



PODER JUDICIÁRIO
TRIBUNAL REGIONAL FEDERAL DA 6ª REGIÃO

ESTUDO TÉCNICO PRELIMINAR - ETP COMPLETO 0266910

(para contratação de serviços e/ou aquisição de bens permanentes e de consumo por licitação)

Guia de suporte ao preenchimento do ETP: 15238786

ID (PAC):

Não se aplica, pois a contratação não foi incluída no PAC-23.

A. Descrição sucinta do objeto

Contratação de Infraestrutura como Serviço (*Infrastructure as a Service - IaaS*) para atender às necessidades de funcionamento dos sistemas do Tribunal Regional Federal da 6ª Região e das subseções judiciárias pelo período de 30 (trinta meses).

B. Justificativa expressa para a contratação

A contratação é necessária para/porque (*expor a finalidade e os motivos da necessidade da contratação*)

O *Datacenter* que atende ao Tribunal Regional Federal da 6ª Região e suas Subseções Judiciárias foi reformado no ano de 2012 para atender às necessidades da Seção Judiciária de Minas Gerais. Assim, a atual infraestrutura de TI que atende ao TRF6 foi preparada para o funcionamento de uma Seccional, razão pela qual o recebimento de sistemas anteriormente centralizados no TRF1 como o PJe, o SEI, Acordo 58, SIREA, eSiest, bancos de dados, entre outros, representou um consumo de recursos não previstos quando das aquisições, conforme cenário de escassez reportado por meio dos autos 0000724-85.2022.4.06.8000.

Diante do crescimento dos sistemas do TRF6, alguns equipamentos já obsoletos e sem garantia contratual passaram a apresentar problemas relacionados ao aumento da carga, entre os quais a queda de desempenho, travamento e até danos físicos, como ocorreu com o Switch Core de tombo 46157. Por se tratar de equipamento de alta criticidade, o defeito do Core provocou a indisponibilidade total do PJe no período de 06 a 10/02/2023 e os serviços somente foram restabelecidos após o isolamento do equipamento, o que representou a perda da redundância e a sobrecarga correspondente do outro equipamento.

Destaca-se que um ativo de rede possui uma garantia de 05 anos e a recomendação de substituição após a vigência, nos termos da [Resolução CJF nº 477/2018](#), em razão da obsolescência técnica ou funcional dos equipamentos. Por tal razão e considerando que diversos equipamentos do *Datacenter* possuem mais de 10 anos de uso, além de não atenderem à demanda técnico-operacional, torna-se necessária a substituição urgente para adequação às necessidades de funcionamento do TRF6.

A substituição de equipamentos de *Datacenter*, por sua vez, demanda a realização de aquisições de diversas áreas de operação, como as redes SAN (*Storage Area Network*), FC (*Fibre Channel*) e Ethernet. A aquisição de novos equipamentos também deve ser acompanhada do licenciamento de *softwares* necessários ao funcionamento dos serviços e sistemas, logo tantas outras contratações devem ser realizadas simultaneamente para o legal desenvolvimento das atividades. Assim, ainda que as aquisições ocorram em conjunto, os recebimentos dos equipamentos, as suas respectivas instalações e configurações de uso, assim como o licenciamento dos diversos *softwares* necessários ao funcionamento, ocorrem em diferentes etapas, o que torna a atualização da infraestrutura um procedimento extremamente moroso.

Outro fator a ser considerado é a demanda por maior espaço físico para acondicionamento das máquinas, em razão do funcionamento simultâneo até que seja realizada a transferência dos serviços. Assim, a instalação de novos equipamentos necessários ao funcionamento da infraestrutura de TI provoca o consumo de maiores recursos de energia e refrigeração durante o período de substituição.

Há, ainda, um elemento essencial à infraestrutura: a disponibilidade. Todos os sistemas do TRF6 devem estar disponíveis para funcionamento em regime de 24 x 7 (vinte e quatro horas, sete dias por semana), o que pode acarretar em situações de falhas em horários sem acompanhamento por equipe especializada e, conseqüentemente, em atraso para o início do atendimento. Considerando que os sistemas e serviços de TI do TRF6 sustentam a área finalística da instituição, torna-se cada vez mais importante que estejam hospedados em ambiente de infraestrutura tecnológica que garanta a disponibilidade e integridade das informações.

Uma alternativa que permite solucionar os problemas acima relatados é a terceirização da infraestrutura, por se tratar de uma solução disponível no mercado. A Infraestrutura como Serviço (*Infrastructure as a Service - IaaS*) já se encontra bastante difundida e permite ao contratante alocar os seus serviços e sistemas em uma nuvem pública e provida de toda a robustez, disponibilidade, segurança e suporte inerentes ao funcionamento do ambiente tecnológico. Além dos fatores citados, trata-se de uma solução que atende aos recursos demandados pelo contratante em um prazo muito mais célere e faturado conforme a utilização do serviço.

Destaca-se que a solução encontra respaldo na [Resolução CNJ nº 370/2021](#), que define em seu Art. 35:

Art. 35. Recomenda-se utilizar serviços em nuvem que simplificam a estrutura física, viabilizam a integração, requisitos aceitáveis de segurança da informação, proteção de dados, disponibilidade e padronização do uso dessa tecnologia no Poder Judiciário.

Por tudo exposto, busca-se com a presente contratação:

- B.1. Obter serviços de alta disponibilidade e com suporte prestados em regime de atendimento 24 x 7 (vinte e quatro horas, sete dias por semana);
- B.2. Reduzir a necessidade de investimento de grande vulto com a aquisição de equipamentos e suas respectivas substituições em períodos médios de 04 a 05 anos;
- B.3. Terceirizar custos operacionais e reduzir custos de infraestrutura e serviços de TI por meio de aplicações hospedadas em infraestrutura em nuvem;
- B.4. Reduzir custos de licenciamento de *softwares* utilizados pelo TRF6;
- B.5. Otimizar a produtividade da equipe de TI do TRF6, que passa a se dedicar à qualidade do serviço e ao suporte especializado;
- B.6. Ampliar os mecanismos de segurança da informação através de recursos como: retenção de dados; sistema de prevenção contra de perda de dados; controle de acesso e gerenciamento de dispositivos, aplicativos e auditoria;
- B.7. Disponibilidade dos serviços em produção;
- B.8. Redução de custos de manutenção e melhor eficiência pelo uso racional dos recursos;
- B.9. Possibilitar o ajuste, sob demanda, da capacidade dessas aplicações, sistemas e serviços;
- B.10. Possibilitar, ainda, a disponibilização de novas aplicações, sistemas e serviços.
- B.11. Agilizar o processo de aquisição, de forma a garantir o restabelecimento da infraestrutura necessária o mais rápido possível e, ainda, a manutenção do parque tecnológico atualizado com menor esforço;
- B.12. Terceirização dos custos para fornecimento de energia, refrigeração, monitoramento, segurança física, prevenção e combate a incêndio;
- B.13. Redução da dependência de pessoal interno qualificado, permitindo que os servidores possam focar na gestão do poder computacional contratado;
- B.14. Modernização de acesso à rede de modo ubíquo, conveniente e sob demanda, utilizando recursos computacionais configuráveis.

A não contratação implicará (expor as conseqüências advindas da não contratação)

A não contratação poderá ensejar a parada dos sistemas de TI caso os equipamentos que integram a infraestrutura do *Datacenter* do TRF6 não suportem a demanda ou mesmo a piora da performance atual dos sistemas como o PJe e SEI.

C. Alinhamento da demanda com diretrizes e metas institucionais

- [Resolução CNJ nº 370, de 28 de janeiro de 2021 - Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário \(ENTIC-JUD\);](#)
- [Resolução CJF nº 685, de 15 de dezembro de 2020 - Plano Estratégico de Tecnologia da Informação da Justiça Federal](#)

Macrodesafio: Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados

Objetivos Estratégicos da Justiça Federal:

- 1) Aperfeiçoar e assegurar a efetividade dos serviços de TI para a Justiça Federal

Indicadores	Metas
1 - Índice de satisfação dos clientes internos com os serviços de TI.	1 - Atingir, até 2025, 85% de satisfação dos clientes internos de TI.
2 - Índice de satisfação dos clientes externos com os serviços de TI.	2 - Atingir, até 2026, 80% de satisfação dos clientes externos de TI.

