambiente "on-premises" do cliente.

2.1.2.25.19.2. Deverá permitir conexão remota com o ambiente "on-premises" em modalidade *site-to-site* através de concentrador VPN criado no ambiente de nuvem pública que se conecta ao dispositivo de *gateway* do cliente.

2.1.2.25.19.3. Deverá permitir a criação e a exclusão de túneis VPN.

2.1.2.25.19.4. O tráfego de dados bidirecional através da conexão deverá empregar túnel VPN utilizando os protocolos IPSec e IKEv2.

2.1.2.25.19.5. A taxa de transferência mínima na conexão do túnel VPN deverá ser de pelo menos 100 Mbps.

2.1.2.25.19.6. Deverá permitir o uso de concentrador (*gateway*) VPN que poderá ser associado às redes privadas virtuais do cliente.

2.1.2.25.19.7. Deverá suportar topologias de conexão *site-to-site* com túnel VPN do tipo 1-1 (1 concentrador VPN no ambiente de rede - 1 concentrador de VPN no ambiente "on-premises"), 1-n (1 concentrador VPN no ambiente de rede - n concentradores de VPN no ambiente "on-premises") e n-n (n concentradores VPN no ambiente de rede - n concentradores de VPN no ambiente "on-premises").

2.1.2.25.19.8. Deverá permitir a monitoria dos túneis VPN.

2.1.2.25.20. **Serviço de Gateway NAT**

2.1.2.25.20.1. Deverá possibilitar o uso de dispositivo NAT para permitir que instâncias computacionais em uma sub-rede privada se conectem à rede mundial de computadores. Tal dispositivo deverá substituir o endereço IPv4 de origem pelo seu endereço IPv4 público ao transmitir o tráfego e converter o endereço IPv4 público nos endereços IPv4 privados ao receber o tráfego.

2.1.2.25.21. **Serviço de Backup**

2.1.2.25.21.1. Serviço gerenciado que permite a realização de cópias de segurança (*backup)* e de restauração de dados na nuvem.

2.1.2.25.21.2. Deverá alocar e gerenciar automaticamente o armazenamento de *backup*.

2.1.2.25.21.3. Deverá permitir a transmissão segura e o armazenamento dos dados criptografados.

2.1.2.25.21.4. Deverá fornecer *backups* consistentes garantindo que correções adicionais não sejam necessárias ao restaurar os dados.

2.1.2.25.21.5. Deverá permitir retenção dos *backups* por pelo menos 2 (dois) anos.

2.1.2.25.21.6. Deverá fornecer sistema de alertas para falhas no processo de *backup* ou ao detectar inconsistência de arquivos.

2.1.2.25.22. **Serviço de Armazenamento de Backup**

2.1.2.25.22.1. Serviço com possibilidade de armazenamento heterogêneo, local ou em nuvem, de cópias de segurança, com alta disponibilidade.

2.1.2.25.22.2. Os dados deverão ser persistidos com redundância, de no mínimo 2 (duas) cópias dos dados em equipamentos de *hardware* diferentes, de forma a prevenir perda de dados com falhas de *hardware*.

2.1.2.25.22.3. Deverá permitir retenção de dados por pelo menos 2 (dois) anos.

2.1.2.25.22.4. Deverá permitir a criptografia dos dados.

2.1.2.25.23. **Serviço de Gateway de Armazenamento**

2.1.2.25.23.1. Serviço escalável e seguro assegurando a replicação assíncrona dos dados armazenados no ambiente "on-premises" (local) para o ambiente de nuvem.

2.1.2.25.23.2. Deverá permitir a conexão de dispositivo de *software* local rodando no ambiente "on-premises" a um serviço gerenciado de armazenamento em nuvem assegurando a integração do ambiente local à infraestrutura de armazenamento do provedor de nuvem.

2.1.2.25.23.3. O dispositivo de *software* local (ou *gateway*) deverá ser implantado no ambiente "on-premises" como máquina física a ser entregue pela contratada/provedor, máquina virtual (VM) a ser hospedada na infraestrutura de virtualização VMware ESXi do contratante ou como instância computacional no ambiente de nuvem.

2.1.2.25.23.4. O dispositivo de *software* local deverá desempenhar o papel de *gateway* de armazenamento de arquivos ou volumes.

2.1.2.25.23.5. O *gateway* de armazenamento de arquivos deverá oferecer suporte a uma interface de arquivo no serviço de armazenamento de objetos garantindo o armazenamento e a recuperação de objetos por meio de protocolos de sistema de arquivos padrões de mercado tais como o Network File System (NFS) ou Server Message Block (SMB).

2.1.2.25.23.6. O *gateway* de armazenamento de arquivos deverá oferecer acesso a objetos no serviço de armazenamento de objetos como arquivos ou pontos de montagem de compartilhamento de arquivo.

2.1.2.25.23.7. O *gateway* de armazenamento de arquivos deverá oferecer acesso de baixa latência aos dados por meio de armazenamento em *cache* local transparente.

2.1.2.25.23.8. O *gateway* de armazenamento de arquivos deverá gerenciar a transferência de dados de/para ambiente de nuvem assegurando proteção contra congestionamentos de rede e otimizando o consumo de largura de banda.

2.1.2.25.23.9. O *gateway* de armazenamento de arquivos deverá possibilitar adicionar e excluir um compartilhamento de arquivos e editar configurações de acesso em compartilhamento de arquivos NFS ou SMB.

2.1.2.25.23.10. O *gateway* de armazenamento de volumes deverá fornecer volumes de armazenamento de dados em nuvem que poderão ser montados como dispositivos iSCSI ("Internet Small Computer System Interface") pelos servidores em operação no ambiente local.

2.1.2.25.23.11. O *gateway* de armazenamento de volumes deverá oferecer suporte a uma interface de bloco no serviço de armazenamento de objetos garatindo o armazenamento e a recuperação de dados por meio do protocolo iSCSI.

2.1.2.25.23.12. O *gateway* de armazenamento de volumes deverá permitir a criação de volumes de armazenamento e entregar tais volumes como dispositivos iSCSI aos servidores em operação no ambiente local.

2.1.2.25.23.13. O *gateway* de armazenamento de volumes deverá permitir o armazenamento local dos dados em *cache* garantindo o acesso de baixa latência aos dados acessados com frequência.

2.1.2.25.23.14. O *gateway* de armazenamento de volumes deverá possibilitar adicionar e excluir um volume, ampliar o tamanho de um volume e visualizar o uso do volume.

2.1.2.25.24. **Serviço de Diretório Gerenciado Integrado com o Microsoft Active Directory**

2.1.2.25.24.1. Deverá implementar serviço de diretório nativo do provedor de nuvem, serviço de diretório gerenciado baseado no Microsoft Active Directory (AD) ou fornecer conector para o serviço de diretório Microsoft Active Directory em operação no ambiente "on-premises" (local).

2.1.2.25.24.2. Deverá possibilitar o gerenciamento usuários, grupos e computadores.

2.1.2.25.24.3. Deverá permitir a criação e a aplicação de políticas de grupo.

2.1.2.25.24.4. Deverá assegurar logon único (SSO - "Single Sign On") em aplicativos e serviços.

2.1.2.25.24.5. Deverá assegurar uma identidade comum para concessão de acesso aos recursos no ambiente de nuvem e "on-premises".

2.1.2.25.24.6. O serviço de diretório gerenciado baseado no Microsoft Active Directory deverá ser criado como um par redundante de controladores de domínio conectados a redes privadas e serem executados em diferentes zonas de disponibilidade possibilitando a configuração de relação de confiança com instância do serviço de diretório Microsoft Active Directory em operação no ambiente "on-premises" com autenticação SSO.

2.1.2.25.24.7. O conector para o serviço de diretório Microsoft Active Directory em operação no ambiente "on-premises" poderá empregar 2 (dois) modos de integração com os serviços de diretório em operação no ambiente de nuvem:

2.1.2.25.24.7.1. Deverá atuar como *gateway* de diretório redirecionando solicitações para o serviço de diretório Microsoft Active Directory local sem armazenar nenhuma informação em *cache* no ambiente de nuvem, conectando ao serviço de diretório existente e assegurando que todos os dados do diretório permaneçam nos controladores de domínio visto que não replica nenhum dos dados do serviço de diretório.

2.1.2.25.24.7.2. Alternativamente, deverá permitir a sincronização do serviço de diretório Microsoft Active Directory em operação no ambiente "on-premises" com o

serviço de diretório remoto em operação no ambiente de nuvem, garantindo que as informações de identidade dos usuários e grupos armazenados no serviço de diretório Microsoft Active Directory do ambiente "on-premises" correspondam às informações armazenados no ambiente de nuvem e permitindo aos usuários alterar e redefinir suas senhas no ambiente de nuvem e ter sua política de senha local aplicada.

2.1.2.25.25. **Serviço de Auditoria e Análise de Logs**

2.1.2.25.25.1. Serviço gerenciado tipo "serverless" que permite coleta e análise de dados de monitoramento dos serviços de nuvem provendo visibilidade na utilização de recursos e no desempenho de aplicações.

2.1.2.25.25.2. Deverá permitir a coleta e a monitoria em tempo real de indicadores de desempenho permitindo medir e avaliar o consumo de recursos por meio do emprego de um repositório de métricas.

2.1.2.25.25.3. Deverá permitir a criação de painéis exibindo as métricas coletadas sobre os recursos consumidos.

2.1.2.25.25.4. Deverá permitir a criação de alarmes que observem métricas e enviem notificações quando um limite é violado.

2.1.2.25.25.5. Deverá permitir a construção de consultas para analisar os dados coletados.

2.1.2.25.25.6. Deverá permitir o armazenamento dos *logs* por pelo menos 1 (um) ano.

2.1.2.25.25.7. Deverá fornecer dados para elaborar ações de correção ou melhorias nas aplicações.

2.1.2.25.25.8. Deverá fornecer visibilidade contínua do estado dos recursos, serviços e contas, permitindo o reconhecimento e remediação de problemas de disponibilidade ou desempenho.

2.1.2.25.26. **Serviço de Análise Preditiva e Criação de Modelo para Aprendizado de Máquina**

2.1.2.25.26.1. Deverá estar disponível serviço gerenciado de aprendizado de máquina para criação de modelos e geração de previsões.

2.1.2.25.26.2. Deverá permitir o emprego de instâncias computacionais configuradas especificamente para treinamento e validação estatística de modelos de ML com aceleração de hardware (NVIDIA GPUs ou similar) e barramento de alta velocidade (PCIe 3.0, NVIDIA NVLink ou similar) entre CPU e acelerador.

2.1.2.25.26.3. Deverá permitir análise de dados, treinamento de modelos e avaliação.

2.1.2.25.26.4. Deverá gerenciar toda a infraestrutura e os fluxos de trabalho necessários para executar e alterar a criação de modelos e a geração de previsões de "Machine Learning".

2.1.2.25.26.5. Deverá ser automaticamente escalável e gerenciado, não sendo necessária nenhuma administração da infraestrutura subjacente do provedor de nuvem.

2.1.2.25.26.6. Deverá possuir API de comunicação REST ou equivalente.

2.1.2.25.26.7. Deverá permitir previsões em tempo real.

2.1.2.25.26.8. Deverá prover infraestrutura de treinamento de aprendizado de máquina do tipo "serverless" sem que seja necessário o gerenciamento da infraestrutura do "framework" de ML.

2.1.2.25.26.9. Deverá suportar múltiplos "frameworks" de aprendizado de máquina, contemplando pelo menos TensorFlow, PyTorch, scikit e Apache MXNet.

2.1.2.25.26.10. Deverá ser complementado por APIs do tipo "serverless" escaláveis e resilientes que deverão implementar pelo menos as seguintes funcionalidades: tradução de linguagem escrita, conversão da linguagem falada para texto ("speech-to-text"), reconhecimento de imagens, reconhecimento ótico de caracteres (OCR - "optical character recognition") e processamento natural de linguagem incluindo suporte para chatbot.

2.1.2.25.26.11. Deverá reconhecer a fala em arquivos de áudio e transcrevê-la em texto para o idioma Português do Brasil (pt-BR).

2.1.2.25.26.12. Deverá permitir a criação de interfaces de conversa em aplicativo usando voz e texto assegurando o desenvolvimento de *chatbots* que convertem a fala de entrada em texto e compreendem a intenção do usuário.

2.1.2.25.27. **Serviço Gerenciado de Execução de Funções**

2.1.2.25.27.1. Deverá estar disponível serviço gerenciado de execução de funções do tipo "serverless" que permita executar códigos sem provisionamento ou gerenciamento de servidores em uma infraestrutura de computação de alta disponibilidade.

2.1.2.25.27.2. Deverá suportar a execução de código em resposta a eventos.

2.1.2.25.27.3. Deverá ser tarifado somente quando houver execução de código.

2.1.2.25.27.4. Deverá permitir a execução de funções nas tecnologias Java, C#, Node.js, Python e similares.

2.1.2.25.27.5. Deverá prover escalabilidade contínua permitindo que as funções sejam executadas em paralelo de tal forma que para cada acionamento possa aumentar os recursos de acordo com o tamanho da carga de trabalho.

2.1.2.25.27.6. Deverá permitir o monitoramento das funções no nível da infraestrutura.

2.1.2.25.27.7. Deverá permitir a interação com as funcionalidades do serviço gerenciado via console, CLI, SDK ou API.

2.1.2.25.27.8. Deverá permitir a verificação de problemas para *debug* das funções.

2.1.2.25.28. **Serviço de Execução de Cargas de Trabalho de Computação em Lote**

2.1.2.25.28.1. Deverá ser gerenciado do tipo "serverless" permitindo a execução de cargas de trabalho de computação em lote de qualquer escala.

2.1.2.25.28.2. Deverá provisionar automaticamente recursos de computação e otimizar a distribuição da carga de trabalho com base na quantidade e porte das cargas de trabalho.

2.1.2.25.28.3. Deverá ser disponibilizado em várias zonas de disponibilidades.

2.1.2.25.28.4. Deverá permitir o envio de unidades de trabalho (como um script de shell, um executável do Linux ou uma imagem de contêiner do Docker) que serão processadas pelo serviço gerenciado.

2.1.2.25.28.5. Deverá permitir que seja especificado que tipos de instâncias computacionais serão empregadas na execução das unidades de trabalho incluindo o número mínimo, o número desejado e o número máximo de vCPUs para o ambiente computacional.

2.1.2.25.29. **Serviço de Cofre de Chaves**

2.1.2.25.29.1. Serviço para controle de chaves criptográficas e outros segredos usados por aplicativos e serviços baseado em dispositivo computacional do tipo módulo de segurança de hardware (HSM - "Hardware Security Module").

2.1.2.25.29.2. Deverá suportar configuração em alta disponibilidade via instanciação de *cluster* em várias zonas de disponibilidades mitigando o impacto de falha em nó HSM individual com *backups* periódicos do *cluster*.

2.1.2.25.29.3. Deverá permitir o *restore* do *cluster* de dispositivos HSM.

2.1.2.25.29.4. Deverá processar operações de criptografia e oferecer armazenamento seguro para chaves criptográficas.

2.1.2.25.29.5. Deverá empregar algoritmos simétricos e assimétricos para criptografar e descriptografar dados.

2.1.2.25.29.6. Deverá utilizar funções de *hash* criptográficas para computar resumos de mensagens e códigos de autenticação de mensagem baseados em *hash*.

2.1.2.25.29.7. Deverá gerar dados aleatórios seguros de forma criptográfica.

2.1.2.25.29.8. Deverá assinar dados de forma criptográfica (incluindo assinatura de código) e verificar assinaturas.

2.1.2.25.29.9. Deverá gerar, armazenar, importar, exportar e gerenciar chaves criptográficas, incluindo chaves simétricas e pares de chaves assimétricas.

2.1.2.25.29.10. Deverá criptografar chaves e segredos, como chaves de autenticação, chaves de conta de armazenamento, chaves de criptografia de dados e senhas.

2.1.2.25.29.11. Deverá prover cliente instalado e executado nas instâncias computacionais que estabelece uma conexão criptografada com o *hardware* do HSM.

2.1.2.25.29.12. Deverá permitir usuários ou aplicativos a acessarem o serviço permitindo o gerenciamento de chaves e segredos.

2.1.2.25.29.13. Deverá permitir a interação com as funcionalidades do serviço gerenciado via console, CLI, SDK ou API.

2.1.2.25.29.14. Deverá fornecer o *log* de uso das chaves e segredos.

2.1.2.25.30. **Serviço Gerenciado de Certificados Digitais**

2.1.2.25.30.1. Deverá permitir a emissão de certificados digitais X.509 v3 públicos com raíz internacional e privados do tipo servidor (FQDN), curinga ("wildcard") e multidomínios ("subject alternative name") com suporte a chaves assimétricas RSA de 2.048 bits e resumo SHA-256.

2.1.2.25.30.2. Deverá permitir a renovação automática dos certificados X.509.

2.1.2.25.30.3. Deverá permitir a importação e a exportação dos certificados X.509.

2.1.2.25.30.4. Deverá permitir a revogação dos certificados X.509.

2.1.2.25.30.5. O certificado X.509 deverá suportar as extensões "Basic Constraints", "Authority Key Identifier", "Key Usage", "Extended Key Usage" e "CRL Distribution Points".

2.1.2.25.30.6. O certificado X.509 emitido deverá ser confiável pelos principais navegadores, incluindo Google Chrome, Microsoft Internet Explorer e Microsoft Edge, Mozilla Firefox e Apple Safari.

2.1.2.25.31. **Serviço de Gerenciamento de Segredos para Aplicações e APIs**

2.1.2.25.31.1. Deverá ser gerenciado do tipo "serverless" garantindo a gestão de segredos tais como credenciais de banco de dados, senhas, chaves de API e até mesmo texto arbitrário ao invés de incorporar tais segredos diretamente no aplicativo ou API.

2.1.2.25.31.2. Deverá substituir credenciais codificadas por uma chamada autenticada em tempo de execução de API fornecida pelo provedor em nuvem por meio de solicitação de consulta HTTP permitindo a recuperação do segredo via programação e garantindo que esse não seja comprometido por meio de exame do código fonte.

2.1.2.25.31.3. Deverá permitir a substituição de segredos de longo prazo por segredos de curto prazo reduzindo o risco de vazamento.

2.1.2.25.31.4. Deverá prover o armazenamento dos segredos em banco de dados nativo ao serviço gerenciado ou equivalente.

2.1.2.25.31.5. Deverá permitir a criação, modificação, recuperação, exclusão e restauração de segredos.

2.1.2.25.31.6. Deverá criptografar o texto de um segredo e armazená-lo com segurança quando estiver em repouso por meio de integração com o serviço de gerenciamento de chaves ou similar.

2.1.2.25.31.7. Deverá armazenar a chave de dados criptografada com os dados do segredo protegidos.

2.1.2.25.31.8. Deverá possibilitar o versionamento dos segredos assegurando sua rotação automática por meio da alteração periódica do segredo no banco de dados dificultando que um invasor acesse o serviço protegido.

2.1.2.25.31.9. Deverá permitir a interação com as funcionalidades do serviço gerenciado via console, CLI, SDK ou API.

2.1.2.25.31.10. Deverá permitir o monitoramento e o registro em *log*.

2.1.2.25.32. **Serviço de Gerenciamento de Chaves**

2.1.2.25.32.1. Consiste em serviço gerenciado do tipo "serverless" que facilita a criação e o controle de chaves de criptografia que são protegidas pelo serviço de cofre de chaves permitindo manter controle sobre o uso das chaves mestras.

2.1.2.25.32.2. As chaves mestras deverão permitir a geração e a criptografia de chaves de dados que serão efetivamente empregadas nas aplicações *web* fornecidas em ambiente de nuvem para criptografar dados incluindo grandes quantidades de dados e outras chaves de criptografia de dados. Ou seja, as chaves mestras deverão criptografar as chaves de dados que deverão criptografar os dados.

2.1.2.25.32.3. Deverá possibilitar a criação, descrição, listagem, habilitação e desabilitação de chaves mestras.

2.1.2.25.32.4. Deverá permitir a ativação e desativação da rotação automática dos elementos criptográficos que compõem uma chave mestra.

2.1.2.25.32.5. Deverá suportar a criação, exclusão, listagem e atualização de aliases, ou seja, a atribuição de nomes amigáveis associados às chaves mestras.

2.1.2.25.32.6. Deverá permitir a exclusão de chaves mestras para concluir o ciclo de vida da chave.

2.1.2.25.32.7. As chaves mestras deverão permitir a realização das seguintes funções criptográficas:

2.1.2.25.32.7.1. Criptografar e descriptografar os dados.

2.1.2.25.32.7.2. Gerar chaves de criptografia de dados que poderão ser exportadas.

2.1.2.25.32.7.3. Gerar números aleatórios adequados para aplicativos de criptografia.

2.1.2.25.32.8. Deverá permitir a execução de solicitações remotas da API do serviço gerenciado por meio da apresentação de credenciais válidas para autenticar as solicitações com permissões expressamente atribuídas para tal finalidade.

2.1.2.25.32.9. Deverá permitir a interação com as funcionalidades do serviço gerenciado via console, CLI, SDK ou API.

2.1.2.25.32.10. Deverá permitir o monitoramento e o registro em *log*.

2.1.2.25.33. **Serviço de Web Aplication Firewall**

2.1.2.25.33.1. Serviço de *firewall* para aplicações *web* que fornece proteção centralizada de aplicações contra ataques e tentativas de exploração de vulnerabilidades, permitindo a monitoria de requisições HTTP e HTTPS encaminhadas, controlando o acesso baseado em endereços IP e países que originaram a requisição, valores em cabeçalhos das requisições, *strings* específicas ou *string* que correspondem a padrões contidos em expressões regulares, tamanho das

requisições, presença de código SQL malicioso (SQL *injection*) ou de script suspeito (*cross-site scripting*).