D. Proposta de solução

D.1. Alternativas de solução disponíveis no mercado

Solução nº	Descrição das alternativas de solução disponíveis no mercado	Fontes de consulta (órgãos públicos que adotaram a solução, fornecedores etc.)	Link das consultas (doc. SEI)
01	PREGÃO 04/2022 - Contratação de solução integrada de serviços de hospedagem de web sites, bancos de dados e segurança gerenciada 24x7 (vinte e quatro horas por dia, sete dias por semana) no modelo Cloud SaaS (Nuvem, Software como Serviço), englobando provimento de infraestrutura e respectivo gerenciamento, serviços de DNS, gestão de vulnerabilidades, teste de intrusão, resposta a incidentes, segurança de aplicações, backup e monitoramento de aplicações e sistemas dos serviços providos em regime 24x7	CONSELHO FEDERAL DE CONTABILIDADE - CFC	0238409
02	PREGÃO 0044/2021 - Contratação de empresa especializada para o fornecimento de Sistema de Gestão Integrada - SGI hospedado em Infraestrutura Computacional de Nuvem, contemplando todos os serviços necessários ao pleno funcionamento da solução, incluindo os serviços de segurança de dados, controle de acesso, backup e restauração/reocupação de dados, desenvolvido 100% por Tecnologia Web, englobando licenças de cessão de direito de uso do software para quantidade ilimitada de usuários	CONSELHO REGIONAL DE MEDICINA DO ESTADO DE SÃO PAULO - CREMESP	0238430
03	PREGÃO 105/2022 - Contratação de empresa especializada para prestação de serviços gerenciados de computação em nuvem, incluindo a concepção, projeto, provisionamento, configuração, migração, suporte, manutenção e gestão de topologias de serviços em dois provedores de nuvem pública, visando a atender às necessidades do Poder Judiciário do Estado do Espírito Santo	PODER JUDICIÁRIO DO ESTADO DO ESPÍRITO SANTO - PJES	0238467
04	PREGÃO 78/2022 - Aquisição de solução de armazenamento consolidado de dados, com garantia de funcionamento pelo período mínimo de 60 (sessenta) meses, incluindo serviços de instalação, configuração, ativação, migração de dados e capacitação operacional.	CÂMARA DOS DEPUTADOS	0238485
05	Aquisição de Equipamentos para Datacenter - Servidores para Bancos de Dados, Switches Fibre Channel, Fitoteca, Servidores para Virtualização, Backup e Ambiente de Desenvolvimento	CONTRATOS TRF1	0240072 0240084 0240087 0240091 0240095
06	Licenciamento de Softwares - VMware, Linux Red Hat, Microsoft Windows Server, Microsoft Windows Server, Remote Desktop, SQL Server e Suporte Premier.	BANCO DE PREÇOS	0245306 0245322 0245332 0245349

D.2. Estimativa de preços das alternativas de solução

Solução nº	Órgãos Contratantes	Valores Anuais
01	CONSELHO FEDERAL DE CONTABILIDADE - CFC	R\$ 2.226.666,60 0238413
02	CONSELHO REGIONAL DE MEDICINA DO ESTADO DE SÃO PAULO - CREMESP	R\$ 4.414.982,86 0238433
03	PODER JUDICIÁRIO DO ESTADO DO ESPÍRITO SANTO - PJES	R\$ 9.357.921,33 0238469
04	CÂMARA DOS DEPUTADOS	R\$ 6.274.339,78 0238486
05	TRIBUNAL REGIONAL FEDERAL DA 1ª REGIÃO	R\$ 1.564.366,07 0240072 0240084 0240087 0240091 0240095
06	AQUISIÇÕES DE EQUIPAMENTOS E LICENCIAMENTOS	R\$ 29.072.831,03 (vide tabela abaixo)

D.2.1. Solução On-premises

Trata-se da solução adotada pelo TRF1 e no TRF6, baseada em aquisição de equipamentos e licenciamentos de softwares nec ao funcionamento dos serviços e sistemas.

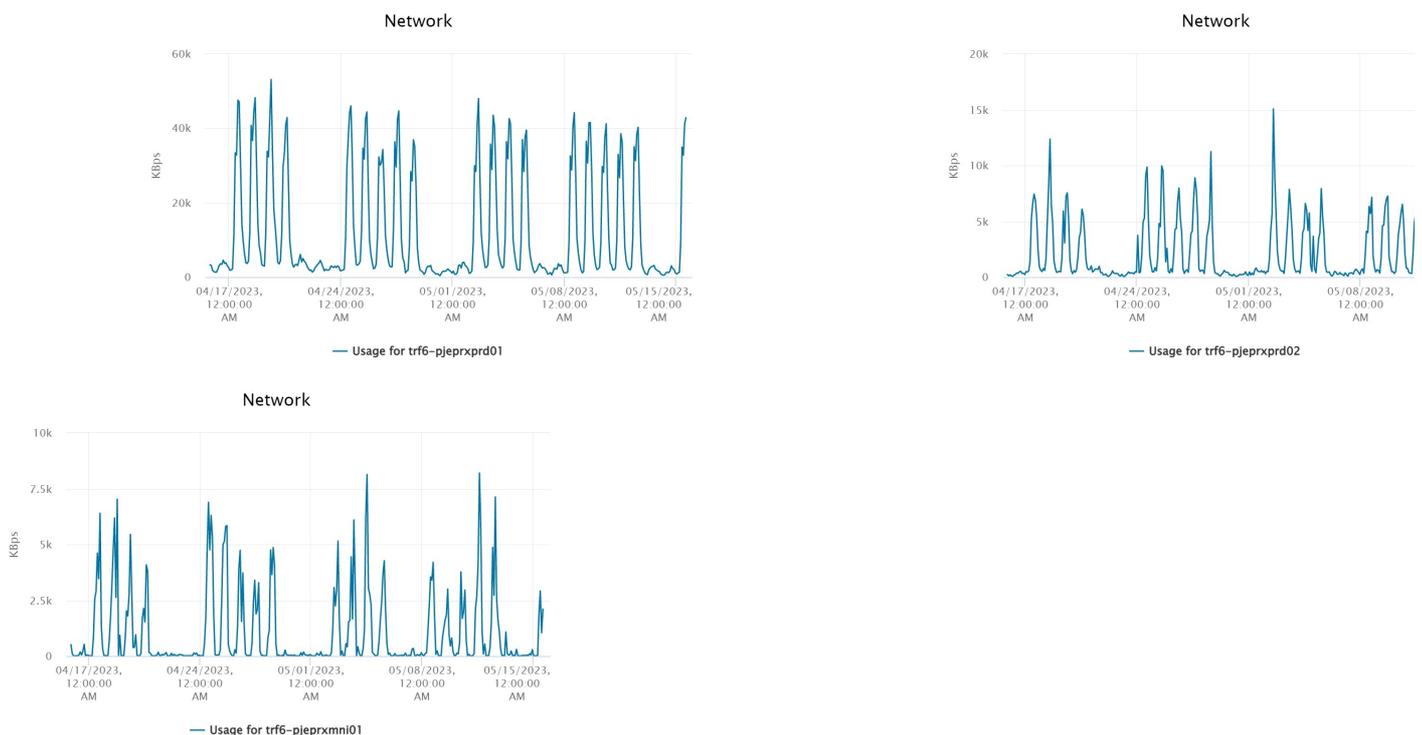
A planilha abaixo detalha a necessidade atual de recursos para o funcionamento do TRF6:

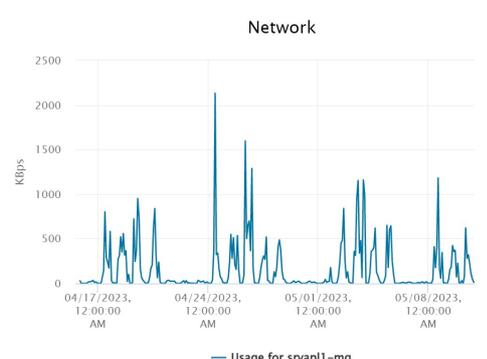
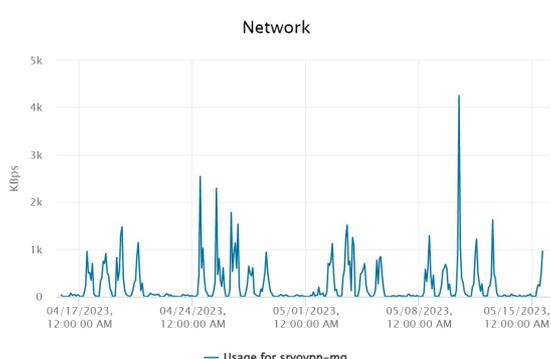
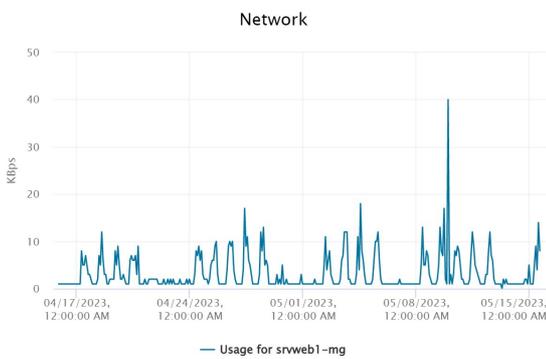
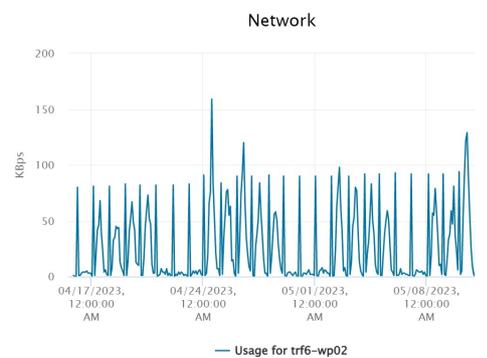
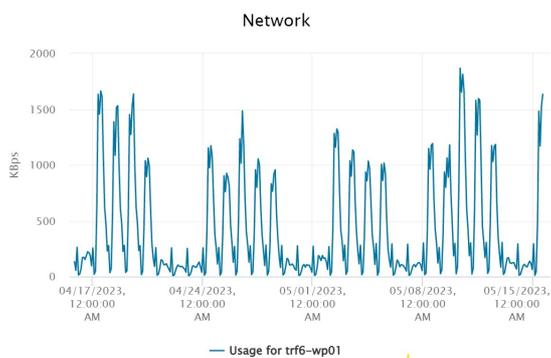
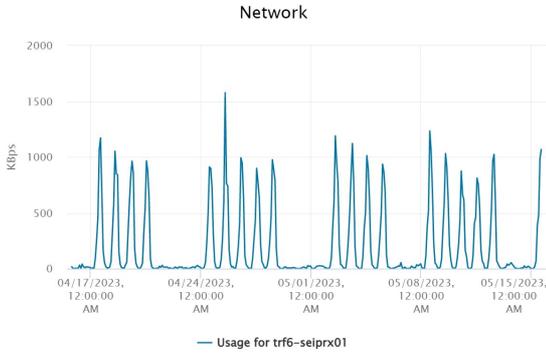
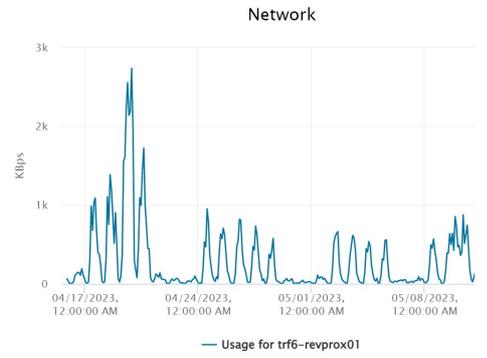
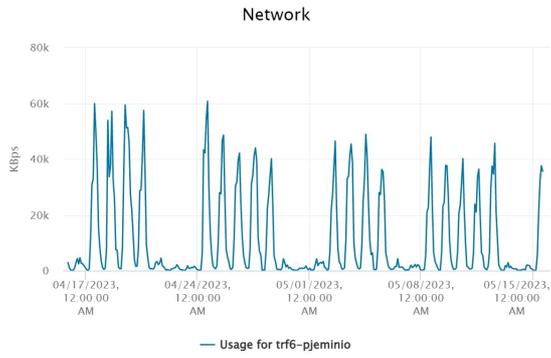
Recursos Necessários		Quantidades	Valores Unitários	Valores Totais	
Equipamentos	Armazenamento 1G	30,35 TB	Aquisição realizada (0001696- 55.2022.4.06.8000)	Aquisição realizada (0001696- 55.2022.4.06.8000)	
	Armazenamento 2G	9,92 TB			
	Acréscimo anual estimado	30 TB			
	Servidores de Banco de Dados	2	R\$ 35.660,00 0240072	R\$ 71.320,00	
	Switches Fibre Channel	2	R\$ 80.315,00 0240084	R\$ 160.630,00	
	Fitoteca	1	R\$ 293.220,07 0240087	R\$ 293.220,07	
	Servidores de Backup	2	R\$ 43.800,00 0240095	R\$ 87.600,00	
	Servidor Banco Clone	1	R\$ 52.700,00 0240095	R\$ 52.700,00	
	Servidores de Virtualização	6	R\$ 149.816,00 0240091	R\$ 898.896,00	
	Memória Sistemas 1G	580 GB	Incluído nos servidores de virtualização	Incluído nos servidores de virtualização	
	Memória Sistemas 2G	272 GB			
	Total em Equipamentos				R\$ 1.564.366,07
	Licenciamentos Anuais	VMWare Vcenter Server	1	R\$ 46.037,41 0245317	R\$ 46.037,41
VMWare ESXi hosts		32 *	R\$ 9.163,10 0245317	R\$ 293.219,20	
VMWare vCPUs 1G		260	R\$ 16.100,29 0245310	R\$ 4.186.074,53	
VMWare vCPUs 2G		68	R\$ 16.100,29 0245310	R\$ 1.094.819,49	
VMWare Suporte		1	R\$ 58.674,84 0245310	R\$ 58.674,84	
Linux Red Hat		90	R\$ 109.386,28 0245327	R\$ 9.844.764,75	
Linux Red Hat Suporte		500	R\$ 590,00 0245327	R\$ 295.000,00	
Microsoft Windows Server		250	R\$ 33.847,48 0245343	R\$ 8.461.870,00	
Microsoft Windows RDP		3.600	R\$ 797,69 0245343	R\$ 2.871.684,00	
Microsoft SQL Server		2	R\$ 23.191,37 0245343	R\$ 46.382,74	
Microsoft Suporte Premier		200	R\$ 1.549,69 0245387	R\$ 309.938,00	
Total em Licenciamentos Anuais				R\$ 27.508.464,96	
TOTAL GERAL				R\$ 29.072.831,03	

D.2.2. Solução de Infraestrutura como Serviço (*Infrastructure as a Service - IaaS*)

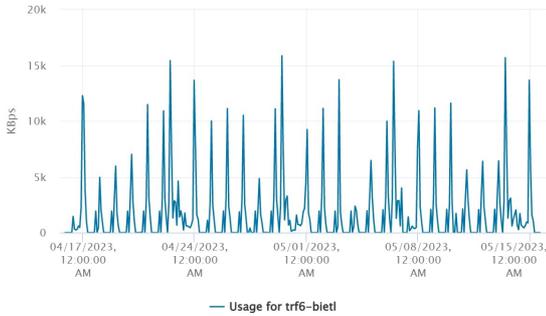
A solução envolve a disponibilização de infraestrutura em nuvem que permite ao contratante o gerenciamento do ambiente, a possibilidade de alteração de recursos das máquinas virtuais e até mesmo a inclusão ou remoção de serviços.