2.1.2.25.33.2. Deverá fornecer proteção sem modificar o código de "back-end".

2.1.2.25.33.3. Deverá proteger aplicações *web* que estejam rodando em instâncias computacionais ou *containers.*

2.1.2.25.33.4. Deverá proteger aplicações *web* que estejam rodando atrás de um *gateway* de API ("API Gateway") ou de um balanceador de carga.

2.1.2.25.33.5. Deverá fornecer monitoramento das aplicações *web* contra ataques provendo funcionalidade de *log* em tempo real.

2.1.2.25.33.6. Deverá permitir a criação e a exclusão de listas de controle de acesso e de regras baseadas em endereços IP/expressões regulares/geolocalização que permitem, bloqueiam ou contabilizam requisições HTTP.

2.1.2.25.33.7. Deverá permitir personalização de regras e grupos de regras, a fim de atender as necessidades das aplicações e eliminar falsos positivos.

2.1.2.25.34. **Serviço de Proteção contra Ataques DDoS**

2.1.2.25.34.1. Deverá detectar e mitigar ataques volumétricos de negação de serviço distribuídos (DDoS) em camada 3 e camada 4.

2.1.2.25.34.2. Deverá detectar e mitigar ataques DDoS não volumétricos em camada 7.

2.1.2.25.34.3. Deverá permitir a escalação de eventos de DDoS para o time de resposta do provedor de nuvem.

2.1.2.25.34.4. Deverá permitir a criação de regras e listas de controle de acesso.

2.1.2.25.35. **Serviço de Avaliação de Vulnerabilidades**

2.1.2.25.35.1. Deverá avaliar o estado da segurança das aplicações disponibilizadas no ambiente de nuvem quanto a exposição, vulnerabilidades e desvios das melhores práticas, gerando listagem detalhada dos problemas de segurança encontrados por nível de gravidade contendo descrições detalhadas dos problemas de segurança e recomendações para resolvê-los.

2.1.2.25.35.2. Deverá automatizar avaliações periódicas de vulnerabilidade de segurança.

2.1.2.25.35.3. Deverá permitir a utilização de agente instalado no sistema operacional das instâncias computacionais que monitorem o tráfego de rede, o sistema de arquivos e as atividades realizadas pelos processos em tempo de execução, coletando um amplo conjunto de dados de comportamento e configuração (telemetria).

2.1.2.25.35.4. Deverá ser compatível com sistemas operacionais Windows e Linux.

2.1.2.25.35.5. Deverá permitir o monitoramento e o registro em *log*.

2.1.2.25.36. **Serviço de Banco de Dados Relacional Gerenciado**

2.1.2.25.36.1. Deverá ser do tipo "serverless" escalável e resiliente suportando o emprego de redes virtuais com endereços IP privados em modalidade PaaS.

Alternativamente, deverá permitir o emprego de bancos de dados relacional em modalidade IaaS.

2.1.2.25.36.2. Deverá permitir a criação de instâncias que suportem mecanismos de bancos de dados relacionais "open-source" em modalidade PaaS. Alternativamente, deverá permitir o emprego de bancos de dados relacionais "open-source" em modalidade IaaS.

2.1.2.25.36.3. Deverá permitir a criação de instâncias que suportem mecanismos de bancos de dados relacionais proprietários. Alternativamente, deverá permitir o emprego de bancos de dados relacionais proprietário em modalidade IaaS.

2.1.2.25.36.4. Deverá permitir que as instâncias de bancos de dados possam empregar pelo menos três tipos de armazenamento em disco: magnético, SSD de uso geral e SSD com IOPS provisionado.

2.1.2.25.36.5. Deverá suportar a criação de instâncias de banco de dados com até 5 TiB de armazenamento.

2.1.2.25.36.6. Deverá suportar o uso de grupos de segurança ("security groups") controlando o acesso a uma instância de banco de dados por intervalos de endereços IP ou por instâncias computacionais.

2.1.2.25.36.7. Deverá suportar configuração em alta disponibilidade via instanciação de *cluster* em várias zonas de disponibilidades.

2.1.2.25.36.8. Deverá permitir a criação de *cluster* com pelo menos 3 (três) réplicas assíncronas assegurando que todas as gravações sejam efetuadas em uma instância principal enquanto que leituras sejam efetuadas tanto na instância principal quanto nas réplicas (*standby*) proporcionando escalabilidade de leitura.

2.1.2.25.36.9. Deverá possibilitar o *failover* manual de uma instância primária para uma réplica em *standby*.

2.1.2.25.36.10. Deverá suportar criptografia dos objetos no armazenamento ("in rest") e/ou na transferência ("in transit").

2.1.2.25.36.11. Deverá possibilitar *backup* manual e/ou automáticos dos dados.

2.1.2.25.37. **Serviço Gerenciado de "Data Warehouse"**

2.1.2.25.37.1. Serviço de "data warehouse" rápido e escalável que permita a análise de dados usando ferramentas SQL padrão e ferramentas de BI existentes.

2.1.2.25.37.2. Deverá ser do tipo "serverless" escalável e resiliente compatível com o padrão ANSI SQL e com drivers ODBC e JDBC.

2.1.2.25.37.3. Deverá permitir a execução otimizada de consultas SQL por meio do uso da técnica de processamento paralelo em massa ("Massively Parallel Processing" - MPP) distribuindo a carga de trabalho entre vários nós e assegurando a execução eficiente de consultas complexas que utilizam grandes volumes de

dados empregando vários nós de computação que realizam todo o processamento de consultas agregando o resultado final em cada nó.

2.1.2.25.37.4. Deverá suportar o armazenamento colunar para tabelas de bancos de dados reduzindo os requisitos de E/S de disco e diminuindo a quantidade de dados a ser carregada do disco.

2.1.2.25.37.5. Deverá pemitir a compactação de dados reduzindo requisitos de armazenamento e diminuindo a E/S de disco melhorando o desempenho da consulta.

2.1.2.25.37.6. Deverá implementar otimizador de consultas baseado no uso da técnica de processamento paralelo.

2.1.2.25.37.7. Deverá armazenar em memória *cache* os resultados de consultas SQL visando reduzir o tempo de execução da consulta e melhorar o desempenho do sistema.

2.1.2.25.37.8. Deverá suportar o uso de grupos de segurança ("security groups") controlando o acesso a uma instância de banco de dados por intervalos de endereços IP ou por instâncias computacionais.

2.1.2.25.37.9. Deverá suportar configuração em alta disponibilidade via instanciação de *cluster* em várias zonas de disponibilidades.

2.1.2.25.37.10. Deverá permitir a execução de operações de carga e descarga de dados em paralelo.

2.1.2.25.37.11. Deverá possibilitar *backup* manual e/ou automáticos dos dados.

2.1.2.25.38. **Serviço de Banco de Dados não Relacional Gerenciado**

2.1.2.25.38.1. Deverá ser do tipo "serverless" rápido e resiliente para aplicações que necessitem de escalabilidade e baixa latência.

2.1.2.25.38.2. Deverá permitir o emprego de bancos de dados não relacionais "open-source" e proprietário.

2.1.2.25.38.3. Deverá ser compatível com MongoDB ou plataforma NoSQL equivalente.

2.1.2.25.38.4. Deverá ser baseado nos mecanismos de armazenamento chave-valor, documento e/ou colunar suportando *backups* automáticos sem disrupção das operações de banco de dados.

2.1.2.25.38.5. Deverá permitir a criação de *cluster* com pelo menos 3 (três) réplicas (*standby*) assegurando que todas as gravações sejam efetuadas em uma instância principal enquanto que leituras sejam efetuadas tanto na instância principal quanto nas réplicas proporcionando escalabilidade de leitura.

2.1.2.25.38.6. Deverá possibilitar a replicação de dados de forma automática entre zonas de disponibilidades de pelo menos uma mesma região geográfica, com o intuito de oferecer alta disponibilidade e durabilidade dos dados.

2.1.2.25.38.7. Deverá possibilitar o *failover* manual de uma instância primária para uma réplica em *standby*.

2.1.2.25.38.8. Deverá suportar criptografia dos bancos de dados no armazenamento ("in rest").

2.1.2.25.39. **Serviço de Migração de Banco de Dados**

2.1.2.25.39.1. Deverá possibilitar a migração de bancos de dados relacionais, "data warehouses", bancos de dados NoSQL e outros tipos de armazenamentos de dados do ambiente "on-premises" para o ambiente de nuvem ou entre diferentes tecnologias de bancos de dados no ambiente de nuvem.

2.1.2.25.39.2. Deverá ser compatível com mecanismos DBMS ("Database Management Systems") populares como fontes de dados, incluindo Oracle, Microsoft SQL Server, MySQL, MariaDB, PostgreSQL e MongoDB.

2.1.2.25.39.3. Deverá disponibilizar uma variedade de mecanismos DBMS de destino disponíveis, incluindo PostgreSQL, MySQL e bancos proprietários do provedor de nuvem.

2.1.2.25.39.4. Deverá permitir migrações individuais e replicar as alterações em andamento para manter as origens e os destinos em sincronia.

2.1.2.25.39.5. Deverá assegurar a migração de qualquer uma das fontes de dados para qualquer um dos destinos de dados oferecendo suporte a migrações de dados heterogêneas entre mecanismos/tecnologias de bancos de dados compatíveis.

2.1.2.25.39.6. Deverá garantir que a migração dos dados seja segura criptografando os dados tanto em repouso quanto em trânsito enquanto trafegam da origem para o destino.

2.1.2.25.39.7. Deverá permitir a criação de uma conexão de origem e de destino para informar de onde extrair e para onde carregar os dados bem como a criação de uma tarefa para mover os dados e a criação de tabelas e chaves primárias associadas se ainda não existirem no destino, ou manualmente no destino.

2.1.2.25.39.8. Deverá possibilitar a migração de bases de origem e destino que usam o mesmo mecanismo/tecnologia de banco de dados ou de bases de origem e de destino que usam mecanismos/tecnologias de banco de dados diferentes.

2.1.2.25.39.9. Deverá garantir alta disponibilidade e suporte a *failover* usando técnicas baseadas em múltiplas zonas de disponibilidade.

2.1.2.25.39.10. Deverá fornecer *failover* automático assegurando que um servidor de replicação de *backup* (*standby*) possa assumir com pouca ou nenhuma interrupção do serviço caso o servidor de replicação primário venha a falhar.

2.1.2.25.40. **Serviço de Análise de Dados**

2.1.2.25.40.1. Deverá ser gerenciado do tipo "serverless" escalável e resiliente simplificando a execução de "frameworks" de "Big Data" tais como o Apache Hadoop e o

Apache Spark para processar e analisar grandes quantidades de dados fornecendo um modelo de programação e estrutura de *cluster* para o processamento de cargas de trabalho.

2.1.2.25.40.2. Deverá permitir o uso de "frameworks" e projetos de código-fonte "open source" relacionados tais como Apache Hive e Apache Pig assegurando processar dados para fins de análises e cargas de trabalho.

2.1.2.25.40.3. Deverá ser composto por conjuntos de *clusters* Apache Hadoop/HBase/Spark com armazenamento HDFS ("Hadoop Distributed File System") ou tecnologia equivalente.

2.1.2.25.40.4. Deverá permitir o processamento de quantidades consideráveis de dados por meio do emprego de "framework" "open source" baseado em Java ou equivalente suportando aplicações distribuídas em *clusters*.

2.1.2.25.40.5. Cada *cluster* deverá ser composto por uma coleção de nós (instâncias computacionais).

2.1.2.25.40.6. Cada *cluster* deverá suportar o sistema de arquivos HDFS ou tecnologia equivalente.

2.1.2.25.40.7. Cada nó do *cluster* deverá desempenhar os seguintes papéis:

2.1.2.25.40.7.1. Nó principal: nó que gerencia o *cluster* executando componentes de *software* para coordenar a distribuição de dados e tarefas entre outros nós para processamento. O nó principal rastreia o *status* de tarefas e monitora a integridade do *cluster*. Cada *cluster* tem um nó principal, e é possível criar um *cluster* de nó único apenas com o nó principal.

2.1.2.25.40.7.2. Nó *core*: nó com componentes de *software* que executam tarefas e armazenam dados no HDFS do *cluster*. *Clusters* de vários nós têm pelo menos um nó *core*.

2.1.2.25.40.7.3. Nó de tarefa: nó com componentes de *software* que apenas executa tarefas e não armazena dados no HDFS.

2.1.2.25.40.8. Deverá suportar o modelo de programação de código-fonte aberto para computação distribuída Hadoop MapReduce ou equivalente simplificando o processo de desenvolvimento de aplicativos distribuídos em paralelo e manipulando toda a lógica enquanto que o desenvolvedor deve apenas escrever as funções Map e Reduce ou equivalente. A função Map ou similar mapeia dados para conjuntos de pares de chave/valor chamados de resultados intermediários enquanto que a função Reduce ou similar combina os resultados intermediários, aplica algoritmos adicionais e produz o resultado final.

2.1.2.25.40.9. Deverá suportar o modelo de programação de código-fonte aberto para computação distribuída Spark ou equivalente empregando gráficos acíclicos

dirigidos para planos de execução e tirando proveito do armazenamento em *cache* na memória para conjuntos de dados.

2.1.2.25.40.10. Deverá permitir enviar trabalhos a um *cluster*.

2.1.2.25.40.11. Deverá possibilitar o ajuste do número de instâncias computacionais disponíveis para um *cluster* automaticamente ou manualmente, em resposta a cargas de trabalho com demandas variáveis, assegurando a escalabilidade de recursos do *cluster*.

2.1.2.25.40.12. Deverá conectar, visualizar, monitorar, clonar e encerrar um *cluster*.

2.1.2.25.41. **Serviço de Importação e Exportação de Dados**

2.1.2.25.41.1. Deverá ser baseado em dispositivo físico e/ou serviço virtualizado resistente contra violação com criptografia automática dos dados armazenados durante o transporte e apagamento dos dados na remessa.

2.1.2.25.41.2. Deverá permitir a importação e exportação dos dados por meio de requisição via console de gerenciamento web, CLI ou REST API, provendo capacidade de pelo menos 50 TB.

2.1.2.25.41.3. Deverá operar com tensão monofásica (P+N+T) nominal de 220 VCA e frequência nominal de 60 Hz, caso seja baseado em dispositivo físico.

2.1.2.25.41.4. Deverá possibilitar a leitura e gravação de dados por meio de compartilhamento NFS ou SMB publicado na infraestrutura de conectividade "on premise" disponibilizando pelo menos 1 (uma) interface de rede Ethernet 10 Gigabit SFP+, caso seja baseado em dispositivo físico.

2.1.2.25.41.5. Deverá possibilitar o emprego de endereço IP estático ou dinâmico (DHCP) a ser provido pela infraestrutrura de conectividade "on-premises", caso seja baseado em dispositivo físico.

2.1.2.25.42. **Serviço de Indexação e Pesquisa de Documentos**

2.1.2.25.42.1. Serviço para indexação de informações com algoritmo de índice textual e mecanismo de busca semântica.

2.1.2.25.42.2. Deverá permitir a indexação e consulta de dados não estruturados sem que faça necessário sua conversão para formatos intermediários tais como XML ou JSON por exemplo.

2.1.2.25.42.3. Deverá permitir o uso de linguagem de programação baseada em requisição HTTP, REST API ou mecanismo equivalente, provendo métodos para pesquisa programática de documentos.

2.1.2.25.42.4. Deverá possibilitar integração com Kibana e Logstash ou pilhas de *software* equivalentes.

2.1.2.25.43. **Serviço de Cache em Memória**

2.1.2.25.43.1. Serviço de cache em memória gerenciado que deverá ser baseado nas plataformas Memcached, Redis ou equivalente.

2.1.2.25.43.2. Deverá assegurar o armazenamento de chaves/valores em memória fornecendo acesso com baixa latência a cópias de dados e resultados de consultas efetuadas em instâncias de bancos de dados.

2.1.2.25.43.3. Deverá suportar configuração em alta disponibilidade via instanciação de *cluster* em várias zonas de disponibilidades e/ou regiões com pelo menos 3 (três) nós mitigando o impacto de falha em nó individual.

2.1.2.25.43.4. Deverá suportar a replicação de chaves/valores no caso de serviço gerenciado baseado na plataforma Redis, caso aplicável, com um nó funcionando como nó primário de leitura/gravação enquanto que todos os outros nós funcionam como réplicas somente leitura do nó primário dentro de um dado grupo de replicação.

2.1.2.25.43.5. Deverá suportar criptografia dos dados transferidos na rede ("in transit").

2.1.2.25.44. **Serviço de Gateway de API**

2.1.2.25.44.1. Deverá ser do tipo "serverless" escalável e resiliente implementando mecanismo de proteção baseado em políticas que atue como intermediário ("proxy") na invocação de chamadas de API remotas provenientes de aplicações.

2.1.2.25.44.2. Deverá processar todas as tarefas envolvidas na aceitação e no processamento de chamadas de API simultâneas, incluindo gerenciamento de tráfego, autorização e controle de acesso, monitoramento e gerenciamento de versão da API.

2.1.2.25.44.3. Deverá atuar como uma "porta de entrada" para os aplicativos acessarem dados, lógica de negócios ou funcionalidade dos serviços de "back-end" em execução no ambiente de nuvem.

2.1.2.25.44.4. Deverá suportar a disponibilização segura de APIs para desenvolvedores de aplicativos permitindo a criação de APIs baseadas nos protocolos HTTP e WebSocket incluindo invocação remota de métodos via REST API ou equivalente por meio da implementação dos métodos HTTP padrão (GET, POST, PUT, PATCH e DELETE).

2.1.2.25.44.5. Deverá permitir a criação, a compilação, a publicação e a invocação de APIs.

2.1.2.25.44.6. Deverá controlar o acesso a uma API usando as políticas de recursos baseadas em usuários de uma determinada conta, intervalos de endereços IP ou blocos CIDR de determinada origem e redes privadas virtuais.

2.1.2.25.44.7. Deverá suportar pelo menos o padrão OAuth 2.0 e implementar mecanismo de "traffic-shaping" ou similar.

2.1.2.25.44.8. Deverá permitir a interação com as funcionalidades do serviço gerenciado via console, CLI, SDK ou API.

2.1.2.25.44.9. Deverá permitir o monitoramento e o registro em *log*.

2.1.2.25.45. **Serviço de Mensageria Assíncrona**

2.1.2.25.45.1. Deverá ser serviço gerenciado do tipo "serverless" escalável e resiliente que implemente mecanismo de fila de mensagens baseado em processamento paralelo assíncrono e distribuído.

2.1.2.25.45.2. Deverá permitir que aplicativos se comuniquem usando várias linguagens de programação, sistemas operacionais e protocolos de mensageria.

2.1.2.25.45.3. Deverá permitir o emprego de sistemas de mensageria "open-source" ou proprietário.

2.1.2.25.45.4. Deverá suportar o envio de mensagens com pelo menos de 64 kilobytes de tamanho.

2.1.2.25.45.5. Deverá suportar o recebimento de pelo menos 1.000 mensagens por segundo assegurando sua durabilidade por meio de técnicas baseadas em armazenamento redundante.

2.1.2.25.45.6. Deverá permitir a criação, modificação e exclusão de filas de mensagens.

2.1.2.25.45.7. Deverá possibilitar a produção e o consumo de mensagens.

2.1.2.25.45.8. Deverá permitir o transporte de eventos em modalidade "many-to-many" (n produtores x n consumidores) suportando pelo menos um dos padrões arquiteturais via RESTful API (HTTP ou HTTPS): "queues/topics", "point-to-point", "publish/subscribe".

2.1.2.25.45.9. Deverá possibilitar o envio de mensagens para outros serviços disponibilizados em ambiente de nuvem computacional, aplicativos móveis, dispositivos habilitados para SMS ("Short Message Service") ou endereços de *e-mail*.

2.1.2.25.45.10. Deverá permitir o monitoramento e o registro em *log*.

2.1.2.25.46. **Serviço de Entrega de Mensagem Eletrônica**

2.1.2.25.46.1. Deverá ser gerenciado do tipo "serverless" escalável baseado no protocolo SMTP ("Simple Mail Transfer Protocol").

2.1.2.25.46.2. Deverá permitir integração com servidores SMTP em operação no ambiente "on-premises" do contratante (Postfix e Exchange) e com outros serviços gerenciados no ambiente de nuvem.

2.1.2.25.46.3. Deverá permitir o envio de mensagens programaticamente via linguagem de programação com interface para o protocolo SMTP e/ou via API/SDK do provedor de nuvem.

2.1.2.25.46.4. Deverá suportar o uso de registros SPF ("Sender Policy Framework") permitindo publicar uma lista de servidores SMTP autorizados a enviar mensagens na configuração de DNS do domínio registrado do contratante.

2.1.2.25.46.5. Deverá possibilitar o uso do padrão DKIM ("DomainKeys Identified Mail") permitindo que as mensagens eletrônicas sejam assinadas com uma chave criptográfica assegurando que não sejam alteradas em trânsito.

2.1.2.25.46.6. Deverá possibilitar a anexação de arquivos nas mensagens a serem enviadas.

2.1.2.25.46.7. Deverá permitir a recepção de mensagens via protocolo SMTP e a criação de regras de recebimento que definam seu destinatário.