Destaca-se que, por falta de ferramenta de gerência, os tráfegos internos e externos somente podem ser estimados por consumos dos recursos de rede das máquinas virtuais, conforme gráficos abaixo:

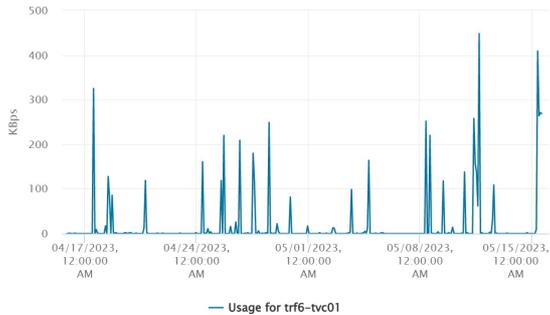




Network



Network



Como o tráfego de saída normalmente é faturado pelos provedores de nuvem, deve-se considerar os valores abaixo para a es da contratação:

Tráfegos / Serviços	Pje 1G	Pje 2G	Pje MNI	Pje minIO	Certidão	SEI	Portal	Intranet	Sistemas Próprios	VPN	Servidor de Aplicações	Estatística	TV Corporativa	Totais Mensais
Tráfego Médio Mensal (KBps)	30.000	8.000	6.000	40.000	1.000	1.000	1.250	100	10.000	1.400	750	7.250	150	106.900
Tráfego Máximo Mensal (KBps)	55.000	15.000	8.200	60.000	2.800	1.600	1.900	160	40.000	4.250	2.200	16.000	450	207.560

A planilha abaixo detalha os recursos de máquinas virtuais, armazenamento e bancos de dados necessários ao atual funcio do TRF6:

Recursos	Quantidades	Valores Mensais Estimados
Bancos de Dados	15	R\$ 1.187.435,98 (Valores Ata ME, disponível em https://nuvemgoverno.com.br/ , acesso em 19/05/2023)
Armazenamento	41 TB	
Máquinas Virtuais Linux	250	
Máquinas Virtuais Windows	200	
Backup	41 TB	
Tráfego	106.900 KBps	

The screenshot shows the 'Resultado - Relatório de Custos Estimados' page on the Nuvem Governo website. It lists various cloud service categories and their estimated costs in US dollars (US\$).

Category	Estimated Cost (US\$)
Tabela 2 - IaaS - VMs, Storage e Rede - Mensal	115.550,80
Tabela 2 - IaaS - VMs, Storage e Rede - Anual	1.386.699,60
Tabela 2 - IaaS - Outros - Mensal	7.393,61
Tabela 2 - IaaS - Outros - Anual	88.723,32
Tabela 3 - PaaS - Mensal	38.353,56
Tabela 3 - PaaS - Anual	460.242,72
Tabela 4 - SaaS - Mensal	1.265,09
Tabela 4 - SaaS - Anual	15.181,08
Total Mensal USN	162.563,06
Total Anual USN	1.950.756,72
Total Mensal em R\$	R\$ 1.187.435,98
Total Anual em R\$	R\$ 14.249.231,76

D.2.3. Solução de Plataforma como Serviço (*Platform as a Service - PaaS*)

A solução representa a disponibilização de um ambiente mais restrito que o da Infraestrutura como Serviço, pois o gerenciamento é realizado pelo provedor de nuvem. Trata-se de um modelo recomendado para serviços estáveis e que não dependem de maiores monitoramentos e evoluções, pois já se encontram em níveis avançados de maturidade operacional. Diante das dificuldades operacionais do TRF6, a solução é passível de utilização no momento.

D.2.4. Solução de Software como Serviço (*Software as a Service - SaaS*)

A solução representa a disponibilização de um serviço completo para atendimento de determinadas necessidades, logotipo e gerência do contratante. Não é viável, portanto, como solução para o TRF6 devido à fragmentação dos inúmeros serviços e sistemas atualmente em utilização.

D.3. Razões da escolha da melhor solução (justificar técnica e economicamente o que o levou a escolher a solução)

O funcionamento do TRF6 depende consideravelmente da ampliação dos recursos de infraestrutura de TI, conforme ce escassez reportado por meio dos autos 0000724-85.2022.4.06.8000. Tais necessidades podem ser atendidas por meio de uma única contra Infraestrutura como Serviço (*Infrastructure as a Service - IaaS*), ou por meio de contratações de equipamentos e licenciamentos diversos, avaliados conforme a estratégia do contratante e as disponibilidades de recursos humanos, orçamentários, temporais, entre outros.

A opção pela contratação de equipamentos e licenciamentos diversos implica em um prazo consideravelmente superior implementação, uma vez que além das aquisições é preciso realizar as interconexões e configurações para o funcionamento. Como consequência exige a disponibilidade de espaço físico em Datacenter, além de maiores consumos de recursos de energia elétrica e de climatização e condicionamento dos equipamentos.

As aquisições de equipamentos e licenciamentos devem necessariamente prever o crescimento estimado da demanda, porém por limitar a implementação de novos projetos devido à uma eventual falta dos recursos. Por outro lado, é possível, ainda, que os bens e se tornem ociosos caso a estratégia de operação do contratante seja direcionada a outras atividades, o que representaria um desperdício de recursos envolvidos.

A análise de custos de aquisições de equipamentos já aponta um custo elevado para a aquisição, além do prazo envolvido recebimento e entrada em produção. Percebe-se, ainda, que os valores referentes aos licenciamentos representam a parcela mais relevante da contratação se refere aos licenciamentos de *softwares*, pois atualmente a comercialização mais usual é realizada por meio de aquisições periódicas, como ocorre com o VMware e Office 365.

Há que se considerar, ainda, que as contratações fragmentadas exigem maiores recursos humanos para a efetivação. Considera-se que as contratações de soluções de TIC obedecem a uma normativa específica ([Resolução CNJ nº 468/2022](#)) e mais complexa que a contratação comum, torna-se necessário o envolvimento de muitas unidades e de servidores para a efetivação. Assim, além da complexidade técnica correspondente, as aquisições de soluções de TIC normalmente exigem também um envolvimento de um quantitativo maior de servidores em um prazo maior para a conclusão.

Pelo exposto, a solução de ambiente *on-premises* se mostra, assim, a mais onerosa entre as opções avaliadas e a que demanda o maior tempo de implementação, o que torna inviável a sua utilização.

O Conselho Nacional de Justiça (CNJ) corrobora, por meio do [Resolução nº 370/2021](#), com a utilização de soluções de nuvem para disciplinar que:

Art. 35. Recomenda-se utilizar serviços em nuvem que simplifiquem a estrutura física, viabilizem a integração, requisitos de segurança da informação, proteção de dados, disponibilidade e padronização do uso dessa tecnologia no Poder Judiciário.

Entre os modelos de nuvem, as soluções de Plataforma como Serviço (*Platform as a Service - PaaS*) e de Software como Serviço (*Software as a Service - SaaS*) se mostram opções vantajosas para sistemas estáveis, pois a gerência ou mesmo o fornecimento é realizado pelo operador de nuvem. Considerando-se que o TRF6 utiliza um grande número de sistemas e muitos deles sem qualquer comunicação com o usuário final, como Oracle e PJe, as soluções se tornam inviáveis para utilização. É possível, todavia, que após a operação em nuvem e a adoção dos sistemas e serviços seja possível a adoção dos modelos no futuro.