2.1.2.25.46.8. Deverá permitir o monitoramento e o registro em *log*.

2.1.2.25.47. **Serviço de Codificação de Vídeo**

2.1.2.25.47.1. Deverá ser gerenciado do tipo "serverless" e seguro permitindo a conversão de arquivos de mídia armazenados no provedor de nuvem em arquivos de mídia nos formatos usados em dispositivos de reprodução dos usuários.

2.1.2.25.47.2. Deverá permitir a transcodificação de um arquivo para até 10 (dez) formatos de mídia de entrada e de saída.

2.1.2.25.47.3. Deverá possibilitar a transcodificação de arquivos por meio de requisição via console de gerenciamento e/ou via API REST.

2.1.2.25.47.4. Deverá enviar notificações ao término do processamento da transcodificação de arquivos.

2.1.2.25.47.5. Deverá suportar CODECs de áudio e de vídeo padrões de mercado.

2.1.2.25.47.6. Deverá suportar a união de vários arquivos de entrada para criar uma única saída.

2.1.2.25.47.7. Deverá permitir a inclusão de marcas d'água em um vídeo durante a transcodificação.

2.1.2.25.47.8. Deverá permitir a codificação de áudio digital em vários canais e faixas.

2.1.2.25.47.9. Deverá possibilitar a transcodificação de legendas de um formato para outro, devendo suportar que as legendas sejam incluídas no mesmo arquivo do áudio e do vídeo e/ou em arquivo de metadados separado dos dados de áudio e vídeo e assegurando o sincronismo do áudio digital e das legendas.

2.1.2.25.47.10. Deverá permitir o monitoramento e o registro em *log*.

2.1.2.25.48. **Serviço de Visualização de Mapas**

2.1.2.25.48.1. Deverá permitir a exibição de mapas como imagens (estáticos) e de mapas interativos e personalizáveis (dinâmicos), pesquisa de localização e localização de rotas por meio de disponibilização de API de mapeamento assegurando o desenvolvimento de aplicações baseadas em geolocalização.

2.1.2.25.48.2. Tal serviço poderá ser fornecido por qualquer provedor de serviços de computação em nuvem que componha a oferta do integrador, não sendo exigido que esse seja fornecido pelo provedor primário, o qual obrigatoriamente deverá atender integralmente (100%) todos os serviços relacionados na Tabela 1.

2.1.2.25.49. **Serviço de Identificação de Robôs**

2.1.2.25.49.1. Deverá empregar técnicas avançadas de análise para diferenciar humanos e *bots* e permitir a detecção de ataques automatizados originados de scripts, emuladores, *bots* ou até mesmo humanos.

2.1.2.25.49.2. Tal serviço poderá ser fornecido por qualquer provedor de serviços de computação em nuvem que componha a oferta do integrador, não sendo exigido que esse seja fornecido pelo provedor primário, o qual obrigatoriamente deverá atender integralmente (100%) todos os serviços relacionados na Tabela 1.

2.1.2.25.50. **Serviço de Transmissão de Vídeos**

2.1.2.25.50.1. Deverá ser gerenciado do tipo "serverless" escalável e resiliente oferecendo *streamings* de vídeo seguros e confiáveis a uma grande variedade de dispositivos de reprodução e redes de entrega de conteúdo servindo como ponto de distribuição para entrega de conteúdo de mídia.

2.1.2.25.50.2. Deverá permitir a publicação de *streaming* de conteúdo de vídeo ao vivo de um dispositivo codificador de origem ("upstream system") em funcionamento no ambiente "on-premises" do contratante.

2.1.2.25.50.3. Deverá suportar redundância do fluxo de entrada de *streaming*, permitindo a existência de um *stream* primário (origem ativa) e de um *stream* secundário que recebe passivamente o conteúdo.

2.1.2.25.50.4. Deverá permitir legendas de entrada.

2.1.2.25.50.5. Deverá permitir que qualquer usuário disponibilize vídeos na rede mundial de computadores.

2.1.2.25.50.6. Deverá permitir que qualquer usuário realize a transmissão de vídeos em tempo real (ao vivo) na rede mundial de computadores.

2.1.2.25.50.6.1. Deverá permitir o acesso em tempo real, com ou sem autenticação, às transmissões de vídeos publicadas pelos usuários do contratante, permitindo que terceiros possam acessar as mesmas a partir do *site* corporativo do contratante (transmissão de sessões de julgamento, cerimônias diversas, etc).

2.1.2.25.50.7. Deverá possibilitar o uso de câmeras de vídeo variadas, sem exigência de equipamentos específicos ou certificados pelo provedor.

2.1.2.25.50.8. Deverá permitir a utilização de diferentes taxas de transmissão no acesso aos vídeos publicados no ambiente de nuvem.

2.1.2.25.50.9. Deverá suportar pelo menos os seguintes formatos: MP4, MPEG, WMV, AVI, MOV.

2.1.2.25.51. **Serviço de Compartilhamento de Arquivos**

2.1.2.25.51.1. Deverá permitir que o usuário compartilhe documentos e controle as permissões de acessos em suas pastas e arquivos. Tal serviço poderá ser fornecido por qualquer provedor de serviços de computação em nuvem que componha a oferta do integrador, não sendo exigido que esse seja fornecido

pelo provedor primário, o qual obrigatoriamente deverá atender integralmente (100%) todos os serviços relacionados na Tabela 1.

2.1.2.25.51.2. Deverá suportar o armazenamento de arquivos de documentos nos padrões Microsoft Office ou BR Office/LibreOffice.

2.1.2.25.51.3. Deverá permitir a edição "on-line" de documentos armazenados na nuvem.

2.1.2.25.51.4. Cada usuário poderá armazenar até 5 GB, respeitada a utilização da sua cota total.

2.1.2.25.51.5. Estima-se o consumo mensal do quantitativo de cem (100) usuários.

2.1.2.26. Os valores máximos em USN de cada item da Tabela 1 foram computados por meio da obtenção do preço médio em dólar para cada serviço a partir de uma configuração padronizada em uma cesta de provedores de nuvem. Cabe enfatizar que o mecanismo de cálculo descrito nessa especificação técnica é meramente estimativo e visa apenas a explicitar o método utilizado pelo contratante para obtenção do valor máximo da USN que será pago para cada item. Considerando tal valor máximo, a contratada deverá realizar os seus próprios cálculos e estimar o valor da USN em sua proposta de preços de acordo com o modelo de negócios dos provedores de nuvem que serão ofertados e intermediados [5].

2.1.2.27. Em caráter ilustrativo segue no Anexo III a projeção do volume global e individual de serviços de computação multinuvem em USN que será consumido pelo contratante.

2.1.2.28. Por sua vez segue no Anexo VII a descrição do modelo de simulação que foi empregado na obtenção da estimativa preliminar dos serviços de computação em nuvem (item 1) e de suporte técnico especializado (item 2).

2.1.3. ESPECIFICAÇÕES TÉCNICAS DA INFRAESTRUTURA DE DATACENTER [6]

2.1.3.1. Os serviços de computação em nuvem a serem prestados deverão ser baseados em infraestrutura de *datacenter* que deverá manter compatibilidade com padrões internacionais durante toda a vigência do contrato.

2.1.3.2. As instalações físicas e recursos de infraestrutura que suportarão o ambiente crítico de serviços de computação em nuvem atenderão, no mínimo, ao conjunto de características a seguir definido relativo a instalações físicas, energia elétrica,

---

[5] Deve ser ressaltado que a estimativa dos valores máximos em USN dos itens contemplados na Tabela 1 se baseou na computação da média obtida em dólar por tipo de serviço de nuvem disponível no simulador público de preços dos provedores de nuvem AWS (https://aws.amazon.com/pricing/services), Azure (https://azure.microsoft.com/en-us/pricing/#product-pricing) e GCP (https://cloud.google.com/pricing/list).

[6] Tais requisitos deverão ser comprovados pelos provedores dos serviços de nuvem durante a execução contratual.

climatização, proteção contra incêndio, segurança física, infraestrutura de acesso a rede mundial de computadores do *datacenter* e segurança lógica do *datacenter*.

2.1.3.3. Tais requisitos deverão ser comprovados pelos provedores dos serviços de nuvem durante a execução contratual.

2.1.3.4. **Características Gerais**

2.1.3.4.1. Atender às exigências contempladas pela certificação TIA 942 TIER II devendo resumidamente implementar componentes redundantes em cada subsistema.

2.1.3.4.2. Os equipamentos de telecomunicações dos provedores de serviços bem como os equipamentos da operadoras de telecomunicações incluindo os comutadores Ethernet LAN e FC SAN deverão possuir módulos de conexão redundantes.

2.1.3.4.3. O cabeamento do *backbone* principal Ethernet LAN e FC SAN ou equivalentes das áreas de distribuição para os comutadores deverão prover cabeamento redundante em par metálico ou fibra.

2.1.3.4.4. É necessário prover sistemas UPS ("Uninterruptible Power Supply") redundantes em topologia N+1 e sistema de gerador elétrico redundante para suprir a carga.

2.1.3.4.5. O sistema de ar condicionado deverá ser projetado para assegurar o funcionamento contínuo em modalidade 24 x 7 x 365 com redundância de N+1.

2.1.3.4.6. O ambiente de *datacenter* deverá ser atendidos por no mínimo 2 operadoras de telecomunicações, tendo como pré-requisito que os cabos ingressem por rotas distintas.

2.1.3.5. **Instalações Físicas**

2.1.3.5.1. As instalações físicas deverão estar localizadas fora de zonas de risco, que não possuam incidentes de alagamentos, terremotos, tempestades que causaram danos físicos, e não poderão estar localizadas em rota de pouso e decolagem de aeronaves.

2.1.3.5.2. Os equipamentos utilizados para a prestação dos serviços tais como servidores, *blades*, *switches*, *storages* dentre outros deverão ser condicionados dentro de racks específicos para esta finalidade, com sistema de proteção contra descargas eletromagnéticas.

2.1.3.5.3. Deverão possuir estrutura física com piso elevado com no mínimo 3 camadas de cabeamento, com vias independentes para viabilizar a passagem de cabos de energia, ópticos e metálicos, o qual deverá suportar a carga mínima observada na norma TIA-942.

2.1.3.6. **Energia**

2.1.3.6.1. Garantir total independência no fornecimento de energia na eventualidade de falha na rede pública de fornecimento para manter o *datacenter* em pleno funcionamento.

2.1.3.6.2. Possuir transformador de energia elétrica de alta voltagem de uso dedicado do *datacenter*.

2.1.3.6.3. Empregar sistema de proteção contra descargas eletromagnéticas e aterramento garantindo equipotencialização de toda infraestrutura metálica que deverá estar interligada e devidamente aterrada.

2.1.3.6.4. Possuir sistema de grupo gerador redundante e independente, com acionamento automático na eventualidade de interrupção no fornecimento de energia da concessionária, com capacidade de funcionamento ininterrupto com combustível local em tanques próprios e abastecimento sem interrupção para autonomia mínima de 24 horas.

2.1.3.6.5. Utilizar sistema UPS redundante de grande porte com baterias para garantir a transição entre o fornecimento normal de energia e o grupo gerador garantindo alimentação elétrica redundante e independente para os equipamentos em operação no *datacenter*.

2.1.3.6.6. Empregar quadros e circuitos elétricos redundantes e independentes.

2.1.3.6.7. Possuir sistema de distribuição de energia totalmente gerenciado com suporte a administração web, agente SNMP e protocolo MODBUS.

2.1.3.7. **Climatização**

2.1.3.7.1. O ambiente do *datacenter* deverá possuir sistema de climatização que garanta as condições térmicas ideais para o funcionamento dos equipamentos no *datacenter*.

2.1.3.7.2. Manter em nível ideal e constante a temperatura, umidade relativa do ar e o controle de poluição do ar, mantendo controladas e administradas as possíveis variações, de acordo com o especificado para uso dos equipamentos em operação.

2.1.3.7.3. O sistema de climatização deverá possuir redundância, sendo que o sistema sobressalente deverá possuir a mesma capacidade que o sistema primário.

2.1.3.8. **Proteção contra Incêndio**

2.1.3.8.1. Possuir dispositivos de prevenção e combate a incêndio adequados ao tipo do ambiente e homologados pelo órgão fiscalizador competente.

2.1.3.8.2. Possuir dispositivos tradicionais de prevenção e combate a incêndio (brigada de incêndio, extintores manuais e detectores de fumaça).

2.1.3.8.3. Garantir a detecção eletrônica precoce de gases no ambiente do *datacenter* incluindo a área na parte inferior do piso elevado, quadros elétricos de distribuição e ar-condicionado, com sistema integrado de alarme monitorado por computador e acompanhado 24 x 7.

2.1.3.8.4. Deverá possuir preferencialmente sistema de supressão de fogo que utilize gás FM-200 ("heptafluoropropane") ou gás com propriedades de supressão superiores.

2.1.3.8.5. Os dispositivos automáticos de extinção de fogo não poderão danificar os equipamentos de TI devendo ser inertes e não tóxicos.

2.1.3.9. **Segurança Física**

2.1.3.9.1. Possuir equipe de segurança 24 x 7 x 365 com câmeras de vídeo em circuito fechado de TV (CFTV) monitoradas e gerenciadas que possibilitem o rastreamento de pessoas dentro do *datacenter*.

2.1.3.9.2. Prover armazenamento das imagens gravadas com retenção de pelo menos 30 (trinta) dias.

2.1.3.9.3. Garantir a disponibilidade de pessoas dedicadas, treinadas e responsáveis pela segurança de acesso ao prédio e aos equipamentos.

2.1.3.9.4. Possuir sistemas de detecção de tentativas de arrombamento e sensores de abertura de portas ou câmeras de vigilância (CFTV) para o acesso aos equipamentos de infraestrutura de energia elétrica em direção aos ambientes de geradores, *nobreaks* e entrada de energia no *datacenter*.

2.1.3.9.5. Possuir integração com sistema de alarme e ser monitorado em tempo integral.

2.1.3.9.6. Disponibilizar mecanismos efetivos de controle de entrada e de saída de pessoas que acessem e façam uso da infraestrutura física do ambiente de *datacenter*, bem como de registros passíveis de pesquisa.

2.1.3.9.7. Possuir travas eletrônicas que de acordo com a política de segurança estabelecida dividam a infraestrutura física do ambiente de *datacenter* em setores de acesso diferentes e com níveis de restrições diferenciados monitorando e verificando toda e qualquer tentativa de acesso.

2.1.3.9.8. O ambiente de datacenter deverá possuir no mínimo 3 (três) níveis de acesso controlado.

2.1.3.10. **Infraestrutura de Acesso à Internet do Datacenter**

2.1.3.10.1. Empregar protocolos de roteamento inteligentes com gerenciamento dinâmico e otimizado de múltiplos *links* com infraestrutura de rede dedicada assegurando maior desempenho e redundância.

2.1.3.10.2. Prover todos os equipamentos, infraestrutura, cabos de comunicação de dados, e demais acessórios com qualidade e dimensionamento adequados.

2.1.3.10.3. O tráfego interno deverá possuir conexões redundantes possibilitando monitoramento em diferentes pontos de interconexão.

2.1.3.10.4. A infraestrutura de rede deverá permitir qualquer tipo de aplicação através da rede mundial de computadores de tal forma que não poderão ser impostas restrições ao uso de quaisquer protocolos, aplicações, endereços, portas ou URLs.

2.1.3.10.5. A cobrança dos serviços de infraestrutura de rede deverá ser baseada no volume de dados efetivamente trafegados no sentido originado de recursos da infraestrura de nuvem em direção a destino não hospedado no ambiente de *datacenter* do provedor de serviços em nuvem, de tal forma que o tráfego no sentido inverso (de entrada) não poderá ser tarifado. Ou seja, apenas o tráfego de saída poderá ser cobrado.

2.1.3.11. **Segurança Lógica do Datacenter**

2.1.3.11.1. Detecção de intrusão para o acesso a rede mundial de computadores devendo proteger o perímetro de rede.

2.1.3.11.2. As políticas de segurança individuais e específicas de servidores virtuais deverão ser configuráveis via interface de acesso *web* ou via linha de comando.

2.1.3.11.3. No momento da ativação, os servidores virtuais deverão, por padrão, serem provisionados com as regras básicas de segurança do ambiente dos provedores de nuvem.

2.1.3.11.4. A partir do momento da configuração inicial o contratante poderá alterar e personalizar as regras conforme necessário.

2.1.3.11.5. Deverá ser disponibilizada interface de acesso *web* que permita ao contratante especificar requisitos de controle de acesso ao ambiente de computação em nuvem.

2.1.4. REQUISITOS TÉCNICOS DE SEGURANCA [7]

2.1.4.1. Segurança da Informação

[7] Tais requisitos deverão ser comprovados pelos provedores dos serviços de nuvem durante a execução contratual.

2.1.4.1.1. É vedado o tratamento em ambiente de nuvem de informações não autorizadas pelo contratante.

2.1.4.1.2. Deverão ser adotadas todas as medidas necessárias para assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações a serem armazenados e trafegadas no ambiente de nuvem.

2.1.4.1.3. Os serviços deverão contemplar plano de comunicação de incidentes, devendo ser informado imediatamente ao contratante todos os incidentes de segurança da informação ou existência de vulnerabilidades do objeto da contratação, assim considerados os eventos não previstos ou não desejados, bem como qualquer violação das regras de sigilo estabelecidas que tenham ocorrido por sua ação ou omissão, independentemente de dolo, que acarretem dano à confidencialidade, disponibilidade, integridade ou autenticidade dos dados do contratante.

2.1.4.1.4. Os serviços deverão contemplar análise e gestão de riscos de segurança de informação. A análise deverá ter periodicidade no mínimo mensal e deve ser apresentado um plano de gestão de riscos contendo: metodologia utilizada, riscos identificados, inventário e mapeamento dos ativos de informação, estimativa dos riscos levantados, avaliação, tratamento e monitoramento dos riscos, assunção ou não dos riscos e outras informações pertinentes.

2.1.4.1.5. Os provedores que integram os serviços ofertados deverão possuir plano de continuidade e de recuperação de desastres e contingência de negócio que possa ser testado regularmente, objetivando a disponibilidade dos dados e serviços em caso de interrupção, bem como desenvolver e colocar em prática procedimentos de respostas a incidentes relacionados com os serviços.

2.1.4.1.6. Os serviços deverão dispor de medidas para garantir a proteção dos dados, antecipando ameaças à privacidade, à segurança e à integridade, prevenindo acesso não autorizado às informações. Todavia, a responsabilidade dos provedores de serviços em nuvem e da contratada se limita diretamente às plataformas que fornecem os serviços contratados, conforme modelo padrão de responsabilidade compartilhada usualmente adotado em serviços de computação em nuvem.

2.1.4.1.7. É vedada a contratada ou ao provedor acesso aos dados hospedados na infraestrutura de nuvem, sem prévia e formal autorização por parte da contratante.

2.1.4.1.8. Os serviços deverão dispor de mecanismos para realizar regularmente testes de segurança da informação (incluindo análise e tratamento de riscos, verificação de vulnerabilidades, avaliação de segurança dos serviços e testes de penetração) podendo o contratante realizar auditorias para comprovar o atendimento do requisito.

2.1.4.1.9. Os serviços deverão prover mecanismo de acesso protegido aos dados por meio de chave de criptografia garantindo que apenas aplicações e usuários autorizados tenham acesso.

2.1.4.1.10. Os serviços deverão permitir a criptografia automática dos dados armazenados usando AES ("Advanced Encryption Standard") de no mínimo 256 bits ou outro algoritmo com força de chave equivalente ou superior.

2.1.4.1.11. Os serviços deverão possibilitar comunicação criptografada e protegida para transferência de dados.

2.1.4.1.12. Os provedores que integram a oferta da contratada deverão possuir pelo menos as certificações enumeradas a seguir com validade vigente na data de assinatura do contrato referentes à infraestrutura de *datacenter* no Brasil onde os serviços em nuvem estarão hospedados: ABNT NBR ISO/IEC 27001:2013, ABNT NBR ISO/IEC 27017:2016 [8] ou CSA STAR Certification LEVEL TWO ou superior e ISO/IEC 27018:2014 [9].

2.1.4.1.12.1. As certificações ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27017:2016 poderão ser apresentadas nas suas versões originais em inglês: ISO/IEC 27001:2013 e ISO/IEC 27017:2015.

2.1.4.1.12.2. Alternativamente e especificamente para a certificação ISO/IEC 27018:2014, a contratada poderá demonstrar que o provedor atende a todos os objetivos e controles dos itens 5 a 18 da referida norma, mediante apresentação de políticas, procedimentos e outros documentos pertinentes.

2.1.4.1.12.3. Qualquer documento deverá ser apresentado em nome do provedor, sendo facultado ao contratante promover diligência destinada a esclarecer ou complementar informações.

2.1.4.1.13. A contratada deverá fornecer, sempre que solicitado pelo contratante, cópias dos *logs* de segurança de todas as atividades de todos os usuários dentro da conta, além de histórico de chamadas de APIs para análise de segurança e auditorias.

2.1.4.1.14. Os serviços deverão dispor de recursos que garantam a segurança da informação dos dados do contratante, incluindo os seguintes itens: sistema de controle de tráfego de borda do tipo *firewall* (norte-sul, leste/oeste, e de aplicações), sistema de prevenção e detecção de intrusão (IDS/IPS) e sistema anti-DDoS. Entretanto, a responsabilidade dos provedores de serviços em nuvem e da contratada se limita diretamente às plataformas que fornecem os serviços contratados, conforme

---

[8] ABNT NBR ISO/IEC 27017:2016 - Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27002 para serviços em nuvem.