A solução de Infraestrutura como Serviço (*Infrastructure as a Service - IaaS*) utiliza recursos de terceiros para hospedar sistemas e sistemas do contratante, conforme a demanda de utilização. Trata-se, portanto, de um serviço dinâmico que está diretamente relacionado ao consumo, pois os recursos podem ser remanejados, reduzidos ou ampliados de acordo com a necessidade do contratante. Como consequência as aplicações podem ser reajustadas para funcionamento conforme a necessidade e eventuais recursos sobressalentes podem ser direcionados para outros serviços e sistemas.

Além da flexibilidade de utilização dos recursos, o modelo de *IaaS* possui uma grande vantagem: o prazo curto usualmente necessário para implementação. Como exemplo de tal dinamismo, a contratação promovida pelo TJES (0238467) previu o início de execução dos serviços até 20 (vinte) dias úteis após a notificação da contratação.

Com a utilização de uma nuvem pública, garante-se aos serviços e sistemas do TRF6 uma alta disponibilidade, incluindo o suporte especializado. Consequentemente, a produtividade da equipe de TI do TRF6 é otimizada, pois direciona os esforços à qualidade do serviço e suporte especializado. Assim, a área técnica aciona a contratada para a execução das atividades sob a fiscalização daquela e mediante a celebração de acordos de níveis de serviço (ANSs) caso não cumpridos os prazos pré-estabelecidos para a execução.

Outra considerável vantagem da nuvem pública é a segurança de dados envolvida, pois o ambiente é monitorado constantemente por especialistas do prestador. As questões de segurança demandam grande especialização e constantes atualizações, razão pela qual é afirmado que a contratação representa um incremento em relação ao serviço envolvido em ambiente *on-premises* do TRF6.

Em relação aos recursos orçamentários, destaca-se que o faturamento acompanha o consumo dos recursos de nuvem. Portanto, assim, a preparação e manutenção do ambiente e os custos decorrentes da aquisição de equipamentos, licenciamentos, energia, refrigeração, monitoramento, segurança física, prevenção e combate a incêndio, entre outros. Deve-se considerar que o ambiente do TRF6 foi preparado com licenciamentos precários fornecidos pelo TRF1, logo alguns licenciamentos deverão ser realizados ainda que seja adotada a solução de Infraestrutura como Serviço (*Infrastructure as a Service - IaaS*), pois persistirá o ambiente *on-premises* para o funcionamento de outros sistemas. Ainda assim, quanto maior o ambiente migrado para a nuvem, proporcionalmente menor será o licenciamento para o ambiente *on-premises*.

É importante destacar que o uso racional dos recursos depende do adequado dimensionamento da necessidade. Por isso, levantou-se no item D.2 os recursos tecnológicos necessários ao funcionamento de sistemas do TRF6 e os respectivos valores para a aquisição e implementação em produção, utilizando-se como parâmetros os valores de aquisição dos equipamentos pelo TRF1 e de outras contratações públicas.

Por tudo exposto e diante da escassez de recursos tecnológicos, humanos e temporais para a estabilização dos sistemas processuais administrativos do TRF6, a solução de Infraestrutura como Serviço (*Infrastructure as a Service - IaaS*) se mostra a mais adequada.

D.4. Justificativas para o parcelamento ou não da solução

Justifica-se o não parcelamento do objeto, em razão da interdependência entre os serviços que compõe o objeto da contratação, considerando-se o grau de interação do conjunto de serviços técnicos, assim como a sua natureza específica e o seu caráter contínuo, aliada criticidade e à complexidade da infraestrutura apoiada.

O fracionamento da solução objeto poderia expor a risco a qualidade e a disponibilidade do ambiente tecnológico da JF6, já seria possível delimitar as responsabilidades, tarefas e ações caso haja mais de um fornecedor dentro do processo de execução dos serviços.

Seguem abaixo algumas considerações técnicas adicionais para o não parcelamento do objeto:

- Quando analisado sob os aspectos técnicos, percebe-se o inter-relacionamento e a interdependência entre os serviços a serem contratados, a impossibilidade de estabelecimento dos limites, por serem extremamente tênues, de início e término das repercussões entre um e outro. Destacam-se as metas de alcance de maturidade, alta disponibilidade e a gestão de riscos de um mesmo ambiente de infraestrutura, em que cada atividade contribuirá em aspectos distintos.
- Para a adequada execução dos serviços ora contratados é fundamental que esteja assegurada a unidade conceitual de todas as atividades técnicas, que no conjunto compõem um todo uno e indivisível, entrelaçado com coerência tecnológica e direcionado para o resultado esperado, que é a disponibilidade do ambiente de infraestrutura de TI, incluídos todos os aspectos necessários ao pleno atendimento das necessidades dos usuários destes serviços.
- A indivisibilidade do objeto é imprescindível, pois tecnicamente e gerencialmente é inviável que os serviços sejam fornecidos por duas contratadas, uma vez que traz ônus direto de maior custo gerencial para controle, além do maior custo gerencial para gestão de contratos constituindo todos estes benefícios em vantagem técnica e economicidade.
- No tocante à economicidade, particionar o objeto poderia impactar diretamente os custos globais da contratação, uma vez que a execução dos serviços por um único prestador tende a permitir ganhos de escala e possibilita a diluição do custo do *overhead* administrativo por um maior número de profissionais alocados para atendimento dos serviços. A gestão e a fiscalização de um número maior de contratos para a execução dos serviços de infraestrutura aumentariam também os custos indiretos com recursos humanos da CONTRATANTE a serem alocados para esta atividade.
- Contratar prestadores distintos para a execução do serviço poderia trazer conflitos de responsabilidades entre as contratadas, prejudicando sobremaneira a execução contratual e a fiscalização por parte da CONTRATANTE.

D.4.1. Aplicação de cotas a microempresas (ME) e empresas de pequeno porte (EPP) (somente para bens de natureza divisível)

Não se aplica, em virtude da impossibilidade de divisão da prestação de serviços.

E. Requisitos da solução escolhida

E.1. Requisitos qualitativos e quantitativos (e análise das contratações anteriores)

NECESSIDADES DE NEGÓCIO

1. REQUISITOS TÉCNICOS DA SOLUÇÃO

1.1. DOS TERMOS E DEFINIÇÕES UTILIZADOS NA DESCRIÇÃO DOS SERVIÇOS

Com a finalidade de definir uma nomenclatura comum às pretensas licitantes, descreve-se a seguir o significado dos termos técnicos utilizados neste documento:

1.1.1. Computação em nuvem: é um modelo para permitir que o provisionamento de recursos e serviços possam ser realizados em qualquer lugar e a qualquer momento, de maneira conveniente, com acesso por meio de rede a recursos computacionais configuráveis tais como redes, servidores, armazenamento, aplicações e serviços, que podem ser rapidamente provisionados e devolvidos com o mínimo de esforço em gerenciamento ou interatividade com o provedor de serviços;

1.1.2. Características essenciais de computação em nuvem:

1.1.2.1. Autoserviço sob demanda - O cliente pode, unilateralmente, provisionar a capacidade computacional necessária como servidores e redes de armazenamento, de maneira automática, portanto sem precisar de interação humana com o provedor de serviços em nuvem.

1.1.2.2. Amplo acesso pela rede - Os recursos computacionais estarão disponíveis por meio da rede e acessados por meio de mecanismos padrões que promovem o uso heterogêneo de plataformas clientes, tais como smartphones, tablets, laptops e estações de trabalho.

1.1.2.3. Grupo de recursos - Os recursos do provedor de serviços em nuvem são agrupados para servir múltiplos clientes usando o modelo *single-tenant* ou *multi-tenant*, com diferentes recursos físicos e virtuais, dinamicamente alocados e realocados conforme demanda, tais como armazenamento, processamento, memória e largura de banda de rede.

1.1.2.4. Rápida Elasticidade - As capacidades podem ser elasticamente aumentadas ou diminuídas de acordo com a demanda atual e o perfil de uso das aplicações. Essas alterações podem ser realizadas a qualquer momento, possibilitando otimização do uso de recursos e consequente economia de valores.