[9] ABNT NBR ISO/IEC 27018:2014 - Tecnologia da informação - Técnicas de segurança - Código de prática para proteção de informações de identificação pessoal (PII) em nuvens públicas que atuam como processadores de PII.

modelo padrão de responsabilidade compartilhada usualmente adotado em serviços de computação em nuvem.

2.1.4.1.15. Deverão ser implementados controles para isolamento e segurança de sistema operacional.

2.1.4.1.16. Deverá existir política de atualização de versão de *software*, indicando sua criticidade e acordar junto ao contratante qual a melhor data para ser aplicada.

2.1.4.1.17. A contratada comprometer-se-á a preservar os dados do contratante contra acessos indevidos e abster-se-á de replicar ou realizar cópias de segurança (*backups*) destes dados para fora do território brasileiro, devendo informar imediatamente e formalmente ao contratante qualquer tentativa de acesso a estes dados.

2.1.4.1.18. A partir do ponto de entrada/saída da Internet nos *datacenters* dos provedores ofertados deverão ser observadas as seguintes disposições:

2.1.4.1.18.1. Inviolabilidade e sigilo do fluxo de suas comunicações pela rede, salvo por ordem judicial, na forma da lei.

2.1.4.1.18.2. Inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial.

2.1.4.1.18.3. Não fornecimento a terceiros de dados do contratante, inclusive registros de conexão, e de acesso a aplicações de Internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei.

2.1.4.1.18.4. Fornecer ao contratante, sempre que solicitado, informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de dados do contratante.

2.1.4.1.19. Os dados, metadados, informações e conhecimento, tratados pelos provedores, não poderão ser fornecidos a terceiros e/ou usados por provedores para fins diversos do previsto nessa especificação técnica, sob nenhuma hipótese, sem autorização formal do contratante.

2.1.4.2. **Segurança de Identidades**

2.1.4.2.1. Os serviços deverão dispor de mecanismo de garantia de identidade realizada previamente à execução das requisições de acesso aos recursos por parte dos usuários.

2.1.4.2.2. Os serviços deverão permitir que somente os usuários autorizados pelo contratante tenham acesso aos recursos em conformidade com os respectivos perfis de uso.

2.1.4.2.3. Os serviços deverão permitir autenticação de usuário para controlar o acesso aos dados com base em listas de controle de acesso para conceder seletivamente permissões para usuários e grupos.

2.1.4.3. **Segurança nas Requisições/Dados**

2.1.4.3.1. Os serviços deverão permitir ou negar uma requisição baseada no endereço IP de origem do requisitante.

2.1.4.3.2. Os serviços deverão permitir que o contratante restrinja o acesso a determinados recursos com base em aspectos da requisição.

2.1.4.3.3. Os serviços deverão utilizar protocolos seguros para autenticar as requisições, por exemplo, HMAC ("Hash Message Authentication Code") - SHA1, conforme RFC 2104, utilizando codificação Base64.

2.1.4.3.4. Os serviços deverão permitir criar listas de controle de acesso (ACLs) para conceder permissões específicas (ou seja, READ, WRITE, FULL_CONTROL) a usuários específicos para um recurso.

2.1.4.4. **Segurança de Chaves**

2.1.4.4.1. Os serviços deverão dispor de mecanismo para gestão integrada de chaves de segurança que permita tratar, gerenciar e proteger chaves.

2.1.4.4.2. Os serviços deverão permitir a auditoria da segurança de chaves.

2.1.4.4.3. Os serviços deverão permitir que os usuários criptografem seus dados antes de enviá-los para o serviço de armazenamento.

2.1.4.4.4. Os serviços deverão permitir visualizar tentativas mal sucedidas de acesso por usuários sem permissão para descriptografar os dados.

2.1.4.4.5. Os serviços deverão permitir que cada recurso protegido seja criptografado com uma chave exclusiva.

2.1.4.4.6. Os serviços deverão permitir que a própria chave de recurso seja criptografada por uma chave separada.

2.1.4.4.7. Os serviços deverão permitir que chaves de criptografia e chaves mestras sejam armazenadas e protegidas com redundância.

2.2. SERVIÇOS DE SUPORTE TÉCNICO ESPECIALIZADO

2.2.1. DESCRIÇÃO SINTÉTICA DOS SERVIÇOS

2.2.1.1. Auxiliar na estratégia de seleção dos serviços de computação em nuvem baseados em estratégias do tipo migração de aplicações legadas ("lift and shift") e desenvolvimento de aplicações nativas no ambiente de nuvem ("cloud-first").

2.2.1.2. Apoiar na utilização de ferramentas nativas de gerenciamento (CLI, SDK e/ou API) dos serviços de nuvem pública.

2.2.1.3. Apoiar no processo de integração dos serviços de nuvem pública aos serviços "on-premises" assegurando a implantação de um ambiente de nuvem híbrido.

2.2.1.4. Projetar serviços de nuvem pública em ambiente híbrido e multinuvem garantindo a disponibilidade e a segurança dos serviços entregues ao contratante minimizando o efeito de "vendor lock-in".

2.2.1.5. Dimensionar o uso dos serviços e recursos em ambiente de nuvem demandados ou reduzir tais serviços e recursos quando superdimensionados assegurando a boa gestão do consumo dos recursos computacionais e o melhor desempenho das aplicações.

2.2.1.6. Elaborar comparativo de investimentos "on-premises" com o consumo de recursos em ambiente de nuvem com base em projeção de gastos por período.

2.2.1.7. Prover metodologias, estratégias e executar a migração de aplicações para o ambiente de nuvem.

2.2.1.8. Definir em conjunto com a área técnica do contratante a respeito dos serviços de infraestrutura e aplicações que poderão ser explorados no ambiente de nuvem pública.

2.2.1.9. Estabelecer metodologias de governança de uso dos recursos disponibilizados no ambiente de nuvem pública.

2.2.1.10. Definir estratégia de "self-service" no uso dos recursos disponibilizados no ambiente de nuvem pública.

2.2.1.11. Criar processo financeiro para analisar os custos mensais atuais/projetados relativos ao consumo de recursos no ambiente de nuvem pública.

2.2.1.12. Facilitar nos processos de gestão de risco e de segurança definindo controles e responsabilidades em conjunto com o contratante.

2.2.1.13. Assegurar a entrega e integração de serviços em ambiente híbrido e multinuvem.

2.2.1.14. Elaborar procedimento de automação e orquestração de cargas de trabalho no ambiente multinuvem.

2.2.1.15. Auxiliar na monitoria e otimização do consumo de recursos no ambiente de nuvem pública.

2.2.1.16. Apoiar na conectividade de rede do ambiente "on-premises" do contratante ao ambiente dos provedores de serviços em nuvem.

2.2.1.17. Viabilizar que os dados dos serviços em nuvem sejam armazenados no país em região global pelo menos no caso do principal provedor de serviços em nuvem ofertado.

2.2.1.18. Assessorar no projeto e na operação de serviços em nuvem hospedados em múltiplas zonas de disponibilidade e/ou regiões assegurando alta disponibilidade das aplicações

publicadas por meio do emprego de tecnologias nativas do ambiente de nuvem pública.

2.2.1.19. Garantir a alocação de recursos humanos qualificados e capacitados nas atividades de arquitetura e engenharia de serviços de nuvem.

2.2.1.20. Suportar o processo de migração dos serviços em nuvem ao término do contrato para novo ambiente de nuvem definindo um processo de saída de forma clara e objetiva visando a minimização do efeito de "vendor lock-in".

2.2.2. **DESCRIÇÃO ANALÍTICA DOS SERVIÇOS**

2.2.2.1. Os serviços listados na Tabela 3 constituem os serviços técnicos especializados que deverão ser prestados pela contratada.

2.2.2.2. Todos os serviços listados na Tabela 3 deverão ser executados nos ambientes de nuvem dos provedores que integram a oferta da contratada.

2.2.2.3. Os serviços poderão ser realizados de forma remota, incluindo treinamentos e reuniões. Entretanto, poderão ser executados em modalidade presencial, caso seja necessário, a ser decidido consensualmente entre contratada e contratante.

2.2.2.4. Os serviços técnicos especializados serão remunerados por meio de Unidades de Serviço Técnico (UST).

2.2.2.5. A unidade de medida adotada (UST) corresponde ao esforço padronizado para a execução de tarefa com determinada complexidade, independentemente da quantidade de recursos humanos alocados. O ateste e pagamento das USTs será condicionada a perferita execução dos serviços e ao atendimento dos níveis de serviços exigidos.

2.2.2.6. A contratada será responsável pela prestação dos serviços descritos nas ordens de serviço devendo utilizar pessoal técnico qualificado nos quantitativos adequados. A definição da composição de recursos, otimização de fluxos e/ou procedimentos são de responsabilidade da contratada.

2.2.2.7. O contratante fará uso e efetuará o pagamento apenas das USTs necessárias à implementação e manutenção dos serviços que solicitar à contratada até o limite máximo das USTs estimadas. O contratante não realizará pagamento prévio de USTs sob qualquer hipótese.

2.2.2.8. A equipe técnica do contratante poderá a qualquer tempo ativar ou desativar serviços, plataformas ou infraestrutura, provisionar e gerenciar recursos em nuvem, utilizando para isso a console de gerenciamento/CLI/SDK do provedor de serviços em nuvem sem o assessoramento ou autorização por parte da contratada.

2.2.2.8.1. As ações realizadas pela equipe técnica do contratante não poderão gerar ordens de serviços referentes à execução de serviços técnicos especializados (Tabela 3).

Nesse caso particular somente serão emitidas ordens de serviços relativas ao consumo dos recursos de computação em nuvem (Tabela 1) em decorrência das ações descritas no item 2.2.2.8.

2.2.2.9. A quantidade de USTs por serviços ofertados não poderá ser superior à quantidade de USTs definidas na Tabela 3.

2.2.2.10. Para fins de realização dos serviços especificados na Tabela 3 a contratada deverá disponibilizar recursos profissionais que estarão diretamente envolvidos na execução de cada ordem de serviço demandada pelo contratante. Tais profissionais deverão atender ao seguinte conjunto de perfis:

2.2.2.10.1. Possuir pelo menos 2 (dois) anos de experiência profissional na realização de atividades similares às descritas na Tabela 3.

2.2.2.10.2. Possuir curso superior completo nas áreas de Informática, Ciência da Computação, Engenharia da Computação, Análise de Sistemas, Sistemas de Informação, Engenharia de Software ou Ciências Exatas, ou qualquer outro curso superior combinado com curso de especialização na área de Informática com carga horária mínima de 360 (trezentos e sessenta) horas, ou curso de mestrado na área de Informática, comprovada por cópia do respectivo diploma, devidamente registrado, e fornecido por instituição de ensino superior reconhecida pelo MEC.

2.2.2.10.3. Possuir certificação ou experiência profissional de arquiteto de soluções, ou papel equivalente, relacionados ao provedor de nuvem (marca de nuvem pública) ou plataforma de nuvem (tecnologia de nuvem) no qual os serviços descritos nas ordens de serviço estiverem sendo executados (por exemplo, AWS Certified Solutions Architect, Azure Solutions Architect, Google Professional Cloud Architect, etc).

2.2.2.10.4. A experiência profissional exigida deverá ser comprovada por documentos válidos para tal fim (carteira de trabalho, contrato de prestação de serviços, declaração do empregador, contrato social no qual figure como sócio, dentre outros cenários de comprovação da vinculação do profissional à contratada), a serem fornecidos ao contratante na execução das ordens de serviço, e novamente fornecidos quando ocorrer a substituição dos profissionais em atuação. Todas as declarações deverão constar de forma clara o nome, endereço eletrônico (*e-mail*), telefone de contato e cargo/função do declarante.

2.2.2.10.5. As certificações exigidas pelo contratante deverão ser comprovadas pela empresa contratada por documentos fornecidos pelas entidades certificadoras ou instituições de ensino, e serem fornecidos novamente ao contratante quando ocorrer a substituição de profissionais em atuação.

2.2.2.10.6. Todos os documentos de comprovação de experiência profissional, formação e capacitação deverão ser apresentados em cópias autenticadas. Serão aceitas

cópias não autenticadas em caso de apresentação das mesmas juntamente com suas versões originais.

2.2.2.10.7. O contratante reserva-se ao direito de efetuar diligências junto aos emitentes ou declarantes dos documentos com a finalidade de elucidação de dúvidas ou comprovação de sua autenticidade.

2.2.2.10.8. Em casos de substituição dos provedores que integram os serviços ofertados, a contratada terá o prazo de até 2 (dois) meses para integrar ao atendimento do contratante um novo profissional com a devida capacidade comprovada no provedor ou plataforma de nuvem em questão.

2.2.2.10.9. A contratada deverá entregar ao contratante listagem dos profissionais a serem alocados antes do início da prestação dos serviços descritos em cada ordem de serviço bem como a qualquer momento em que haja substituição dos profissionais.

2.2.2.10.10. Caberá ao arquiteto de soluções a ser disponibilizado pela contratada a análise e definição dos cenários apropriados, execução dos procedimentos de configuração, migração/implantação, testes, colocação em produção e acompanhamento/monitoramento do serviço em produção.

2.2.2.10.11. São premissas básicas das atividades a serem realizadas pelos arquitetos de soluções no ambiente de nuvem pública fornecido pela contratada:

2.2.2.10.11.1. As aplicações do contratante provisionadas no ambiente de em nuvem deverão se manter portáveis entre diversos provedores, exceto se expressamente autorizado pelo contratante o uso de serviços proprietários de um dado provedor.

2.2.2.10.11.2. As aplicações do contratante provisionadas em nuvem deverão ter suas matrizes de riscos e planos de saída criados e/ou atualizados pelos arquitetos responsáveis pela execução de tais atividades.

2.2.2.11. As tarefas de Planejamento/Criação/Diagnóstico, Execução/Alteração/Implantação e Exclusão referentes aos serviços técnicos especializados listados na Tabela 3 serão cobradas com base em cada solicitação atendida.

2.2.2.12. Solicitações que possuam complexidade alta poderão ser decompostas em módulos menores para fins de solicitação. O contratante decidirá em conjunto com a contratada quais solicitações poderão ser subdivididas.

2.2.2.13. Ao final do contrato, a contratada será responsável pelo processo de migração para a infraestrutura da nova contratada, garantindo o funcionamento e níveis de serviços das aplicações e infraestruturas de produção. Entretanto, cabe salientar que tal demanda será realizada através da contratação de USTs específcas para tal finalidade e será classificada de acordo com a Tabela 3.

2.2.2.14. Os valores de referência UST especificados na Tabela 3 terão seu cômputo ajustado de acordo com a natureza da solicitação do contratante, conforme detalhado na tabela abaixo.

Tabela 2 - Natureza da Solicitação de Serviços Técnicos Especializados

Natureza da Tarefa	**Complexidade**	**Ajuste no Valor de Referência (Fator Multiplicador)**
Planejamento/Criação/Diagnóstico	Alta	1,5
Execução/Alteração/Implantação	Média	1,0
Exclusão	Baixa	0,5

2.2.2.15. A relação dos serviços de suporte técnico especializado constam da Tabela 3. Tais serviços não são exaustivos e indicam essencialmente itens básicos de serviço técnico especializado a ser prestado. Tais serviços deverão ser prestados pela contratada, e não pelo provedor de nuvem, diferentemente do suporte empresarial de que trata o item 2.4.3. A descrição detalhada dos serviços da Tabela 3 é conduzida a seguir.

2.2.2.16. Os valores em USTs relacionados na Tabela 3 já levam em consideração o fator multiplicador relacionado na Tabela 2.

2.2.2.17. Na Tabela 3 se encontram os níveis mínimos de serviço (NMS [10]) das ordens de serviços relativas ao planejamento/criação/diagnóstico (complexidade alta), de execução/alteração/implantação (complexidade média) e de exclusão (complexidade baixa).

2.2.2.18. A contratada quando demandada na criação de ambientes, implementação de aplicações ou serviços que envolvam estruturas de IaaS e PaaS, deverá utilizar racionalmente tanto USTs quanto USNs evitando desperdícios.

[10] Níveis mínimos de serviços são critérios objetivos e mensuráveis estabelecidos com a finalidade de aferir e avaliar fatores como qualidade, desempenho e disponibilidade dos serviços.

Tabela 3 - Serviços Técnicos Especializados

Item	Descrição do Serviço	Valor de Referência (em UST)	Complexidade	Valor (em UST)	Prazo Máximo de Finalização (em Horas Úteis)
1	Arquitetura de Solução em Nuvem	7	Alta Média	10,5 7	50 30
2	Configuração de Máquina Virtual	1	Alta Média Baixa	1,5 1 0,5	4 3 2
3	Configuração de VPN Site-to-Site	1,5	Alta Média Baixa	2,25 1,5 0,75	4 3 2
4	Configuração de Regra de Filtragem em Firewall	0,5	Alta Média Baixa	0,75 0,5 0,25	2 1 1
5	Configuração de Rede Virtual	0,5	Alta Média Baixa	0,75 0,5 0,25	4 2 1
6	Configuração de Sub-Rede de Rede Virtual	0,5	Alta Média Baixa	0,75 0,5 0,25	4 2 1
7	Configuração de IP Público	0,05	Média	0,05	1
8	Configuração de Domínio de DNS	1,5	Alta Média Baixa	2,25 1,5 0,75	4 2 1
9	Configuração de Balanceador de Carga	1,2	Alta Média Baixa	1,8 1,2 0,6	4 3 2
10	Configuração de Certificado SSL	0,5	Alta Média Baixa	0,75 0,5 0,25	4 2 1
11	Configuração de Disco Customizado de Sistema Operacional de Máquina Virtual	1	Alta Média Baixa	1,5 1 0,5	5 3 2
12	Configuração de Disco com Provisionamento de IOPS	0,5	Alta Média Baixa	0,75 0,5 0,25	2 1 1
13	Criptografia de Dados e Discos	1	Alta Média Baixa	1,5 1 0,5	4 2 1
14	Configuração de Sistema de Arquivos em Rede	2	Alta Média Baixa	3 2 1	4 2 1
15	Implantar Serviço de Backup	0,5	Alta Média Baixa	0,75 0,5 0,25	2 1 1
16	Configuração de Escalabilidade Automática (*Autoscaling*)	1	Alta Média Baixa	1,5 1 0,5	5 3 2
17	Hospedagem de *Containers*	1,5	Alta Média Baixa	2,25 1,5 0,75	5 3 2
18	Migração de Ambientes ao Término do Contrato	6	Alta Média Baixa	9 6 3	14 10 2
19	Serviço de Aplicações Gerenciadas	4	Alta Média Baixa	6 4 2	8 6 2
20	Serviço de Banco de Dados Gerenciado	2	Alta Média Baixa	3 2 1	7 4 2
21	Serviço de Gerenciamento de Cache em Memória	1,5	Alta Média Baixa	2,25 1,5 0,75	4 3 2
22	Configuração de Gestão de Identidade,	0,5	Alta	0,75	2

	Permissões e Acessos		Média Baixa	0,5 0,25	1 1
23	Configuração de Operação Assistida	4	Alta Média Baixa	6 4 2	20 15 10
24	Serviço de Monitoramento	0,25	Alta Média Baixa	0,38 0,25 0,13	2 1 1
25	Arquitetura On-Premises	6	Alta Média Baixa	9 6 3	40 20 5
26	Implantar Cofre de Senhas	1	Alta Média Baixa	1,5 1 0,5	2 1 1
27	Configuração de Serviço de Autenticação Integrado com Microsoft ADS	1,5	Alta Média Baixa	2,25 1,5 0,75	16 8 4
28	Implantação de Auditoria e Análise de Logs	0,5	Alta Média Baixa	0,75 0,5 0,25	4 2 1
29	Configuração de Sistema de Objetos	2	Alta Média Baixa	3 2 1	4 2 1
30	Configuração de Gateway NAT	0,5	Alta Média Baixa	0,75 0,5 0,25	4 2 1
31	Serviço Gerenciado de Data Warehouse	2	Alta Média Baixa	3 2 1	15 10 5
32	Serviço de Banco de Dados não Gerenciado	2	Alta Média Baixa	3 2 1	7 4 2
33	Configuração de Firewall de Aplicação W*eb*	0,5	Alta Média Baixa	0,75 0,5 0,25	4 3 2
34	Configuração de Proteção contra Ataques DDOS	0,5	Alta Média Baixa	0,75 0,5 0,25	4 3 2
35	Serviço de Indexação e Pesquisa de Documentos	1,5	Alta Média Baixa	2,25 1,5 0,75	4 3 2
36	Serviço de Análise Preditiva e Criação de Modelo para Aprendizado de Máquina	3	Alta Média Baixa	4,5 3 1,5	30 20 10
37	Serviço de Avaliação de Vulnerabilidades	0,5	Alta Média Baixa	0,75 0,5 0,25	7 4 2
38	Serviço Gerenciado de Execução de Funções	1	Alta Média Baixa	1,5 1 0,5	5 3 2
39	Serviço de Migração de Banco de Dados	2	Alta Média Baixa	3 2 1	10 5 2
40	Serviço de Gateway de API	1	Alta Média Baixa	1,5 1 0,5	4 3 2
41	Serviço de Mensageria Assíncrona	0,5	Alta Média Baixa	0,75 0,5 0,25	4 3 2
42	Serviço de Entrega de Mensagem Eletrônica	0,5	Alta Média Baixa	0,75 0,5 0,25	2 1 1
43	Implantação de Infraestrutrura de Serviços "On-Promises"	4	Alta Média Baixa	6 4 2	40 20 10
44	Serviço de Análise de Dados	2	Alta Média Baixa	3 2 1	15 10 5
45	Serviço de Importação e Exportação de	1,5	Alta	2,25	10

	Dados		Média Baixa	1,5 0,75	5 2
46	Serviço de Execução de Cargas de Trabalho de Computação em Lote	1,5	Alta Média Baixa	2,25 1,5 0,75	4 3 2
47	Serviço de Codificação de Vídeo	0,5	Alta Média Baixa	0,75 0,5 0,25	5 3 2
48	Serviço de Rede de Entrega de Conteúdo	1,5	Alta Média Baixa	2,25 1,5 0,75	4 3 2
49	Serviço de Gateway de Armazenamento	1,5	Alta Média Baixa	2,25 1,5 0,75	12 6 3
50	Serviço Gerenciado de Publicação de Aplicações Web	1	Alta Média Baixa	1,5 1 0,50	10 5 3
51	Serviço de Gerenciamento de Segredos para Aplicações e APIs	0,5	Alta Média Baixa	0,75 0,5 0,25	4 3 2
52	Serviço de Gerenciamento de Chaves	0,5	Alta Média Baixa	0,75 0,5 0,25	6 3 1

2.2.2.19. Segue abaixo descrição de cada serviço listado na Tabela 3.

2.2.2.19.1. **Arquitetura de Solução em Nuvem** - consiste na execução de arquitetura de solução requisitada pelo contratante.

2.2.2.19.2. **Configuração de Máquina Virtual** - consiste no provisionamento e configuração de instância de máquina virtual na infraestrutura de nuvem, abrangendo, conforme o caso: instalação e atualização do sistema operacional, associação de disco(s) de armazenamento, configurações básicas de rede e outras atividades necessárias para a instância entre em operação.

2.2.2.19.3. **Configuração de VPN Site-to-Site** - consiste na configuração de VPN IPSEC que conecte os *datacenters* do contratante ao provedor de nuvem.

2.2.2.19.4. **Configuração de Regra de Filtragem em Firewall (NACL, InBound/OutBound)** - consiste na implementação de regra de firewall.

2.2.2.19.5. **Configuração de Rede Virtual** - criar estrutura de rede virtual.

2.2.2.19.6. **Configuração de Sub-Rede de Rede Virtual** - criar estrutura de sub-rede de rede virtual.

2.2.2.19.7. **Configuração de IP Público** - configurar IP público.

2.2.2.19.8. **Configuração de Domínio de DNS** - configurar zona em serviço de DNS.

2.2.2.19.9. **Configuração de Balanceador de Carga** - implementar balanceador de carga.

2.2.2.19.10. **Configuração de Certificado SSL** - gerar certificado digital válido internacionalmente para um domínio especifico (*multdomain* ou *wildcard*).

2.2.2.19.11. **Configuração de Disco Customizado de Sistema Operacional de Máquina Virtual** - customizar disco com propósito genérico.

2.2.2.19.12. **Configuração de Disco com Provisionamento de IOPS** - customizar disco especializado para alto desempenho.

2.2.2.19.13. **Criptografia de Dados e Discos** - implementar serviço de criptografia de dados e discos.

2.2.2.19.14. **Configuração de Sistema de Arquivos em Rede** - implementar sistema de arquivos acessível remotamente via protocolos NFS ou SMB incluindo "exports" e "shares".

2.2.2.19.15. **Implantar Serviço de Backup** - consiste na configuração de rotina diária de *backup* dos ambientes de produção incluindo a política de retenção.

2.2.2.19.16. **Configuração de Escalabilidade Automática (*Autoscaling*)** - implementar funcionalidade de escalabilidade automática em serviço de nuvem em operação.

2.2.2.19.17. **Hospedagem de *Containers*** - implementar serviço de *cluster* de *containers*, permitindo orquestração de *containers* Docker ou similar, com gerenciamento e controles de segurança.

2.2.2.19.18. **Migração de Ambientes ao Término do Contrato** - atividade de execução da transição da infraestrutura empregada pelas aplicações para outro provedor de nuvem ao final do contrato, ou quando houver necessidade de internalização de aplicações na infraestrutura local do contratante.

2.2.2.19.19. **Serviço de Aplicações Gerenciadas** - implementar aplicações baseadas no modelo de serviços gerenciado a partir do emprego de arquiteturas de referência recomendadas pelos provedores nos quais os serviços forem implementados.

2.2.2.19.20. **Serviço de Banco de Dados Gerenciado** - implementar banco de dados gerenciado.

2.2.2.19.21. **Serviço de Gerenciamento de Cache em Memória** - implementar serviço de *cache* em memória.

2.2.2.19.22. **Configuração de Gestão de Identidade, Permissões e Acessos** - administrar usuários, permissões, acessos e papéis utilizados no uso dos serviços em nuvem via integração com serviço de gerenciamento de identidades e acessos.

2.2.2.19.23. **Configuração de Operação Assistida** - atendimento em caráter de urgência para situações onde o contratante necessita de apoio consultivo/operacional na resolução de problemas afetos à infraestrutura de nuvem, quando estes tenham sido causados pela intervenção da equipe técnica do contratante, sem o assessoramento ou acompanhamento da contratada - poderá ainda ser utilizada na migração de recursos para outro provedor, em caso de transição contratual.

2.2.2.19.24. **Serviço de Monitoramento** - implementação de indicadores/métricas dos serviços da infraestrutura com geração de alertas - o serviço deverá ser capaz de distinguir entre problemas internos, na rede do provedor, ou fora do seu escopo.

2.2.2.19.25. **Arquitetura On-premises** - serviços de execução e planejamento de arquiteturas de soluções em nuvem que venham a ser integradas com infraestrutura e soluções em operação no ambiente *on-premises* do contratante.

2.2.2.19.26. **Implantar Cofre de Senhas** - consiste no provisionamento e configuração de repositório para armazenamento de chaves criptográficas e senhas a serem utilizadas pelas aplicações.

2.2.2.19.27. **Configuração de Serviço de Autenticação Integrado com Microsoft ADS** - consiste na configuração do serviço de autenticação da nuvem e na integração com o serviço de diretório local do contratante (Microsoft Active Directory).

2.2.2.19.28. **Implantação de Auditoria e Análise de Logs** - consiste na implementação de repositório central possibilitando a coleta e análise de *logs* de aplicação.

2.2.2.19.29. **Configuração de Buckets de Objetos** – provisionar estrutura de repositório/ *bucket* de objetos acessível remotamente via protocolo/API S3 ou equivalente.

2.2.2.19.30. **Configuração de Gateway NAT** - configurar *gateway* NAT.

2.2.2.19.31. **Serviço Gerenciado de Data Warehouse** - implementar "data warehouse" gerenciado.

2.2.2.19.32. **Serviço de Banco de Dados não Gerenciado** - implementar banco de dados não gerenciado.

2.2.2.19.33. **Configuração de Firewall de Aplicação Web** - consiste na implementação de regra de *firewall* de aplicação *web*.

2.2.2.19.34. **Configuração de Proteção contra Ataques DDOS** - consiste na mplementação de regras em camada 4 ou 7 mitigando ataques DDOS.

2.2.2.19.35. **Serviço de Indexação e Pesquisa de Documentos** - implementar serviço de indexação de documentos gerenciado.

2.2.2.19.36. **Serviço de Análise Preditiva e Criação de Modelo para Aprendizado de Máquina** - implementar serviço de análise preditiva e criação de modelo para aprendizado de máquina incluindo aplicações baseadas em API especializadas tais como conversão da linguagem falada para texto, processamento natural de linguagem, etc.

2.2.2.19.37. **Serviço de Avaliação de Vulnerabilidades** - implementar serviço gerenciado de avaliação de vulnerabilidades.

2.2.2.19.38. **Serviço Gerenciado de Execução de Funções** - implementar serviço gerenciado de execução de funções.

2.2.2.19.39. **Serviço de Migração de Banco de Dados** - implementar serviço gerenciado de migração de banco de dados.

2.2.2.19.40. **Serviço de Gateway de API** - implementar serviço gerenciado de *gateway* de API.

2.2.2.19.41. **Serviço de Mensageria Assíncrona** - implementar serviço gerenciado de mensageria assíncrona.

2.2.2.19.42. **Serviço de Entrega de Mensagem Eletrônica** - implementar serviço gerenciado de entrega de mensagem eletrônica.

2.2.2.19.43. **Implantação de Infraestrutrura de Serviços "On-Promises"** - implementar infraestrutura de serviços no ambiente de *datacenter* do contratante conectada à infraestrutura de serviços em nuvem do provedor.

2.2.2.19.44. **Serviço de Análise de Dados** - implementar serviço gerenciado de análise de dados.

2.2.2.19.45. **Serviço de Importação e Exportação de Dados** - implementar serviço gerenciado de importação e exportação de dados.

2.2.2.19.46. **Serviço de Execução de Cargas de Trabalho de Computação em Lote** - implementar serviço gerenciado de execução de cargas de trabalho de computação em lote.

2.2.2.19.47. **Serviço de Codificação de Vídeo** - implementar serviço gerenciado de codificação de vídeo.

2.2.2.19.48. **Serviço de Rede de Entrega de Conteúdo** - implementar serviço gerenciado de rede de entrega de conteúdo.

2.2.2.19.49. **Serviço de Gateway de Armazenamento** - implementar serviço gerenciado de rede de *gateway* de armazenamento conectando o ambiente "on-premises" ao ambiente do provedor de nuvem.

2.2.2.19.50. **Serviço Gerenciado de Publicação de Aplicações Web** - implementar serviço gerenciado de publicação de aplicações *web*.

2.2.2.19.51. **Serviço de Gerenciamento de Segredos para Aplicações e APIs** - implementar serviço de gerenciamento de segredos para aplicações e APIs.

2.2.2.19.52. **Serviço de Gerenciamento de Chaves** - implementar serviço de gerenciamento de chaves.

2.2.2.20. Em caráter ilustrativo segue no Anexo IV a projeção do volume global e individual de serviços de suporte técnico especializado em UST que será consumido pelo contratante.

2.3. SERVIÇOS DE TREINAMENTO

2.3.1. Todas as despesas necessárias à prestação dos serviços incluindo deslocamento e hospedagem serão de exclusiva responsabilidade da contratada, caso os serviços sejam executados presencialmente após consentimento mútuo entre contratada e contratante.

2.3.2. Os serviços de treinamento tem por propósito capacitar servidores do contratante na utilização dos serviços de computação em nuvem ofertados e consistem na transferência de conhecimento sobre as ferramentas, metodologias e tecnologias envolvidas.

2.3.3. Os serviços de treinamento poderão ser prestados presencialmente nas dependências do contratante ou remotamente em modalidade "online" com infraestrutura de videoconferência do tipo "webminar" a ser fornecida pela contratada, desde que previamente pactuado entre ambas as partes, em data e horário a ser pactuado consensualmente.

2.3.4. No caso de treinamento presencial, o contratante fornecerá o espaço físico com projetor, quadro branco, microcomputadores, infraestrutura de rede e cabeamento para a execução dos treinamentos, que necessariamente deverão ser ministrados em suas dependências, situadas à Avenida Borges de Medeiros, n° 1565, Bairro Centro, Porto Alegre, RS, CEP 90010-908, 7° andar. Quaisquer outros recursos necessários à realização dos treinamentos deverão ser disponibilizados pela contratada, sem ônus adicional ao contratante.

2.3.5. Cada turma poderá ter no máximo 20 (vinte) participantes. Tal quantitativo poderá ser fracionado no caso de treinamento presencial devido a restrições de espaço físico nas dependências do contratante, caso acordado entre ambas as partes.

2.3.6. Os serviços de treinamento deverão ser solicitados e agendados com no mínimo 20 (vinte) dias úteis de antecedência, salvo entendimento diverso entre as partes.

2.3.7. Os serviços de treinamento deverão ser ministrados em horário comercial para uma turma com carga horária diária de 7 (sete) horas ou em outro formato a ser definido e negociado entre contratada e contratante.

2.3.8. Os serviços de treinamento deverão ter a duração mínima de 5 (cinco) dias e a duração máxima de 10 (dez) dias.

2.3.9. Os serviços de treinamento deverão ser divididos preferencialmente em etapas, sendo que esses não poderão ser meramente expositivos, devendo contemplar também o uso prático dos serviços de computação em nuvem ofertados incluindo o desenvolvimento de estudos de caso.

2.3.10. Os treinamentos fornecidos pela contratada deverão ser apresentados em língua portuguesa. O material didático deverá ser fornecido em formato digital e/ou impresso para todos os participantes com o conteúdo abordado durante o treinamento em língua portuguesa ou, opcionalmente, em língua inglesa, desde que justificado e com anuência do contratante.

2.3.11. A contratada deverá apresentar a ementa completa do curso, carga horária e conteúdo programático, a qual deverá ser aprovada pelo contratante.

2.3.12. A contratada deverá emitir, ao final de cada treinamento ministrado, certificado de conclusão para cada participante, no qual deverão constar a identificação do treinando, o período de realização, o conteúdo e a carga horária do treinamento.

2.3.13. O instrutor responsável pela execução do treinamento deverá possuir experiência comprovada como instrutor dos serviços de computação em nuvem ofertados bem

como pleno conhecimento dos serviços em nuvem alvo do treinamento. A comprovação da capacitação do instrutor dar-se-á com base na apresentação de certificados que comprovem capacitação para tal finalidade, o que deverá ocorrer antes da realização de cada sessão de treinamento.

2.3.14. A preparação do ambiente de treinamento deverá ser realizada em conjunto pelas equipes da contratante e da contratada, de forma a garantir a correta configuração e disponibilidade do ambiente de treinamento.

2.3.15. Caso a qualidade do treinamento em alguma turma seja considerada insatisfatória pela maioria simples dos alunos, o contratante poderá exigir que esse seja refeito, sem ônus para o contratante.

2.3.16. O conteúdo programático deverá contemplar pelo menos os seguintes assuntos:

2.3.16.1. Conceitos básicos de serviços em ambiente de nuvem pública.

2.3.16.2. Visão geral dos serviços de computação em nuvem pública.

2.3.16.3. Visão geral das APIs e interfaces de gerência (CLI, portal, SDKs, etc).

2.3.16.4. Visão geral dos mecanismos de gestão de acessos e identidades para acesso a recursos e serviços.

2.3.16.5. Arquitetura e administração de topologias de aplicações em nuvem.

2.3.16.6. Migração de aplicações do ambiente "on-premises" para o ambiente em nuvem.

2.3.16.7. Melhores práticas para o desenvolvimento de aplicações em ambiente de nuvem.

2.3.16.8. Gerenciamento de instâncias computacionais e redes virtuais.

2.3.16.9. Gerenciamento de *storage* e *backup*.

2.3.16.10. Otimização da arquitetura de computação em nuvem.

2.3.16.11. Automação de serviços em nuvem.

2.3.16.12. Instalação, criação e execução de *containers*.

2.3.16.13. Projeto de arquitetura de redes para suportar o ambiente de nuvem.

2.3.16.14. Gerenciamento de custos na nuvem.

2.3.16.15. Gerenciamento de nuvem híbrida.

2.3.16.16. Implementação e provisionamento de topologias/*stacks* na plataforma de gestão de nuvem.

2.3.16.17. Implementação de serviços de computação em nuvem no ambiente "on-premises".

2.4. SERVIÇOS DE MONITORAMENTO, RELATÓRIOS, SUPORTE TÉCNICO E SUSTENTAÇÃO

2.4.1. Monitoramento

2.4.1.1. O serviço de monitoramento de recursos visa assegurar ao acompanhamento do uso de recursos consumidos pelos serviços de computação em nuvem utilizados pelo

contratante. Tal atividade será de responsabilidade da equipe técnica da contratada e/ou provedores de nuvem.

2.4.1.2. Os custos relativos à prestação dos serviços deverão estar includos no modelo de precificação empregado no cálculo das USN's.

2.4.1.3. A contratada deverá prover sistema de monitoramento em regime 24 x 7 x 365 para a infraestrutura de recursos em nuvem empregada pelo contratante.

2.4.1.4. O serviço de monitoramento de recursos de nuvem deverá fornecer indicadores, alertas e gráficos que permitam acompanhar em tempo real ou o histórico de utilização dos recursos computacionais empregados pelo contratante.

2.4.1.5. O contratante deverá poder acessar o serviço de monitoramento de recursos de computação em nuvem a qualquer momento.

2.4.1.6. O serviço de monitoramento de recursos de nuvem deverá permitir a configuração de alertas em caso de indisponibilidades ou quando recursos chave alcancem limites de utilização.

2.4.2. **Relatórios**

2.4.2.1. Será permitido ao contratante usar console de gestão dos serviços em nuvem para emitir relatórios de desempenho, problemas, configuração, mudanças e segurança do ambiente.

2.4.2.2. Os custos relativos à prestação dos serviços deverão estar includos no modelo de precificação empregado no cálculo das USN's.

2.4.2.3. Tal console deverá atender aos requisitos técnicos enumerados a seguir:

2.4.2.3.1. Controlar e monitorar o acesso dos usuários em seus diferentes tipos de perfis de acesso por meio de relatórios de auditoria.

2.4.2.3.2. Prover relatórios e análise das ocorrências e incidentes com base nos relatórios de auditoria e/ou desempenho.

2.4.2.3.3. Permitir a geração de relatórios de desempenho e disponibilidade por períodos de cobertura.

2.4.2.3.4. Permitir auditoria e notificação da ocorrência de incidentes, baseado nas métricas e parâmetros cadastrados, enviando notificações por *e-mail* ou mecanismo equivalente.

2.4.2.3.5. Armazenar informações de desempenho do ambiente de nuvem alocado e consumido pelo contratante por um período mínimo de 12 (doze) meses.

2.4.2.3.6. Disponibilizar as informações enumeradas abaixo:

2.4.2.3.6.1. Desempenho por ambiente.

2.4.2.3.6.2. Utilização de processador, memória e discos nas instâncias computacionais.

2.4.2.3.6.3. Volume de tráfego.

2.4.2.3.6.4. Verificação de registros de *logs*.

2.4.2.3.7. Permitir a geração de relatórios mensais completos de faturamento dos serviços utilizados incluindo relatórios parciais com prévia de faturamento do próximo mês de competência considerando os recursos computacionais consumidos do 1° (primeiro) dia do período (mês) de apuração até a data/hora de emissão do relatório.

2.4.3. **Suporte Técnico**

2.4.3.1. A contratada deverá adquirir suporte técnico em regime de 365 x 24 x 7 dos provedores de serviços em nuvem ofertados.

2.4.3.2. Os custos relativos à prestação dos serviços de suporte técnico deverão estar inclusos no modelo de precificação empregado no cálculo das USN's.

2.4.3.3. Os serviços de suporte técnico deverão ser prestados pela contratada e/ou provedor sem qualquer ônus adicional para o contratante.

2.4.3.4. Os serviços de suporte deverão permitir a comunicação por meio de *e-mail*, telefone ou outro meio a ser combinado consensualmente.

2.4.3.5. Os serviços de suporte técnico compreendendo a resolução de problemas e/ou esclarecimento de dúvidas na utilização dos serviços fornecidos pelos provedores.

2.4.3.6. Os chamados deverão ser registrados em central de atendimento e classificados por nível de severidade de acordo com o impacto no ambiente computacional do provedor de nuvem.

2.4.3.7. Os possíveis níveis de severidade são:

2.4.3.7.1. Severidade 1 - sistema crítico em produção está parado ou fora de funcionamento e não há meios de contornar a falha. Número significativo de usuários foi afetado ou impacto operacional significativo foi causado.

2.4.3.7.2. Severidade 2 - sistema crítico em produção está apresentando falhas de funcionamento, sem causar interrupção do serviço, mas afetando significativamente seu desempenho. Impacto crítico aos usuários.

2.4.3.7.3. Severidade 3 - sistema não crítico está parado ou fora de funcionamento. O problema pode ser contornado. Impactos operacionais moderados a pequenos. Impacto moderado aos usuários.

2.4.3.7.4. Severidade 4 - dúvidas, problemas na utilização, esclarecimentos da documentação, sugestões, solicitações de desenvolvimento de novas funcionalidades ou melhorias. Impacto mínimo aos usuários.

2.4.3.8. Os chamados serão agrupados por nível de severidade e seus prazos de atendimento serão contabilizados mensalmente conforme tabela que segue:

Tabela 4 - Prazo para Atendimento dos Serviços de Suporte Técnico

Nível de Serviço	Tempo máximo para início do atendimento (em horas úteis)	Prazo máximo de solução (em horas úteis) - Horário comercial (das 8h às 18h)
Chamados com severidade 1	1	3
Chamados com severidade 2	2	4
Chamados com severidade 3	4	5
Chamados com severidade 4	6	8

2.4.3.9. Os prazos de atendimento dos serviços de suporte técnico descritos na Tabela 4 se aplicam a cada serviço de computação em nuvem contemplado na Tabela 1.

2.4.3.10. A contratada e/ou provedor não será responsabilizada pelo prazo máximo estabelecido na Tabela 4 quando o chamado for originado por falha, interrupção ou qualquer outra ocorrência nos serviços de telecomunicações ou energia elétrica que atendem à infraestrutura interna do contratante, indisponibilidade de dados, inconsistência de dados e informações geradas pelo contratante, infraestrutura e capacidade de ambiente de tecnologia do contratante, não se caracterizando, nesses casos, a indisponibilidade dos serviços ou inadimplemento da contratada e/ou provedor.

2.4.3.11. Toda intervenção no ambiente produtivo deverá ser executada somente mediante prévia autorização do contratante a partir de informações claras dos procedimentos que serão adotados e executados pela contratada e/ou provedor.