1.1.2.5. Serviço Mensurado - Os sistemas em nuvem automaticamente controlam e otimizam o uso de recursos, considerando-se as capacidades de monitoramento em um nível apropriado para o tipo de serviço, tais como armazenamento, processamento, largura de banda e usuários ativos por contas. O uso de recursos pode ser monitorado, controlado e reportado de forma a garantir transparência tanto para o provedor quanto para o consumidor do serviço utilizado.

1.1.3. Modelo de Serviços em nuvem IaaS - *Infrastructure as a Service* (Infraestrutura como Serviço): capacidade fornecida ao cliente para provisionar processamento, armazenamento, comunicação de rede e outros recursos de computação fundamentais para a execução de aplicações. O cliente pode instalar e executar softwares em geral, incluindo sistemas operacionais e aplicativos. O cliente não gere nem controla a infraestrutura na nuvem subjacente, mas tem controle sobre os sistemas operacionais, armazenamento e aplicativos instalados, e possivelmente, um controle limitado de alguns componentes de rede.

1.1.4. Modelo de Serviços em nuvem PaaS - *Platform as a Service* (Plataforma como Serviço): capacidade fornecida ao cliente para provisionar na infraestrutura de nuvem aplicações adquiridas ou criadas para o cliente, desenvolvidas com linguagem de programação, bibliotecas, serviços e ferramentas suportados pelo provedor de serviços em nuvem. O cliente não gerencia nem controla a infraestrutura na 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.

1.1.5. Modelo de Serviços em nuvem SaaS - *Software as a Service* (Software como Serviço): capacidade de fornecer uma solução de software completa que pode ser contratada de um provedor de serviços em nuvem. Toda a infraestrutura subjacente, incluindo software de aplicativo e dados de aplicativo ficam no datacenter do provedor de serviços. O provedor de serviço gerencia hardware, software, garante a disponibilidade e a segurança do aplicativo e de seus dados.

1.1.6. Provedor de Serviços em Nuvem: prestador que possui infraestrutura de tecnologia da informação (TI) destinada ao fornecimento de infraestrutura, plataformas e aplicativos baseados em computação em nuvem.

1.1.7. Integrador de Serviços de Nuvem: parceiro de Serviço de Nuvem (Cloud Broker) que oferece serviços profissionais gerenciados relacionados a operações de infraestrutura de um ou mais provedores de nuvem pública. O integrador deve ser capaz de oferecer três pilares de recursos: uma plataforma de gerenciamento de recursos de nuvem (*Cloud Management Platform*) - serviços profissionais de gerenciamento; e operação, implementação e consultoria contínua sobre os serviços gerenciados.

1.1.8. Nuvem Pública: infraestrutura de computação em nuvem pertencente a um provedor de serviços em nuvem e gerencia ele. Os recursos computacionais são baseados em virtualização, agrupados e compartilhados entre clientes, e acessados via IP ou uma conexão de rede dedicada. O uso dos recursos é monitorado e pago conforme o uso.

1.1.9. Datacenter: instalação construída com o objetivo de alojar recursos em nuvem, tais como servidores e outros equipamentos baseados no modelo "as a Service" (como serviço). Um datacenter é uma infraestrutura que centraliza as operações e equipamentos de TI de um provedor de serviços em nuvem e o local de armazenamento e gerenciamento dos dados dos clientes.

1.1.10. Solução de Tecnologia da Informação: conjunto de bens e/ou serviços de TI e automação que se integram para o alcançar resultados pretendidos com a contratação. Integram a Solução os recursos de computação em nuvem, a plataforma de gestão em nuvem, os serviços de gerenciamento, migração e treinamento.

1.1.11. Orquestração: habilidade de coordenar e gerenciar recursos em diferentes provedores de nuvem públicas.

1.1.12. Serviço na modalidade por reserva de recurso: serviços reservados previamente por um período de um ano ou mais com faturamento mensal. Para efeitos desta contratação não será aceito pagamento adiantado (*upfront*).

1.1.13. Serviço na modalidade por demanda: serviços alocados por demanda, sem um período predeterminado de alocação de recursos e com faturamento periódico, conforme a Ordem de Serviço.

1.1.14. Máquina virtual: ambiente computacional implementado em uma máquina física, a partir de tecnologias de virtualização. Este ambiente possui, minimamente, seu próprio processador, memória RAM e interface de rede, podendo a ele serem agregados outros componentes como, por exemplo, volumes de armazenamento (*storage*).

1.1.15. Máquina virtual de uso genérico: são as máquinas virtuais utilizadas para propósito geral, com cargas de trabalho que requerem equilíbrio entre processamento e memória.

1.1.16. Instância de Computação: corresponde a um componente de computação em nuvem composto de máquina virtual e serviços agregados, tais como armazenamento, componentes de rede e demais serviços que mantenham essa máquina virtual em operação.

1.1.17. Instância de Banco de Dados: corresponde a uma plataforma de banco de dados gerenciado. Uma instância de banco de dados pode conter várias bases de dados de um mesmo tipo criadas pelo usuário. É possível acessar a instância de banco de dados usando as mesmas ferramentas e os mesmos aplicativos.

1.1.18. Carga de trabalho (*Workload*): conjunto de recursos que compõem uma arquitetura técnica destinada a suportar um conjunto de serviços de TI. As cargas de trabalho podem requerer uma ou mais instâncias e recursos de computação para agregar valor ao negócio por meio de serviços de TI.

1.1.19. Região: agrupamentos de localizações geográficas específicas em que os recursos computacionais se encontram hospedados. Considera-se que o território brasileiro está localizado em uma única região.

1.1.20. Zona: locais isolados dentro de cada região dos quais os serviços de nuvem pública se originam e operam.

1.1.21. Multinuvem: uma estratégia de utilização dos serviços de computação em nuvem por meio de dois ou mais provedores de nuvem pública.

1.1.22. Metadado: Dados estruturados que descrevem e permitem encontrar, gerenciar, compreender e/ou preservar documentos arquivísticos ao longo do tempo.

1.1.23. Marketplace: Loja online operada por um provedor de nuvem que oferece acesso a aplicativos de software e serviços que são desenvolvidos ou que se integram ou complementam as soluções disponibilizadas pelo provedor de nuvem.

1.2. DAS MÉTRICAS PARA ACIONAMENTO DOS SERVIÇOS DE COMPUTAÇÃO EM NUVEM

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

1.2.2. A USN visa a se estabelecer como método previsível, linear e flexível para obtenção de uma quantidade objetiva definida a ser cobrada pelos serviços de computação em nuvem e consiste no estabelecimento de valor de referência específico para cada tipo de serviço, conforme métrica individual associada ao consumo dos recursos.

1.2.3. O fator de USN utilizado neste documento é composto pela média aritmética simples dos valores praticados por diferentes provedores. Essa métrica visa a padronizar a relevância entre os serviços em termos de custo operacional, logo foi utilizada a referência dos valores praticados pelos provedores em dólar na região de hospedagem referente ao Brasil. Ressalta-se que essa métrica (USN) é um valor adimensional que diferencia a relevância de um recurso/serviço frente aos demais constantes no catálogo do provedor. Logo, não se deve confundir essa medida de esforço computacional, que representa os recursos envolvidos para a prestação do serviço, com os valores para cada unidade de USN, que será ofertada em reais (R\$) pelo *broker* ou integrador oportunamente no momento do pregão.

1.2.4. O detalhamento dos valores obtidos para a composição dos fatores da USN de cada serviço está descrito no Anexo 1 (Termo de Referência).

1.2.5. 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 para a CONTRATANTE.

1.2.6. Ao menos um provedor disponibilizado pela CONTRATADA deverá fornecer todos os serviços listados na Tabela 1, conforme as descrições e níveis mínimos de serviço respectivos, assegurando compatibilidade à plataforma do provedor de computação em nuvem por meio de soluções constantes no catálogo ou em ferramenta de *marketplace* do provedor.