2.4.3.12. Ao término do atendimento deverão ser conduzidos testes de validação da resolução do problema.

2.4.3.13. Nos casos em que o atendimento não se mostrar satisfatório o contratante poderá fazer a reabertura do chamado mantendo-se as condições e prazos do chamado inicial.

2.4.4. **Sustentação**

2.4.4.1. A contratada deverá prestar serviços de sustentação dos recursos computacionais em nuvem alocados e consumidos pelo contratante entregando recursos humanos qualificados que deverão executar pelo menos o seguinte conjunto exemplificado de atividades:

2.4.4.1.1. Prover o levantamento de requisitos, avaliação, modelagem do ambiente, dimensionamento de capacidade, plano de migração e implantação no ambiente de computação em nuvem.

2.4.4.1.2. Elaborar documentação de implantação de serviços no ambiente de computação em nuvem a ser discutida entre contratada e contratante.

2.4.4.1.3. Planejar, acompanhar e executar mudanças no ambiente de computação em nuvem visando à resolução de problemas.

2.4.4.1.4. Participar do processo de resolução de problemas junto ao contratante.

2.4.4.1.5. Realizar sistematicamente rotinas de prevenção de problemas no ambiente de computação em nuvem.

2.4.4.1.6. Organizar e administrar o tratamento de incidentes graves junto aos provedores em nome do contratante.

2.4.4.1.7. Acompanhar e escalar incidente junto aos provedores de nuvem com impacto nos níveis de serviço até sua solução final.

2.4.4.1.8. Dar suporte ao contratante nas resoluções de incidentes ocasionados pela solução e/ou atualizações de versões nos serviços de nuvem.

2.4.4.1.9. Atender solicitações do contratante para diagnosticar, corrigir e testar a solução de incidentes no ambiente de computação em nuvem.

2.4.4.1.10. Analisar desempenho e apontar possíveis gargalos no ambiente de computação em nuvem.

2.4.4.1.11. Notificar ao contratante, imediatamente e por escrito, sobre qualquer anormalidade verificada na execução dos serviços.

2.4.4.1.12. Comunicar, por escrito, a conclusão de quaisquer atividades envolvidas na execução do objeto contratual, principalmente aquelas que necessitem de aprovação por parte do contratante.

2.5. MODELO DE EXECUÇÃO DO OBJETO

2.5.1. Solicitação, Execução e Acompanhamento dos Serviços

2.5.1.1. O modelo de execução do objeto envolve essencialmente a abertura de ordens de serviço (OS) que contemplem combinação dos serviços referentes ao item 1 e/ou ao item 2. Portanto, uma única OS poderá conter serviços relativos ao item 1 e/ou ao item 2.

2.5.1.2. Os serviços de computação multinuvem (item 1) serão prestados pelos provedores de nuvem.

2.5.1.3. Os serviços de suporte técnico especializado (item 2) serão prestados pela contratada.

2.5.1.4. O procedimento de abertura de OS relativa aos itens 1 e/ou 2 deverá se basear no modelo de OS apresentado no Anexo II.

2.5.1.5. A contratada deverá manter estrutura de Central de Atendimento (CA) para abertura de chamados no regime 8 x 5. A CA da contratada deverá ser acionada por meio de ligação gratuita ou local a partir da cidade de Porto Alegre, *web* ou *e-mail* ou outro formato a ser definido entre contratada e contratante. O atendimento será realizado

na língua portuguesa, ou na língua inglesa, caso autorizado expressamente pelo contratante.

2.5.1.6. Na abertura do chamado, a contratada deverá realizar registro em sistema próprio fornecendo um número de registro diferenciado para o contratante. Para cada interação que envolver o chamado, o contratante deverá informar à contratada o número do registro correspondente.

2.5.1.7. As informações referentes a chamados, incluindo providências e ações de resolução tomadas, deverão ser armazenadas em sistema de controle de chamados da contratada, cujo acesso deverá estar disponível ao contratante. Nesse sentido, deverão ser criadas contas de acesso para a equipe de servidores designados pelo contratante para fins de acompanhamento e auditoria de chamados.

2.5.1.8. A contratada deverá realizar os devidos escalonamentos de acordo com o nível de atendimento dos chamados, reportados pelo contratante e/ou pelo sistema de monitoramento.

2.5.1.9. Em qualquer mudança na situação de chamados deverá ser encaminhada uma notificação ao contratante contendo as informações de registro do chamado para endereço eletrônico previamente designado, inclusive quando houver mudança de *status* interrompendo a contagem do tempo de atendimento.

2.5.1.10. Os chamados abertos somente poderão ser concluídos e fechados após autorização do contratante.

2.5.1.11. A contratada deverá encaminhar ao contratante até o 5° (quinto) dia útil do mês subsequente ao da prestação dos serviços relatório de fechamento mensal acompanhado da correspondente nota fiscal/fatura.

2.5.1.12. O relatório de fechamento mensal deverá conter a relação de chamados abertos pelo contratante até o término do mês anterior incluindo os indicadores de nível de serviço alcançados de cada chamado.

2.5.2. **Chamados de Planejamento/Criação/Diagnóstico**

2.5.2.1. Para chamados de planejamento/criação/diagnóstico, a contratada deverá agendar reunião virtual e/ou presencial com o contratante após a abertura do chamado para tratar da demanda do contratante. No caso de reunião virtual, a contratada será responsável por prover a infraestrutura tecnológica, restando ao contratante a responsabilidade por prover terminal de acesso à Internet com capacidade de reprodução de áudio e vídeo.

2.5.2.2. Após explicitada a demanda do contratante, a contratada terá até 10 (dez) dias úteis, contados a partir do dia útil subsequente ao da realização da reunião de que trata o item **Erro! Fonte de referência não encontrada.**, para apresentar 2 (dois) planos

de arquitetura de solução para implementação dos serviços demandados pelo contratante, cada plano na plataforma de um dos provedores de nuvem que a contratada intermediar. Cada plano de arquitetura trará, no mínimo, as seguintes informações:

2.5.2.2.1. Descrição detalhada do serviço a ser entregue.

2.5.2.2.2. Arquitetura proposta pela contratada para implementação do serviço demandado.

2.5.2.2.3. Orçamento detalhado dos serviços do provedor de nuvem que serão usados para implementação do serviço demandado contemplando o preço original do fabricante em dólar e o preço efetivamente cobrado pela contratada.

2.5.2.2.4. Orçamento detalhado dos serviços profissionais entregues pela contratada que serão usados para implementação do serviço demandado.

2.5.2.2.5. Prazo para entrega dos serviços.

2.5.2.2.6. Descrição detalhada de restrições, dependências e quaisquer informações relevantes acerca do plano proposto.

2.5.2.3. O contratante realizará a análise dos planos de arquitetura de modo a verificar se contêm todos os requisitos técnicos exigidos. Caso contrário, solicitará à contratada que refaça os planos de arquitetura.

2.5.2.4. Após o aceite dos planos de arquitetura, o contratante analisará os 2 (dois) orçamentos e decidirá se os serviços demandados serão implementados.

2.5.2.5. Caso decida pela implementação dos serviços, fará a opção, via de regra, pelo orçamento de menor preço, exceto quando existirem fatores técnicos ou de prazo que justifiquem a adoção do orçamento de maior preço. Neste último caso, o contratante justificará sua escolha de forma detalhada.

2.5.2.6. Os serviços referentes à elaboração dos planos de arquitetura serão pagos independente da decisão do contratante de implementar os serviços descritos.

2.5.3. **Chamados de Execução/Alteração/Implantação ou Exclusão**

2.5.3.1. Para chamados de execução/alteração/implantação ou exclusão, a contratada deverá agendar reunião presencial ou virtual com o contratante após a abertura do chamado, tratar da demanda do contratante. No caso de reunião virtual, a contratada será responsável por prover a infraestrutura tecnológica da mesma, restando ao contratante a responsabilidade por prover terminal de acesso à Internet com capacidade de reprodução de áudio e vídeo.

2.5.3.2. Após a execução dos serviços, cujos prazos estão designados na coluna "Prazo Máximo" da Tabela 3, o contratante realizará a análise dos serviços implementados, para verificar se estão em conformidade com o plano de arquitetura. Caso contrário, solicitará à contratada que refaça os serviços.

2.5.4. **Alteração dos Catálogos de Serviços**

2.5.4.1. Os catálogos de serviços relacionados aos serviços de computação em nuvem (Tabela 1) e aos serviços técnicos especializados (Tabela 3) poderão ser alterados pelo contratante de acordo com a conveniência e oportunidade.

2.5.4.2. A alteração dos catálogos de serviços deverá ser formalizada por meio de aditivo contratual.

2.5.4.3. A alteração dos catálogos de serviços consistirá na inclusão de novos serviços e na exclusão de serviços considerados desnecessários no decorrer da execução do contrato, contendo a motivação, as informações previstas nas Tabelas 1 e 3, além da descrição detalhada do serviço.

2.5.4.4. A inclusão ficará limitada a 14 (quatorze) serviços descritos na Tabela 1 e a 13 (treze) serviços descritos na Tabela 3, ou seja, em um numerário equivalente a 25% do quantitativo total de serviços contidos nas tabelas supracitadas.

2.5.4.4.1. O valor de referência de USN será dimensionado utilizando-se como referência valores adotados por no mínimo 2 (dois) provedores de nuvem.

2.5.4.4.2. O valor de referência de UST será dimensionado utilizando-se como referência valores adotados por no mínimo 2 (dois) integradores de nuvem.

2.6. **ENCERRAMENTO DOS SERVIÇOS E TRANSIÇÃO CONTRATUAL**

2.6.1. O encerramento se refere ao processo de finalização da prestação dos serviços ao final do contrato. A fim de possibilitar a transição contratual que assegure migração com o menor impacto para a continuidade dos serviços, será elaborado plano de encerramento dos serviços prestados.

2.6.2. A contratada deverá elaborar o plano de encerramento, no prazo de 180 (cento e oitenta) dias corridos antes do encerramento do contrato, para o repasse integral e irrestrito dos conhecimentos e das competências necessárias e suficientes para promover a continuidade dos serviços de computação em nuvem.

2.6.3. O plano de encerramento dos serviços deverá tratar, no mínimo, do seguinte conjunto de tópicos:

2.6.3.1. Identificação dos profissionais da contratada que irão compor a equipe de repasse, bem como seus papéis e suas responsabilidades.

2.6.3.2. Cronograma geral do repasse, identificando etapas e atividades com as respectivas datas de início e término, os produtos gerados e os recursos envolvidos.

2.6.4. Constarão dos produtos gerados, entre outros, os seguintes elementos:

2.6.4.1. Documentação e base de conhecimento atualizada com todos os procedimentos operacionais, *templates*, *scripts*, código fonte, documentação *as-built* e parâmetros de instalação e configuração dos serviços.

2.6.4.2. Fornecimento de todos os artefatos lógicos (documentos técnicos, *scripts*, código fonte, etc) utilizados para a operacionalização do contrato.

2.6.5. A contratada deverá dispor de meios que proporcionem portabilidade e tornem possível a migração dos serviços prestados para outros provedores de serviços em nuvem ou para outro ambiente definido pelo contratante.

2.6.6. A contratada deverá basear seus serviços em tecnologias abertas e padronizadas para a Internet, tais como HTTP, XML, JSON, etc.

2.6.7. Sempre que possível, a contratada deverá utilizar serviços, protocolos e ferramentas "open source".

2.6.8. A contratada deverá suportar a conversão do formato "Open Virtualization Format" (OVF) e outros padrões abertos de virtualização para os padrões utilizados pelo provedor. A conversão de formato também deverá ser suportada no sentido inverso, ou seja, dos padrões utilizados pelo provedor para o formato OVF e outros padrões abertos de virtualização.

2.6.9. Os serviços de computação em nuvem deverão possibilitar que os dados do contratante estejam disponíveis para transferência em direção aos seus *datacenters*.

2.6.10. A contratada deverá apoiar o contratante durante todo o processo de migração, dos dados e de quaisquer outros ativos para o novo ambiente.

2.6.11. A contratada deverá entregar ao contratante imagens de servidores virtuais, dados e informações do contratante que estejam armazenados ou hospedados no ambiente provido pela contratada, no formato OVF ou outro previamente acordado.

2.6.12. A contratada deverá apoiar a equipe técnica do contratante na migração das aplicações instaladas e configuradas no decorrer do contrato para a nova estrutura de nuvem, caso aplicável.

2.6.13. A contratada deverá assegurar que as imagens de servidores virtuais, dados e informações do contratante hospedados no ambiente provido pela contratada sejam destruídos, sem possibilidade de recuperação, após o encerramento do contrato, mediante autorização expressa do contratante.

2.6.14. A propriedade dos dados e informações gerados pelo contratante no ambiente provido pela contratada, a qualquer momento, durante a vigência, término ou expiração do contrato, será exclusivamente do contratante.

2.6.15. Durante o período de vigência do contrato, a contratada deverá garantir que toda a documentação requerida pelo contratante para facilitar a migração para outro provedor ou ambiente será mantida atualizada e será entregue ao contratante durante o processo de migração para outro provedor ou ambiente.

2.7. Toda informação confidencial gerada e/ou manipulada em razão desta contratação, seja ela armazenada em meio físico, magnético ou eletrônico, deverá ser devolvida, mediante formalização entre as partes, ao término ou rompimento do contrato, ou por solicitação do contratante.

LOTE 2

2.8. **SERVIÇOS DE COMUNICAÇÃO DE DADOS NA MODALIDADE LAN-TO-LAN PARA INTERCONEXÃO DOS DATACENTERS DO CONTRATANTE AOS DATACENTERS DOS PROVEDORES DE NUVEM**

2.8.1. Os serviços de comunicação multimídia (SCM) a serem contratados deverão prover circuitos de alta capacidade e baixa latência assegurando transmissão em modalidade LAN-to-LAN e conexão direta com os provedores de nuvem pública reconhecidos pelo mercado.

2.8.2. Tais serviços serão consumidos sob demanda, de acordo com as efetivas necessidades do contratante. Dada tal característica do serviço contratado, a data de término da ativação dos circuitos de dados será de até 90 (noventa) dias após autorizado pelo contratante.

2.8.3. Os serviços de comunicação de dados em modalidade LAN-to-LAN deverão suportar o tráfego de dados e de aplicações multimídia compreendendo o fornecimento, instalação e manutenção de circuitos, equipamentos e *softwares* para viabilizar a conexão dos *datacenters* do contratante às portas de conexão de fibra ótica de 1 Gbps ou 10 Gbps contratadas dos provedores de serviços em nuvem.

2.8.4. Os circuitos de comunicação de dados LAN-to-LAN deverão interligar as localidades denominadas: "Ponta A" (composta pelo prédio do Foro Central II (*datacenter* primário (DC1) do Poder Judiciário Gaúcho) e pelo prédio do Tribunal de Justiça (*datacenter* secundário (DC2) do Poder Judiciário Gaúcho)) à "Ponta B" (composta pelos *datacenters* dos provedores de nuvem ofertados).

2.8.5. A ponta A de cada conexão será instalada no prédio do Foro Central II, na Rua Manoelito de Ornellas, 50 - Porto Alegre - RS e no Prédio do Tribunal de Justiça, localizado na Avenida Borges de Medeiros, 1565 - Porto Alegre - RS, à critério do contratante, enquanto que a ponta B será instalada no *site* do provedor de serviços de nuvem ofertado a ser conectado ao ambiente "on-premises" do contratante.

2.8.6. Os circuitos de dados deverão ser disponibilizados de forma redundante nos 2 (dois) *datacenters* (DC1 e DC2) do Poder Judiciário Gaúcho, conforme topologia de conectividade de rede sugerida no Anexo V. Por conseguinte, a contratada será responsável pela entrega de 2 (dois) circuitos de dados tanto na ponta A quanto na ponta B com proteção automática entregando cada par a taxa de transmissão de 1 Gbps ou 10 Gbps, de tal forma que os serviços deverão ser precificados com base na oferta de 2 (dois) canais visando dupla abordagem de interconexão ao provedor de nuvem.

2.8.7. Os circuitos de dados redundantes com taxa de transmissão de 10 Gbps deverão conectar os *datacenters* do contratante ao provedor de serviços de computação em nuvem primário enquanto que os circuitos de dados redundantes com taxa de transmissão de 1 Gbps deverão conectar os *datacenters* do contratante ao provedor de serviços de computação em nuvem secundário.

2.8.8. Cada circuito de dados individual pertencente ao conjunto de 2 (dois) circuitos de dados redundantes deverá obrigatoriamente possuir caminho físico de transporte distinto e independente. Mais especificamente, os circuitos de dados em operação num mesmo *datacenter* do contratante poderão compartilhar o mesmo trajeto até o *backbone* da operadora/contratada enquanto que os circuitos de dados em distintos *datacenters* do contratante não poderão compartilhar o mesmo trajeto até o backbone da operadora/contratada assegurando a redundância das conexões.

2.8.9. Os circuitos de dados deverão permitir o emprego do protocolo BGP ou equivalente permitindo que o contratante possa encaminhar o tráfego originado de sua rede interna 10.200.0.0/16, 10.201.0.0/16, 10.202.0.0/16, 10.203.0.0/16, 10.204.0.0/16, 10.205.0.0/16, 10.206.0.0/16, 10.207.0.0/16, 10.208.0.0/16 e 10.209.0.0/16) em direção às redes virtuais privadas do contratante em operação nos provedores de serviços de computação em nuvem (ponta B), cabendo salientar que existe conectividade redundante em camada de enlace (nível 2) baseada no protocolo LACP entre ambos os *datacenters* do contratante.

2.8.10. Os circuitos de dados que serão fornecidos e instalados no ambiente de *datacenter* do contratante (DC1 e DC2) deverão possuir interfaces do tipo 1 GbE ou 10 GbE utilizando *transceivers* 1000Base-LX SFP (mini-GBIC) 1.310 nm SMF ou *transceivers* 10GBase-LR SFP+ (mini-GBIC) 1.310 nm SMF com conector LC..

2.8.11. A comunicação de dados deverá ser provida através de *backbone* próprio da contratada, não sendo permitida a utilização de *backbones* de terceiros.

2.8.12. O fornecimento do serviço de comunicação de dados LAN-to-LAN deverá basear-se exclusivamente na tecnologia Ethernet de comutação de quadros (*Ethernet Frame Switching*) em *layer* 2 (ou camada de enlace) de acordo com a coleção de padrões IEEE 802.3 e suportar a pilha de protocolos IP v4.

2.8.13. A comunicação de dados deverá ser provida fim a fim de forma dedicada e exclusiva através de meio de transmissão baseado em fibra óptica, não sendo permitidos outros meios físicos de interconexão.

2.8.14. Cada circuito de comunicação de dados LAN-to-LAN deverá prover a taxa de transmissão garantida simétrica e bidirecional de 1 Gbps ou 10 de Gbps entre a ponta A e a ponta B.

2.8.15. A taxa de perda de pacotes deverá ser igual ou inferior a 1%.

2.8.16. A latência não deverá ultrapassar 50 ms.

2.8.17. O índice de disponibilidade dos circuitos de comunicação de dados LAN-to-LAN deverá ser de, no mínimo, 99,4% ao mês, levando em conta os períodos de manutenção dos circuitos, dos quais deverão ser agendados e acordados com a equipe técnica do contratante e executados somente fora do seu horário de expediente.

2.8.18. A interconexão das redes privadas virtuais e respectivas subredes IP em operação no ambiente dos provedores de nuvem aos equipamentos comutadores centrais Ethernet LAN em funcionamento no DC1 e no DC2 do contratante deverão ser realizadas por circuitos digitais dedicados.

2.8.19. Não poderão ocorrer pontos de concentração que possam estabelecer estrangulamento de tráfego ou interdependência de funcionamento entre os *datacenters* do contratante e dos provedores de nuvem.

2.8.20. Os circuitos de comunicação de dados deverão ser transparentes a protocolos utilizados no seu *payload,* sendo vedada qualquer forma de aplicação de filtros assegurando que a contratada não exercerá qualquer tpo de limitação quanto a quantidade (em bytes) e conteúdo da informação trafegada no acesso.

2.8.21. Os circuitos de comunicação de dados deverão possuir taxa de transmissão constante full-duplex e simétrica com disponibilidade de 24 x 7 x 365.

2.8.22. Os circuitos de comunicação de dados deverão receber uma identificação única a ser utilizada tanto pelo contratante como pela contratada.

2.8.23. Não poderão existir quaisquer restrições a protocolos ou aplicações na conexão LAN-to-LAN.

2.8.24. Os circuitos de comunicação de dados deverão ser entregues no interior dos *datacenters* do contratante nos quais deverão ocorrer as conexões dos circuitos de dados fornecidos pela contratada aos equipamentos de rede marca Extreme Networks modelo BD 8810 em operação em ambos os *datacenters* do contratante.

2.8.25. Caso seja empregado o protocolo BGP na camada de rede ou mecanismo/protocolo equivalente, a conexão e o estabelecimento da sessão BGP (ou entidade similar) será realizada diretamente através do roteador de borda do contratante, o qual correntemente é composto por um *cluster* com 2 (dois) equipamentos marca Fortinet modelo Fortigate FG-1500D configurados em uma arquitetura do tipo HA (*High Avalilability*) e baseados em sistema operacional FortiOS 6.x. A contratada deverá fornecer todos os parâmetros necessários para que o contratante possa realizar as configurações para o correto estabelecimento da sessão BGP ou mecanismo/protocolo equivalente junto aos equipamentos indicados.

2.8.26. Será de responsabilidade da contratada o fornecimento de todos os equipamentos, módulos, cabos, materiais, insumos ou quaisquer outros itens e serviços necessários para promover a conexão dos circuitos de comunicação de dados aos equipamentos de rede em operação nos *datacenters* do contratante.

2.8.27. Todos os equipamentos e materiais de infraestrutura a serem fornecidos pela contratada deverão ser homologados pela ANATEL.

2.8.28. A instalação, confguração e manutenção da infraestrutura de fibra óptica e equipamentos é de responsabilidade da contratada.

2.8.29. Todos os custos oriundos para a interligação da ponta A com a ponta B serão de responsabilidade da contratada.

2.8.30. Todo processo de instalação e implantação dos serviços será acompanhado e supervisionado pela equipe técnica do contratante, à qual a contratada deverá se reportar antes de qualquer ação e decisão referente à implantação dos circuitos de dados.

2.8.31. Todos os custos com realização de canalização, entradas, tubulações, suportes e periféricos, compreendendo todo o percurso de infraestrutura de cabeamento, desde a ponta A até a ponta B serão de responsabilidade da contratada.

2.8.32. Os custos pelo uso dos equipamentos e sua manutenção deverão estar compreendidos no valor da mensalidade.

2.8.33. A contratada deverá efetuar a manutenção preventiva e corretiva dos circuitos de acesso e equipamentos, incluído os equipamentos instalados nas dependências da contratante.

2.8.34. A manutenção inclui reposição dos equipamentos, peças e infraestrutura, como cabos, conectores, adaptadores, entre outros.

2.8.35. Os equipamentos defeituosos, caso não possam ser reparados, deverão ser substituídos.

2.8.36. O contratante poderá utilizar eventuais ferramentas próprias de monitoria para aferir a disponibilidade do serviço contratado, o que não eximirá a obrigatoriedade da contratada de realizar a monitoria do serviço fornecido.

2.8.37. A indisponibilidade de um circuito será medida considerando-se o tempo decorrido entre a ocorrência efetiva da indisponibilidade e a restauração completa de sua operação.

2.8.38. Serão excluídas dessa contagem as interrupções causadas por eventual falta de energia elétrica nos *datacenters* do contratante ou outros fatores técnicos relacionados às suas instalações e infraestrutura que venham a causar interrupção do serviço fornecido pela contratada, desde que devidamente comprovados.

2.8.39. Quaisquer modificações e/ou reconfigurações que necessitem ser executadas nos equipamentos pela contratada, deverão ser autorizadas e acompanhadas por um técnico do contratante.

2.8.40. As interrupções programadas por solicitação da contratada, ou por necessidade da contratante, em função de parada técnica para manutenção e reconfiguração de seus

equipamentos, desde que previamente acordadas entre as partes, não serão contabilizadas para o cálculo de disponibilidade do serviço.

2.8.41. Serão excluídas da contagem as interrupções programadas para manutenção, desde que a contratada efetue comunicação com pelo menos 5 (cinco) dias úteis de antecedência e que a interrupção ocorra entre 00h00min e 06h00min de segunda à sexta e de 00h00min e 08h00min em sábados, domingos e feriados nacionais ou estaduais.

2.8.42. O prazo máximo para solução de problemas de indisponibilidade no serviço será de 2 (duas) horas corridas após a abertura da ocorrência do incidente.

2.8.43. O valor do desconto por indisponibilidade dos serviços será determinado considerando cada intervalo de 30 (trinta) minutos de indisponibilidade de cada circuito, de acordo com a seguinte equação:

$$VD = VM * N / 1440$$

Onde:

VD = valor do desconto

VM = valor mensal dos serviços

N = quantidade de unidades de períodos inteiros de 30 (trinta) minutos de indisponibilidade

1440 = total de períodos inteiros de 30 (trinta) minutos no período mensal de serviços.

2.8.44. Os serviços ofertados deverão ser precificados conforme Anexo IX (Modelo de Proposta de Preços - Lote 2).

2.8.45. Relevante enfatizar que será de responsabilidade da contratada:

2.8.45.1. A completa instalação dos equipamentos de rede, fibras ópticas, dutos, observando as normas de engenharia para tal, incluindo cuidados com aterramento, fixação correta de estruturas e dispositivos entre outros.

2.8.45.2. O fornecimento dos materiais e acessórios necessários a fixação das estruturas e equipamentos usados na execução dos serviços, incluindo porcas, parafusos, cabos, conectores entre outros.

2.8.45.3. Obter os licenciamentos que se fizerem necessários junto a ANATEL, incluindo licenciamento da frequência, caso aplicável, e de acordo com a regulamentação vigente.

2.8.45.4. Registro de ART e outras obrigações junto ao CREA para obras de instalação de torres, postes ou outras obras civis que venham a ser necessárias, sempre que a legislação assim exigir.

2.8.45.5. Garantir sigilo e inviolabilidade das informações que eventualmente possa ter acesso durante os procedimentos de instalação e manutenção de seus equipamentos, bem como durante a operação do serviço.

2.9. ACORDOS DE NÍVEL DE SERVIÇO

2.9.1. SERVIÇOS DE COMPUTAÇÃO MULTINUVEM

2.9.1.1. A contratada será glosada pela não prestação dos serviços em nuvem computacional dentro dos prazos acordados nas ordens de serviço.

2.9.1.2. O contratante poderá solicitar relatórios de funcionamento ininterrupto dos serviços em nuvem computacional para fins de apuração dos respectivos níveis de disponibilidade.

2.9.1.2.1. Em caso de indisponibilidade dos serviços, será aferido o tempo de restauração do serviço da seguinte forma:

TRS = (HR - HI)

Onde:

HR = Horário da Recuperação do Serviço
HI = Horário de Início da Indisponibilidade

2.9.1.2.2. Em caso de descumprimento do prazo de disponibilidade dos serviços a contratada ficará sujeita à glosa no pagamento de acordo com as seguintes condições:

2.9.1.2.2.1. Se o TRS for compreendido entre 3 horas e 1 min e 4 horas corridas deverá ser aplicado o desconto de 3%.

2.9.1.2.2.2. Se o TRS for compreendido entre 4 horas e 1 min e 5 horas corridas deverá ser aplicado o desconto de 5%.

2.9.1.2.2.3. Se o TRS for compreendido entre 5 horas e 1 min e 6 horas corridas deverá ser aplicado o desconto de 10%.

2.9.1.2.2.4. Se o TRS for acima de 6 horas e 1min deverá ser aplicado o desconto de 15%.

2.9.1.2.3. O TRS exclui o tempo de indisponibilidade planejada.

2.9.1.2.4. O valor do desconto acima deverá ser calculado para cada ordem de serviço correspondente ao mês de aferição e ao serviço indisponível.

2.9.2. SERVIÇOS DE SUPORTE TÉCNICO ESPECIALIZADO

2.9.2.1. A contratada será glosada pela não prestação dos serviços técnicos especializados dentro dos prazos acordados nas ordens de serviço conforme segue:

2.9.2.1.1. Em caso de descumprimento do prazo estabelecido para o término das ordens de serviço abertas pelo contratante descrito na Tabela 3, sem que haja justificativa aceita pelo contratante, a contratada ficará sujeita à glosa no pagamento de acordo com o seguinte cálculo:

2.9.2.1.1.1. Se o tempo de atraso (TA) na prestação do serviço técnico previsto em cada ordem de serviço em percentual do prazo máximo previsto for maior do que 30% e igual ou inferior a 80% deverá ser aplicado o desconto de 30% do valor do serviço demandado.

2.9.2.1.1.2. Se o tempo de atraso (TA) na prestação do serviço técnico previsto em cada ordem de serviço em percentual do prazo máximo previsto for maior do que 80% deverá ser aplicado o desconto de 80% do valor do serviço demandado.

2.9.2.1.2. O valor do desconto acima deverá ser calculado para cada ordem de serviço correspondente ao mês de aferição.

2.9.3. SERVIÇOS DE MONITORAMENTO, RELATÓRIOS, SUPORTE TÉCNICO E SUSTENTAÇÃO

2.9.3.1. A contratada será glosada pelo não atendimento dos chamados técnicos de suporte relativos aos serviços de computação em nuvem descritos na Tabela 1 dentro dos prazos acordados no item 2.4.3 conforme segue:

2.9.3.1.1. 1% do valor do serviço afetado por hora de atraso no atendimento de chamado de suporte técnico cujo impacto foi categorizado como sendo de "Severidade 1".

2.9.3.1.2. 0,5% do valor do serviço afetado por hora de atraso no atendimento de chamado de suporte técnico cujo impacto foi categorizado como sendo de "Severidade 2".

2.9.3.1.3. 0,25% do valor do serviço afetado hora de atraso no atendimento de chamado de suporte técnico cujo impacto foi categorizado como sendo de "Severidade 3".

2.9.3.1.4. 0,1% do valor do serviço afetado por hora de atraso no atendimento de chamado de suporte técnico cujo impacto foi categorizado como sendo de "Severidade 4".

2.9.4. SERVIÇOS DE COMUNICAÇÃO DE DADOS

2.9.4.1. A contratada deverá obedecer aos acordos de níveis de serviços descritos na Tabela 5 conforme a severidade do incidente e respectivo prazo de solução:

Tabela 5 - Prazo para Atendimento dos Serviços de Suporte Técnico

Severidade	Situação	Prazo de Solução
Alta	Serviço indisponível	2 Horas
Média	Serviço com degradação de qualidade	4 Horas
Baixa	Problemas com baixo impacto no serviço	8 Horas

2.9.4.1.1. O prazo máximo para solução de problemas que geram indisponibilidade total dos serviços (severidade alta) será de 2 (duas horas) corridas, após a abertura do chamado de serviço.

2.9.4.1.2. O prazo máximo para solução de problemas que geram degradação do serviço (severidade média) será de 4 (quatro horas) corridas, após a abertura do chamado de serviço. Entende-se por degradação do serviço, problemas de latência, perda de pacotes, problemas de roteamento e outros problemas que não causem a interrupção total do serviço, mas que afetem o seu funcionamento normal.

2.9.4.1.3. O prazo máximo para solução de problemas com baixo impacto nos serviços (severidade baixa) será de 8 (oito horas) corridas, após a abertura do chamado de serviço. Entende-se que os referidos problemas tenham baixo impacto no serviço ou risco de gerar parada ou degradação no serviço, como: alto índice de utilização de CPU, interfaces atingindo valores de tráfego próximo ao limite de sua capacidade dentre outros problemas não especificados taxativamente.

2.9.4.2. A contratada será glosada pelo não atendimento dos níveis de serviço descritos na Tabela 5 dentro dos prazos acordados conforme segue:

Tabela 6 - Glosas no Descumprimento dos Acordos de Níveis de Serviço

Percentual %	Base de Cálculo	Aplicação	Ocorrência
2,5	Sobre o valor mensal do contrato	Por hora de atraso	Por descumprimento de prazo estipulado para solução de incidentes de alta severidade
2	Sobre o valor mensal do contrato	Por hora de atraso	Por descumprimento de prazo estipulado para solução de incidentes de média severidade
0,5	Sobre o valor mensal do contrato	Por hora de atraso	Por descumprimento de prazo estipulado para solução de incidentes de baixa severidade

3. CONDICIONANTES AMBIENTAIS APLICÁVEIS AO OBJETO

3.1. Não aplicável visto que serão empregados equipamentos de propriedade dos provedores de serviços em nuvem ofertados pela contratada, cabendo a tais atores da relação contratual a responsabilidade de recolher e descartar adequamente peça defeituosa bem como arcar com todos os custos de transporte para tal finalidade.

4. VISTORIA

4.1. As licitantes poderão vistoriar os "datacenters" [11] do contratante, em companhia de um servidor do Poder Judiciário, com o objetivo de inteirar-se sobre as condições das instalações e do grau de dificuldade existente.

4.2. A vistoria aos "datacenters" tem como objetivo dar ciência da estrutura existente, fornecendo o conhecimento de aspectos que possam influir direta ou indiretamente na execução dos serviços.

4.3. A vistoria deverá ser agendada com no mínimo dois dias de antecedência, pelo(s) telefone(s) (51) 3210-7852 com o servidor designado, Marcelo da Silva Strzykalski (matrícula 13989219).

4.4. A vistoria poderá ser realizada até dois dias úteis antes da abertura da licitação, objetivando conhecer as condições de desenvolvimento dos serviços e obtenção de subsídios para elaboração da proposta comercial e participação do certame.

4.5. Tendo em vista a faculdade da realização da vistoria, os licitantes não poderão alegar o desconhecimento das condições e grau de dificuldades existentes como justificativa para se eximirem das obrigações assumidas em decorrência deste edital.

5. AMOSTRAS

5.1. Caso evidências coletadas na análise da totalidade dos documentos técnicos fornecidos pela licitante classificada em primeiro lugar não comprovem que os serviços ofertados atendem aos requisitos técnicos exigidos do objeto descritos no item 2.1.2 dessa especificação técnica em sua integralidade, os serviços em nuvem ofertados poderão passar por uma etapa de homologação técnica por meio de execução de procedimento amostral com o objetivo de verificar que esses efetivamente venham a atender plenamente aos requisitos do Edital.

5.2. Portanto, o procedimento amostral ocorrerá facultativamente, somente em caso de insucesso na comprovação integral dos requisitos técnicos por meio do emprego da documentação comprobatória fornecida pela licitante para fins de atendimento dos requisitos técnicos exigidos no item 2.1.2.

5.3. O contratante solicitará à ofertante do menor preço que demonstre a execução dos serviços descritos nesta especificação técnica visando à comprovação do atendimento dos requisitos exigidos na licitação. O comparecimento de representante da licitante

---

[11] O *datacenter* principal está instalado nas dependências físicas do prédio do Foro Central II (Rua Manoelito de Ornellas, n° 50, CEP 90110-230, Porto Alegre, RS) enquanto que o *datacenter* secundário está instalado nas dependências físicas do prédio do Tribunal de Justiça (Avenida Borges de Medeiros, n° 1565, CEP 90010-908, Porto Alegre, RS).

deverá ocorrer em até 5 (cinco) dias úteis após ter sido notificada pelo pregoeiro. A ausência de representante para dar início ao trabalho de demonstração após o fim desse prazo será motivo de desclassificação da proposta.

5.4. Após comparecimento dentro do prazo estabelecido no item 5.3, a licitante deverá configurar ambientes de serviços de computação em nuvem em pelo menos um dos provedores de nuvem que intermediar, envolvendo os serviços listados na Tabela 1, de acordo com o plano detalhado que receber do contratante, em até 2 (dois) dias úteis, contados a partir do dia útil seguinte ao recebimento do plano detalhado do contratante.

5.5. Após configurados os ambientes, a licitante receberá ordens de serviço consecutivas que envolvem serviços listados na Tabela 3 e nos itens enumerados a seguir. Detalhes a respeito das ordens de serviço serão fornecidos no momento da demonstração dos serviços. Qualquer custo envolvido na demonstração dos serviços será da licitante.

5.5.1. Criação da infraestrutura por *script* de automação: rede, *storage* e máquinas virtuais (VMs) com discos SSD criptografados por *hardware* usando serviço de chaves da respectiva nuvem, em ambiente com rede virtual privada, com o *range* 10.0.1.0/16, ou outro *range*, de acordo com o definido pelo contratante.

5.5.2. Criar e iniciar pelo menos 2 (duas) VMs em cada provedor de nuvem.

5.5.3. Instalar plataforma de *containers* nos 2 (dois) provedores de nuvem.

5.5.4. Adicionar as VMs criadas na plataforma de *containers* de cada provedor de nuvem.

5.5.5. Configurar uma aplicação em cada provedor de nuvem com pelo menos 2 (duas) VMs e um banco de dados. Quando a aplicação estiver executando uma das VMs deverá ser desligada visando simular falha, sendo que a aplicação não poderá parar de funcionar após a VM ser desligada.

5.5.6. Definir a topologia de rede virtual e de sub-redes.

5.5.7. Definir regras de *firewall* no nível da borda de rede e *firewall* para as instâncias.

5.5.8. Definir regras de bloqueio geográfico para acesso a aplicação como, por exemplo, permitir que certa aplicação só receba requisições oriundas do Brasil.

5.5.9. Permitir escolher tipos e tamanhos de unidades de processamento, por vCPU ou memória, observando o cardápio de opções do provedor de nuvem.

5.5.10. Realizar *deploy* de aplicação com escalabilidade automática, conforme a demanda.

5.5.11. Finalizar as VMs e devolver os recursos para os provedores de nuvem.

5.6. A licitante deverá apresentar pelo menos um profissional que possua certificação de arquiteto de soluções em cada um dos provedores de nuvem que intermediar durante a realização do procedimento amostral.

5.7. Os serviços prestados na demonstração técnica serão examinados e avaliados por comissão formada por servidores do contratante para esta finalidade. Os serviços deverão ser realizados no prédio do Tribunal de Justiça do Rio Grande do Sul, situado

na Rua Avenida Borges de Medeiros 1565, CEP 90010-908, Porto Alegre-RS, durante os horários de 09h às 12h ou 13h às 18h. A licitante deverá agendar o horário para a demonstração junto à Diretoria de Tecnologia da Informação e Comunicação (DITIC), por meio do telefone (51) 3210-7570.

6. CONDIÇÕES DE ENTREGA E DE RECEBIMENTO

6.1. Não aplicável visto que serão empregados equipamentos e licenças de *software* de propriedade dos provedores de serviços em nuvem ofertados pela contratada.

7. PRAZO E CONDIÇÕES DE GARANTIA E MANUTENÇÃO

7.1. Não aplicável visto que serão empregados equipamentos e licenças de *software* de propriedade dos provedores de serviços em nuvem ofertados pela contratada.

8. ESTIMATIVA DO VOLUME DE SERVIÇOS

8.1. O dimensionamento preliminar dos serviços de computação em nuvem e de suporte técnico especializado a serem contratados poderá ser visualizado no Anexo VII, o qual considerou informações baseadas no levantamento dos ambientes técnicos em operaçao nos 2 (dois) *datacenters* do contratante e previsões constantes no plano anual de contratações e informações relacionadas ao padrão esperado de atividades do Poder Judiciário Gaúcho.

Anexo I - Termo de Responsabilidade e Sigilo

Eu, _____ CPF: _____, pelo presente instrumento, na condição de prestador de serviços terceirizados para o Tribunal de Justiça do Rio Grande do Sul, comprometo-me a cumprir todas as orientações e determinações a seguir especificadas e outras normatizadas no Ato Nº 11/2004-P disponível no *site* da Internet do contratante no endereço http://www.tjrs.jus.br, em função do contato que terei com informações pertencentes ao contratante, ou por ele custodiadas, em razão da permissão de acesso aos recursos computacionais necessários para a execução de minhas atividades profissionais, estando ciente, de acordo, aderente e responsável nos seguintes aspectos:

1. Obedecer, cumprir e respeitar, de forma específica, a Lei Geral de Proteção de Dados e o Ato 037/2020-P, que dispõe sobre a política de proteção e de segurança de dados pessoais, bem como todas as políticas, diretrizes e normas de segurança da informação do TJRS, que regem o uso dos recursos a mim disponibilizados, sejam esses digitais ou impressos, bem como o manuseio das informações a que tenho acesso, ou possa vir a ter, em decorrência da execução de minhas atividades profissionais, responsabilizando-se pelo seu descumprimento.
2. A prestadora de serviços deverá manter sigilo, sob pena de responsabilidade civil, penal e administrativa, acerca de todo e qualquer assunto de interesse do TJRS ou de terceiros de que tiver conhecimento em razão da execução do contrato, devendo orientar os seus profissionais neste sentido.
3. Qualquer meio de acesso a informações ou instalações, como identificador de usuário (*user id*), senhas de acesso a sistemas (*password*), aplicativos, Internet, Intranet, conta de correio eletrônico (*e-mail*), crachás, cartões, chaves, dispositivo eletrônico de criptografia ou afins, que o contratante me forneceu ou vier a me fornecer são individuais e intransferíveis e estarão sob minha custódia e serão utilizados exclusivamente no cumprimento de minhas responsabilidades funcionais, devendo ser por mim devolvidos ou disponibilizados ao contratante em caso de desligamento, encerramento de serviços ou mudança de função.
4. Meus acessos à Internet e a conta de correio eletrônico por meio dos recursos fornecidos a mim e pertencentes ao contratante devem ser utilizados única e exclusivamente para a realização de atividades explicitamente especificadas no escopo dos serviços a serem prestados.
5. Todos os meus acessos efetuados, lógicos ou físicos, e informações por mim manipuladas (sistemas de informação, correspondências, cartas, correios eletrônicos, etc.) serão passíveis de verificação por representantes do contratante, que recebam atribuição para tal, a qualquer momento, independentemente de aviso prévio. Em decorrência disso, fico ciente que o contratante é o legítimo proprietário de todos os equipamentos, infraestrutura, informações e sistemas de informação que serão por mim utilizados.
6. Não devo adquirir, reproduzir, instalar, utilizar e/ou distribuir cópias não autorizadas de *softwares* ou programas aplicativos, produtos, inclusive aqueles desenvolvidos internamente no contratante.
7. Não é permitida a entrada ou saída de quaisquer informações pertencentes ao contratante, quer essas sejam em meios magnéticos (CDs, fitas, disquetes, *pen drives*, etc.), em meios físicos (papel, impressos, etc.) ou em meios lógicos (webmail, internet, etc.) sem o conhecimento e autorização de seu responsável.
8. Em caso de utilização de acesso remoto, desde que devidamente autorizado, aos recursos do contratante para a execução de minhas atividades profissionais, devo manusear as informações obedecendo aos mesmos critérios de segurança exigidos nas instalações internas, para o desempenho de minhas atividades.
9. Devo zelar pela segurança, pelo uso correto e pela manutenção adequada dos equipamentos pertencentes ao contratante, compreendendo dentre outros aspectos:
    a) Nunca deixar um equipamento ativo sem antes bloquear seu acesso ou desativar a senha quando dele se

afastar ou se ausentar.

b) Jamais emprestar minha senha ou utilizar a senha de outros.
c) Nunca utilizar senhas triviais que possam ser facilmente descobertas.
d) Não divulgar informações do contratante, de partes, de advogados e de prestadores de serviços.
e) Não deixar relatórios ou quaisquer mídias com informações confidenciais expostos em locais de fácil acesso.
f) Não utilizar recursos e/ou equipamentos particulares, na rede do contratante, para a realização de qualquer tipo de atividade, seja ela profissional ou não, sem a devida avaliação e autorização do contratante.
g) Somente utilizar *software* que tenha sido devidamente homologado pelo órgão ou gestor responsável.
h) Respeitar as legislações de direitos autorais e de propriedade intelectual.
i) Quando houver a necessidade de descartar as informações, fazer de forma a impedir o seu resgate independentemente do meio de armazenamento na qual a informação se encontra.
j) Informar imediatamente o órgão responsável e ao Departamento de Informática acerca de qualquer violação das regras de sigilo por quem quer que seja.