1.2.7. No caso do fornecimento do serviço por meio de ferramenta de *marketplace* do provedor, a referida ferramenta deverá ser passível de mensuração na mesma métrica definida para os serviços da Tabela 1, para fins de medição e cobrança do quantum de USN consumido pelo serviço.

1.2.8. Deverá ser disponibilizado pela CONTRATADA um portal contendo informações sobre:

1.2.8.1. Planilha de preços: valores praticados pela CONTRATADA com os preços de todos os serviços (em USN) e informações de quais serviços do provedor são gratuitos;

1.2.8.2. Relatório de Faturamento: relatórios com consumo de serviços do provedor;

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

1.2.8.4. Relatórios de avaliação de otimização e performance, contendo sugestões de melhorias, ajustes em diversos aspectos da infraestrutura.

1.2.9. Os relatórios deverão ser disponibilizados pelo portal em periodicidade diária, semanal ou mensal, a depender das características do serviço ou recurso avaliado, e abrangendo aqueles listados na tabela 1 deste documento. O serviço estará sob as responsabilidades da CONTRATADA, não sendo cobrado como serviço adicional.

1.2.10. Caso o CONTRATANTE esgote o quantitativo de USNs previstas para o item 1 (serviços de computação em nuvem), reconfigurado o exaurimento do contrato.

1.2.10.1. O contratante poderá optar pelo acréscimo de 25% (vinte e cinco por cento) previstos em lei antes do exaurimento.

1.2.11. O CONTRATANTE poderá optar por formalizar aditivo contratual para incluir itens não previstos inicialmente na tabela de serviços em nuvem (tabela 1).

1.2.11.1. Para a composição de custos do novo serviço, deverá ser utilizada a mesma metodologia de composição de custos, a qual seja: a média entre os 04 (quatro) provedores utilizados na formação do Fator de USN (Anexo IV do Termo de Referência).

1.3. REQUISITOS TÉCNICOS DO SERVIÇO DE COMPUTAÇÃO EM NUVEM

1.3.1. Os serviços descritos na Tabela 1 deverão ser executados em território nacional, o que inclui armazenar os dados das informações do CONTRATANTE em *datacenters* instalados fisicamente no Brasil, incluindo replicação e cópias de segurança (*backups*), conforme disposto na Instrução Normativa nº 05/DSIC/SCS/GSIPR, 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.

1.3.2. A CONTRATADA deverá providenciar os recursos tecnológicos e humanos necessários à execução dos serviços de computação em nuvem, que incluem, no mínimo, as seguintes ações:

1.3.2.1. Elaboração de Projeto da arquitetura dos serviços de computação solicitados.

1.3.2.2. Provisionamento, configuração, atualização, otimização e documentação dos serviços de computação.

1.3.2.3. Gerenciamento proativo baseado em monitoramento 24x7 com registro e resolução de problemas durante o período contratado.

1.3.2.4. Implementação de mecanismo de detecção e resposta a incidentes no ambiente da solução.

1.3.3. A CONTRATADA deverá prover acesso irrestrito ao portal dos provedores de nuvem, incluindo acessos de conta *root*, acesso irrestrito ao console, dentre outros.

1.3.4. O acesso à conta concedido ao CONTRATANTE deverá ser totalmente separado de qualquer outro cliente da CONTRATADA.

1.3.5. A CONTRATADA deverá prover um relatório de controle de custos do ambiente contratado, por meio de um *advisor*, a cada três (três) meses, apontando os itens nos quais é possível atuar para redução de custos.

1.3.6. A CONTRATADA deverá intermediar e agregar valor a todos os serviços de computação em nuvem prestados pelo provedor de nuvem, incluindo a prestação de suporte técnico, orientação técnica especializada, além dos serviços específicos de gerenciamento total e migração.

Tabela 1 - Catálogo de serviços de computação em nuvem oferecidos por provedores de nuvem

Código	Recursos de Computação em Nuvem	Métrica	Fator Médio *
1	Máquina Virtual Linux - provisionada com 2 vCPU e 8 GB de memória RAM, reservada por 1 ano	Instância / Hora	0,08317
2	Máquina Virtual Linux Corporativo - provisionada com 2 vCPU e 8 GB de memória RAM, reservada por 1 ano	Instância / Hora	0,14317
3	Máquina Virtual Windows - provisionada com 2 vCPU e 8 GB de memória RAM, reservada por 1 ano	Instância / Hora	0,17517
4	Máquina Virtual Linux - provisionada com 4 vCPU e 16 GB de memória RAM, reservada por 1 ano	Instância / Hora	0,16668
5	Máquina Virtual Linux Corporativo - provisionada com 4 vCPU e 16 GB de memória RAM, reservada por 1 ano	Instância / Hora	0,22668
6	Máquina Virtual Windows - provisionada com 4 vCPU e 16 GB de memória RAM, reservada por 1 ano	Instância / Hora	0,35068
7	Máquina Virtual Linux - provisionada com 8 vCPU e 32 GB de memória RAM, reservada por 1 ano	Instância / Hora	0,33368
8	Máquina Virtual Linux Corporativo - provisionada com 8 vCPU e 32 GB de memória RAM, reservada por 1 ano	Instância / Hora	0,46368
9	Máquina Virtual Windows - provisionada com 8 vCPU e 32 GB de memória RAM, reservada por 1 ano	Instância / Hora	0,70168
10	Máquina Virtual Linux - provisionada com 16 vCPU e 64 GB de memória RAM, reservada por 1 ano	Instância / Hora	0,66672
11	Máquina Virtual Linux Corporativo - provisionada com 16 vCPU e 64 GB de memória RAM, reservada por 1 ano	Instância / Hora	0,79672
12	Máquina Virtual Windows - provisionada com 16 vCPU e 64 GB de memória RAM, reservada por 1 ano	Instância / Hora	1,40272
13	Máquina Virtual Linux - provisionada com 32 vCPU e 128 GB de memória RAM, reservada por 1 ano	Instância / Hora	1,33372
14	Máquina Virtual Linux Corporativo - provisionada com 32 vCPU e 128 GB de memória RAM, reservada por 1 ano	Instância / Hora	1,46372
15	Máquina Virtual Windows - provisionada com 32 vCPU e 128 GB de memória RAM, reservada por 1 ano	Instância / Hora	2,80572
16	Máquina Virtual Linux - provisionada com 2 vCPU e 8 GB de memória RAM, por demanda	Instância / Hora	0,11552
17	Máquina Virtual Linux Corporativo - provisionada com 2 vCPU e 8 GB de memória RAM, por demanda	Instância / Hora	0,16052
18	Máquina Virtual Windows - provisionada com 2 vCPU e 8 GB de memória RAM, por demanda	Instância / Hora	0,20752
19	Máquina Virtual Linux - provisionada com 4 vCPU e 16 GB de memória RAM, por demanda	Instância / Hora	0,23102
20	Máquina Virtual Linux Corporativo - provisionada com 4 vCPU e 16 GB de memória RAM, por demanda	Instância / Hora	0,27602
21	Máquina Virtual Windows - provisionada com 4 vCPU e 16 GB de memória RAM, por demanda	Instância / Hora	0,41502
22	Máquina Virtual Linux - provisionada com 8 vCPU e 32 GB de memória RAM, por demanda	Instância / Hora	0,46212
23	Máquina Virtual Linux Corporativo - provisionada com 8 vCPU e 32 GB de memória RAM, por demanda	Instância / Hora	0,55962
24	Máquina Virtual Windows - provisionada com 8 vCPU e 32 GB de memória RAM, por demanda	Instância / Hora	0,83012
25	Máquina Virtual Linux - provisionada com 16 vCPU e 64 GB de memória RAM, por demanda	Instância / Hora	0,92422
26	Máquina Virtual Linux Corporativo - provisionada com 16 vCPU e 64 GB de memória RAM, por demanda	Instância / Hora	1,02172
27	Máquina Virtual Windows - provisionada com 16 vCPU e 64 GB de memória RAM, por demanda	Instância / Hora	1,66242
28	Máquina Virtual Linux - provisionada com 32 vCPU e 128 GB de memória RAM, por demanda	Instância / Hora	1,84842