10. Reconheço que a lista acima é meramente exemplificativa e ilustrativa e que outras hipóteses de confidencialidade, que já existam ou que venham a surgir no decorrer da contratualidade, devem ser consideradas e mantidas em segredo, e que em caso de dúvida acerca da confidencialidade de determinada informação devo tratá-la sob sigilo, até que venha a ser autorizado a tratá-la diferentemente pelo órgão ou gestor responsável. Em hipótese alguma irei interpretar o silêncio do contratante como liberação de quaisquer dos compromissos ora assumidos.
11. Descumprindo os compromissos por mim assumidos neste Termo de Responsabilidade e Sigilo de Informações, estarei sujeito às penalidades aplicáveis, como medidas administrativas e/ou disciplinares internas, e/ou, ainda, ações penais, cíveis e/ou trabalhistas previstas em lei.
12. Estou ciente de que, para fins penais, de acordo com o art. 327 do Código Penal, equipara-se a funcionário público quem exerce cargo, emprego ou função em órgão público ou entidade paraestatal, e quem trabalha para empresa prestadora de serviço contratada ou conveniada para a execução de atividade típica da Administração Pública.

Porto Alegre, _____ de _____ de _____ .

_____	_____
Assinatura	Assinatura
	Nome do Empregado RG e Órgão Emissor
Matrícula: _____	
	_____ _____
Cargo/Função: _____	
Tribunal de Justiça do Estado do Rio Grande do Sul	Empresa:
CNPJ/MF: 89.522.064/0001-66	CNPJ/MF:
	Nº Contrato:
Testemunhas (nome e RG)	

Anexo II - Modelo de Ordem de Serviço

TRIBUNAL DE JUSTI ÇA DO RIO GRANDE DO SUL	**ORDEM DE ABERTURA DE CHAMADO**
	Contrato nº XX/XXXX
	OS-AAAA-XXX

1. **DESCRIÇÃO GERAL DOS SERVIÇOS/PRODUTOS, INCLUINDO O QUE SERÁ E O QUE NÃO SERÁ EXIGIDO**

2. **ANÁLISE DE RISCOS RESIDUAIS**

3. **ANÁLISE DE ALTERNATIVAS DE MERCADO**

4. **DEFINIÇÃO DE RESPONSABILIDADES**

Contratada	Contratante

5. **SERVIÇOS E QUANTIDADES DE USNs**

Numeração	Serviços	Quantidade de USNs	Prazo

6. **SERVIÇOS E QUANTIDADES DE USTs**

Serviços	# do Item 5 ao qual está relacionado	Quantidade de USTs	Prazo

7. **PRAZO PARA EXECUÇÃO DE TODA A DEMANDA**

Data e hora de início	Data e hora de término

Porto Alegre, ___ de _____ de _____.

_____ _____

Responsável técnico da empresa Contratada

Responsável técnico TJRS

Anexo III - Estimativa do Volume de Serviços de Computação Multinuvem

Anexo III-A - Estimativa Global Sintética de Consumo de USNs

Quantitativo Mensal Estimado (em USN)	Quantitativo Anual Estimado (em USN)
115.625	1.387.499 [12]

Anexo III-B - Estimativa Global Analítica de Consumo de USNs

Item	Descrição do Serviço	Previsão Mensal (USN)	Previsão Anual (USN)	Consumo Ano (%)
1	Máquina Virtual Linux - provisionado com 1 vCPU e 2 GB de memória RAM, por demanda	540	6.485	0,4674%
2	Máquina Virtual Linux - provisionado com 2 vCPU e 4 GB de memória RAM, por demanda	981	11.773	0,8485%
3	Máquina Virtual Linux - provisionado com 4 vCPU e 16 GB de memória RAM, por demanda	2.602	31.228	2,2507%
4	Máquina Virtual Windows - provisionado com 1 vCPU e 2 GB de memória RAM, por demanda	408	4.894	0,3527%
5	Máquina Virtual Windows - provisionado com 2 vCPU e 4 GB de memória RAM, por demanda	729	8.751	0,6307%
6	Máquina Virtual Windows - provisionado com 2 vCPU e 4 GB de memória RAM, por demanda	1.735	20.819	1,5005%
7	Serviços de Registro de Containers	32	389	0,0280%
8	Serviços de Orquestração de Containers	1.3340	160.082	11,5374%
9	Serviço Gerenciado de Publicação de Aplicações Web	584	7.009	0,5051%
10	Serviço de Armazenamento de Blocos (SSD)	229	2.753	0,1984%
11	Serviço de Armazenamento de Blocos (HDD)	46	551	0,0397%
12	Serviço de Armazenamento de Objetos - dados com maior frequência de uso	2.672	32.058	2,3105%
13	Serviço de Armazenamento de Objetos - dados com menor frequência de uso	78	931	0,0671%
14	Serviço de Armazenamento de Arquivos	251	3.018	0,2175%
15	Tráfego de Saída da Rede	58	698	0,0503%
16	Tráfego de Conexão Intra-região - serviços fornecidos em múltiplas regiões	29	349	0,0252%
17	Porta de Conexão de Fibra Ótica 1 Gbps	2.088	25.056	1,8058%
18	Porta de Conexão de Fibra Ótica 10 Gbps	3.240	38.880	2,8022%
19	Serviço de DNS - Hospedagem de Zonas	3	36	0,0026%
20	Serviço de DNS - Consultas	29	346	0,0249%
21	Serviço de Balanceamento de Carga	90	1.080	0,0778%
22	Serviço de Rede de Entrega de Conteúdo	42	508	0,0366%
23	IP Público	1	6	0,0004%
24	Serviços de Rede Privada Virtual	7	86	0,0062%
25	Serviço de VPN Gateway	716	8.597	0,6196%
26	Serviço de Gateway NAT	67	804	0,0579%
27	Serviço de Backup	50	600	0,0432%
28	Serviço de Armazenamento de Backup	88	1.051	0,0757%

[12] Cabe enfatizar que o presente quantitativo é meramente estimativo e corresponde ao somatório, em USN, de todos os serviços de computação em nuvem que poderão ser empregados. Cabe ainda salientar que a demanda real e a execução no decorrer do contrato poderá ser inferior a essa quantidade, estando o contratante desobrigado a executá-la em sua integralidade.

29	Serviço de Gateway de Armazenamento	75	900	0,0649%
30	Serviço de Diretório Gerenciado Integrado com o Microsoft Active Directory	1.128	13.530	0,9752%
31	Serviço de Auditoria e Análise de Logs	75	900	0,0649%
32	Serviço de Análise Preditiva e Criação de Modelo para Aprendizado de Máquina	38.621	463.450	33,4018%
33	Serviço Gerenciado de Execução de Funções	3	35	0,0025%
34	Serviço de Execução de Cargas de Trabalho de Computação em Lote	683	8.196	0,5907%
35	Serviço de Cofre de Chaves	2	24	0,0017%
36	Serviço Gerenciado de Certificados Digitais	2	27	0,0019%
37	Serviço de Gerenciamento de Segredos para Aplicações e APIs	0	5	0,0003%
38	Serviço de Gerenciamento de Chaves	0	3	0,0002%
39	Serviço Web Aplication Firewall	36	436	0,0314%
40	Serviço de Proteção contra Ataques DDoS	1	12	0,0009%
41	Serviço de Avaliação de Vulnerabilidades	1	6	0,0004%
42	Serviço de Banco de Dados Relacional Gerenciado	4.638	55.652	4,0110%
43	Serviço Gerenciado de "Data Warehouse"	7.085	85.018	6,1274%
44	Serviço de Banco de Dados não Relacional Gerenciado	6	73	0,0053%
45	Serviço de Migração de Banco de Dados	91	1.092	0,0787%
46	Serviço de Análise de Dados	29.373	35.2471	25,4033%
47	Serviço de Importação e Exportação de Dados	57	680	0,0490%
48	Serviço de Indexação e Pesquisa de Documentos	202	2423	0,1747%
49	Serviço de Cache em Memória	842	10.105	0,7283%
50	Serviço de Gateway de API	7	88	0,0063%
51	Serviço de Mensageria Assíncrona	2	20	0,0014%
52	Serviço de Entrega de Mensagem Eletrônica	30	360	0,0259%
53	Serviço de Codificação de Vídeo	162	1.944	0,1401%
54	Serviço de Visualização de Mapas	504	6.048	0,4359%
55	Serviço de Identificação de Robôs	720	8.640	0,6227%
56	Serviço de Transmissão de Vídeos	36	432	0,0311%
57	Serviço de Compartilhamento de Arquivos	508	6.096	0,4394%

Anexo IV - Estimativa do Volume de Serviços de Suporte Técnico Especializado

Anexo IV-A - Estimativa Global Sintética de Consumo de USTs

Quantitativo Mensal Estimado (em UST)	Quantitativo Anual Estimado (em UST)
921	11.054 [13]

Anexo IV-B - Estimativa Global Analítica de Consumo de USTs

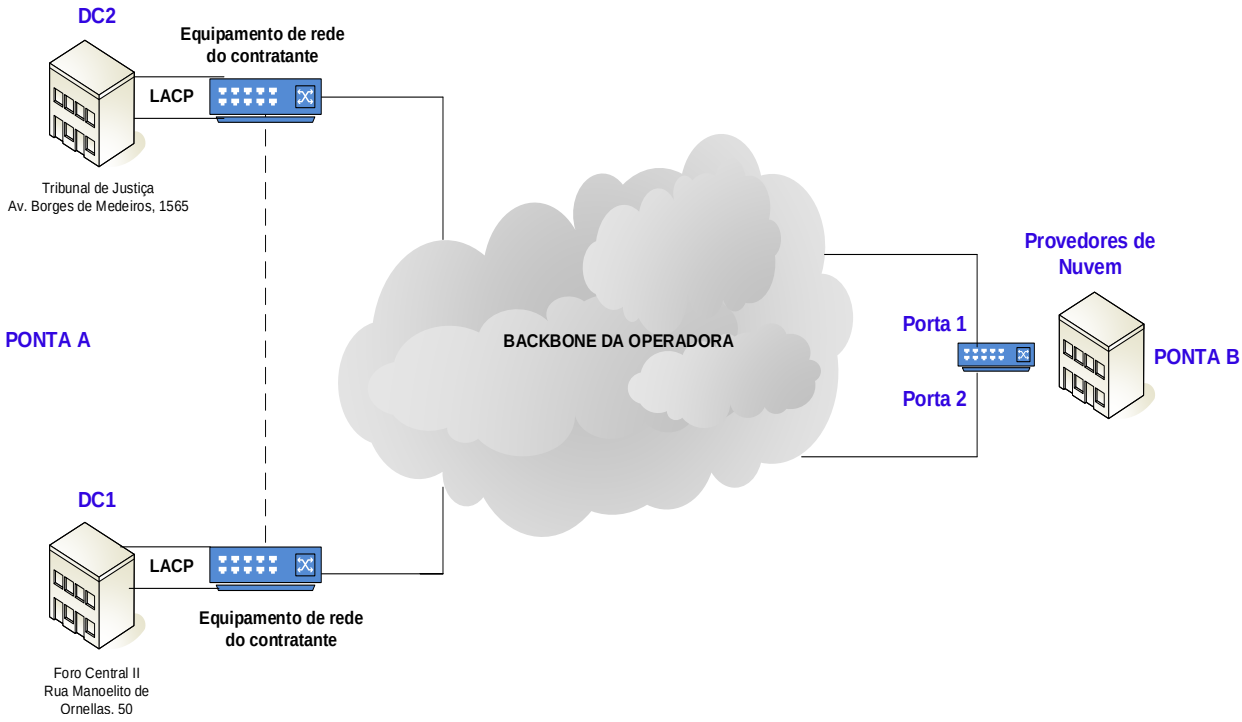
Item	Descrição do Serviço	Previsão Mensal (UST)	Previsão Anual (UST)	Consumo Ano (%)
1	Arquitetura de Solução em Nuvem	84	1008	9,1188%
2	Configuração de Máquina Virtual	7	78	0,7056%
3	Configuração de VPN Site-to-Site	5	54	0,4885%
4	Configuração de Regra de Filtragem em Firewall	3	39	0,3528%
5	Configuração de Rede Virtual	2	18	0,1628%
6	Configuração de Sub-Rede de Rede Virtual	3	39	0,3528%
7	Configuração de IP Público	1	12	0,1086%
8	Configuração de Domínio de DNS	5	54	0,4885%
9	Configuração de Balanceador de Carga	8	94	0,8467%
10	Configuração de Certificado SSL	2	18	0,1628%
11	Configuração de Disco Customizado de Sistema Operacional de Máquina Virtual	3	36	0,3257%
12	Configuração de Disco com Provisionamento de IOPS	2	18	0,1628%
13	Criptografia de Dados e Discos	3	36	0,3257%
14	Configuração de Sistema de Arquivos em Rede	13	156	1,4112%
15	Implantar Serviço de Backup	3	39	0,3528%
16	Configuração de Escalabilidade Automática (*Autoscaling*)	3	36	0,3257%
17	Hospedagem de *Containers*	21	252	2,2797%
18	Migração de Ambientes ao Término do Contrato	153	1836	16,6092%
19	Serviço de Aplicações Gerenciadas	56	672	6,0792%
20	Serviço de Banco de Dados Gerenciado	28	336	3,0396%
21	Serviço de Gerenciamento de Cache em Memória	10	117	1,0584%
22	Configuração de Gestão de Identidade, Permissões e Acessos	3	39	0,3528%
23	Configuração de Operação Assistida	52	624	5,6450%
24	Serviço de Monitoramento	1	17	0,1493%
25	Arquitetura On-Premises	84	1008	9,1188%
26	Implantar Cofre de Senhas	3	36	0,3257%
27	Configuração de Serviço de Autenticação Integrado com Microsoft ADS	10	117	1,0584%
28	Implantação de Auditoria e Análise de Logs	2	18	0,1628%
29	Configuração de Sistema de Objetos	13	156	1,4112%
30	Configuração de Gateway NAT	2	18	0,1628%
31	Serviço Gerenciado de Data Warehouse	51	612	5,5364%
32	Serviço de Banco de Dados não Gerenciado	28	336	3,0396%
33	Configuração de Firewall de Aplicação W*eb*	2	18	0,1628%
34	Configuração de Proteção contra Ataques DDOS	2	18	0,1628%
35	Serviço de Indexação e Pesquisa de Documentos	5	54	0,4885%
36	Serviço de Análise Preditiva e Criação de Modelo para Aprendizado de Máquina	123	1476	13,3525%

[13] Cabe enfatizar que o presente quantitativo é meramente estimativo e corresponde ao somatório, em UST, de todas as atividades previstas. Cabe ainda salientar que a demanda real e a execução no decorrer do contrato poderá ser inferior a essa quantidade, estando o contratante desobrigado a executá-la em sua integralidade.

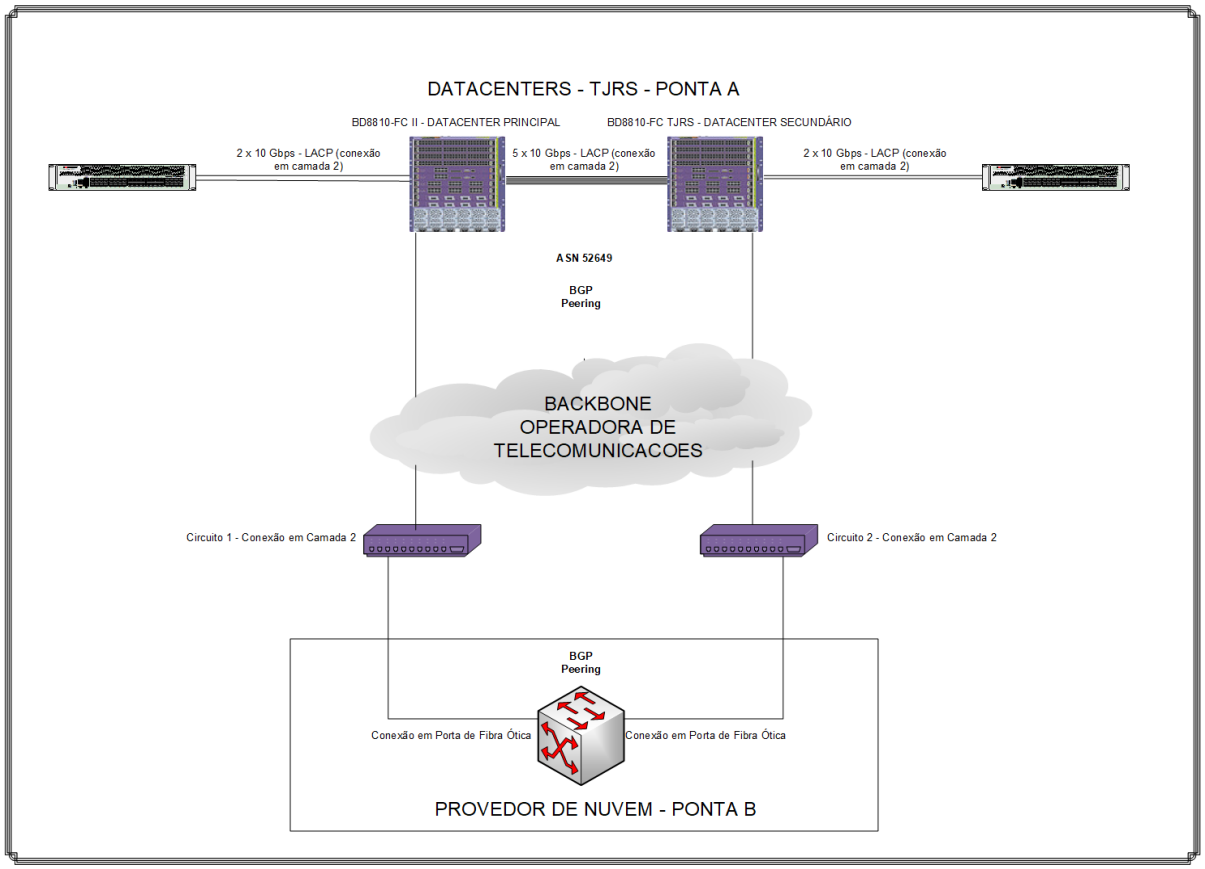
37	Serviço de Avaliação de Vulnerabilidades	2	18	0,1628%
38	Serviço Gerenciado de Execução de Funções	6	66	0,5971%
39	Serviço de Migração de Banco de Dados	11	132	1,1941%
40	Serviço de Gateway de API	6	66	0,5971%
41	Serviço de Mensageria Assíncrona	3	33	0,2985%
42	Serviço de Entrega de Mensagem Eletrônica	2	18	0,1628%
43	Implantação de Infraestrutrura de Serviços "On-Promises"	22	264	2,3883%
44	Serviço de Análise de Dados	51	612	5,5364%
45	Serviço de Importação e Exportação de Dados	5	54	0,4885%
46	Serviço de Execução de Cargas de Trabalho de Computação em Lote	8	99	0,8956%
47	Serviço de Codificação de Vídeo	2	18	0,1628%
48	Serviço de Rede de Entrega de Conteúdo	5	54	0,4885%
49	Serviço de Gateway de Armazenamento	5	54	0,4885%
50	Serviço Gerenciado de Publicação de Aplicações Web	3	36	0,3257%
51	Serviço de Gerenciamento de Segredos para Aplicações e APIs	2	18	0,1628%
52	Serviço de Gerenciamento de Chaves	2	18	0,1628%

Anexo V - Topologia de Conectividade dos Circuitos de Dados Baseados na Modalidade LAN-to-LAN para Interconexão dos Datacenters do Contratante aos Datacenters dos Provedores de Nuvem

Anexo V-A - Topologia de Conectividade - Visão Lógica



Anexo V-B - Topologia de Conectividade - Visão Física



Anexo VI - Planilha Empregada na Estimativa Preliminar dos Serviços de Computação em Nuvem e de Suporte Técnico Especializado

Estará disponível por "download" na rede mundial de computadores planilha "exemplificativa" contemplando a estimativa de consumo de USNs e USTs incluindo preços simulados dos serviços de computação em nuvem com base no método definido no item 2.1.2.6.4 visando minimizar a ocorrência de divergências nos valores precificados. Todavia, deve ser mencionado que as licitantes não estarão obrigadas a praticar tais preços visto o caráter meramente ilustrativo de tal planilha.