29	Máquina Virtual Linux Corporativo - provisionada com 32 vCPU e 128 GB de memória RAM, por demanda	Instância / Hora	1,9459€
30	Máquina Virtual Windows - provisionada com 32 vCPU e 128 GB de memória RAM, por demanda	Instância / Hora	3,1629€
Código	VMware SDDC	Métrica	Fator U
31	Serviço de Hospedagem de VMware SDDC, reservado por 3 anos	Instância / Mês	5.076,980€
32	Serviço de Hospedagem de VMware SDDC, reservado por 1 ano	Instância / Mês	6.908,256€
Código	Armazenamento (por demanda)	Métrica	Fator U
33	Serviço de armazenamento de blocos (SSD)	Gigabyte / Mês	0,15262€
34	Serviço de armazenamento de blocos (HDD)	Gigabyte / Mês	0,06687€
35	Serviço de armazenamento de objetos	Gigabyte / Mês	0,03340€
36	Serviço de armazenamento em rede compatível com NFS	Gigabyte / Mês	0,39650€
Código	Rede (por demanda)	Métrica	Fator U
37	Tráfego de saída da rede	Gigabyte / Mês	0,11375€
38	Tráfego de rede interna entre zonas	Gigabyte / Mês	0,01000€
39	Tráfego de rede do balanceador de carga	Gigabyte / Mês	0,00935€
40	Serviço de balanceamento de carga	Regra / Hora	0,03235€
41	Serviço de balanceamento de carga utilizando gerenciador de tráfego por DNS **	Milhão de Consultas DNS / Mês	0,69500€
42	Serviço de balanceamento de carga utilizando gerenciador de tráfego por endpoint **	Endpoint / Mês	0,50000€
43	Porta de conexão de fibra 1Gbps	Unidade / Hora	0,3468€
44	Porta de conexão de fibra 5 Gbps	Unidade / Hora	2,6356€
45	Serviço de DNS - Hospedagem de zonas	Zona / Mês	0,40000€
46	Serviço de DNS - Consultas	Milhão de Consultas / Mês	0,50000€
47	Serviço de VPN	Gigabyte / Mês	0,06425€
48	VPN Gateway	Túnel / Mês	0,05500€
49	NAT Gateway	Unidade / Hora	0,0464€
50	NAT gateway - Tráfego	Gigabyte / Mês	0,06100€
51	IP Público	Unidade / Hora	0,00635€
Código	Segurança (por demanda)	Métrica	Fator U
52	Serviço de Cofre de Senhas	Chave / Mês	0,12650€
53	Serviço Web Application Firewall por ACL ***	ACL / Mês	5,00000€
54	Serviço Web Application Firewall por Regra ***	Regra / Mês	1,00000€
55	Serviço Web Application Firewall por hora ***	Gateway / Hora	0,15300€
56	Serviço de Backup	Instância / Mês	5,00000€
57	Serviço de armazenamento de Backup	Gigabyte / Mês	0,10320€
58	Serviço de Auditoria e Análise de Logs	Gigabyte / Mês	1,79781€
Código	Serviços Gerenciados de Banco de Dados	Métrica	Fator U
59	Serviço Gerenciado de Banco de Dados MySQL com 4 vCPU e 16 GB de memória RAM, reservado por 1 ano	Instância / Hora	0,27900€
60	Serviço Gerenciado de Banco de Dados MySQL com 8 vCPU e 32 GB de memória RAM, reservado por 1 ano	Instância / Hora	0,55795€
61	Serviço Gerenciado de Banco de Dados MySQL com 16 vCPU e 64 GB de memória RAM, reservado por 1 ano	Instância / Hora	1,1158€
62	Serviço Gerenciado de Banco de Dados MySQL com 32 vCPU e 128 GB de memória RAM, reservado por 1 ano	Instância / Hora	2,2326€
63	Serviço Gerenciado de Banco de Dados PostgreSQL com 4 vCPU e 16 GB de memória RAM, reservado por 1 ano	Instância / Hora	0,28505€
64	Serviço Gerenciado de Banco de Dados PostgreSQL com 8 vCPU e 32 GB de memória RAM, reservado por 1 ano	Instância / Hora	0,57000€
65	Serviço Gerenciado de Banco de Dados PostgreSQL com 16 vCPU e 64 GB de memória RAM, reservado por 1 ano	Instância / Hora	1,14000€
66	Serviço Gerenciado de Banco de Dados PostgreSQL com 32 vCPU e 128 GB de memória RAM, reservado por 1 ano	Instância / Hora	2,2824€
67	Serviço Gerenciado de Banco de Dados SQLServer com 4 vCPU e 16 GB de memória RAM, reservado por 1 ano	Instância / Hora	1,0672€
68	Serviço Gerenciado de Banco de Dados SQLServer com 8 vCPU e 32 GB de memória RAM, reservado por 1 ano	Instância / Hora	2,13120€
69	Serviço Gerenciado de Banco de Dados SQLServer com 16 vCPU e 64 GB de memória RAM, reservado por 1 ano	Instância / Hora	4,2590€
70	Serviço Gerenciado de Banco de Dados SQLServer com 32 vCPU e 128 GB de memória RAM, reservado por 1 ano	Instância / Hora	8,2446€
71	Serviço Gerenciado de Banco de Dados ORACLE com 4 vCPU e 16 GB de memória RAM, reservado por 1 ano	Instância / Hora	0,61490€
72	Serviço Gerenciado de Banco de Dados ORACLE com 8 vCPU e 32 GB de memória RAM, reservado por 1 ano	Instância / Hora	1,22980€
73	Serviço Gerenciado de Banco de Dados ORACLE com 16 vCPU e 64 GB de memória RAM, reservado por 1 ano	Instância / Hora	2,45950€
74	Serviço Gerenciado de Banco de Dados MySQL com 4 vCPU e 16 GB de memória RAM	Instância / Hora	0,38180€
75	Serviço Gerenciado de Banco de Dados MySQL com 8 vCPU e 32 GB de memória RAM	Instância / Hora	0,55552€
76	Serviço Gerenciado de Banco de Dados MySQL com 16 vCPU e 64 GB de memória RAM	Instância / Hora	1,52720€
77	Serviço Gerenciado de Banco de Dados MySQL com 32 vCPU e 128 de GB memória RAM	Instância / Hora	3,05440€
78	Serviço Gerenciado de Banco de Dados PostgreSQL com 4 vCPU e 16 GB de memória RAM	Instância / Hora	0,44800€
79	Serviço Gerenciado de Banco de Dados PostgreSQL com 8 vCPU e 32 GB de memória RAM	Instância / Hora	0,6185€
80	Serviço Gerenciado de Banco de Dados PostgreSQL com 16 vCPU e 64 GB de memória RAM	Instância / Hora	1,79200€
81	Serviço Gerenciado de Banco de Dados PostgreSQL com 32 vCPU e 128 GB de memória RAM	Instância / Hora	3,58400€
82	Serviço Gerenciado de Banco de Dados SQLServer com 4 vCPU e 16 GB de memória RAM	Instância / Hora	1,3018€
83	Serviço Gerenciado de Banco de Dados SQLServer com 8 vCPU e 32 GB de memória RAM	Instância / Hora	2,60340€
84	Serviço Gerenciado de Banco de Dados SQLServer com 16 vCPU e 64 GB de memória RAM	Instância / Hora	5,2034€
85	Serviço Gerenciado de Banco de Dados SQLServer com 32 vCPU e 128 GB de memória RAM	Instância / Hora	10,4082€

86	Serviço Gerenciado de Banco de Dados ORACLE com 4 vCPU e 16 GB de memória RAM	Instância / Hora	0,70300
87	Serviço Gerenciado de Banco de Dados ORACLE com 8 vCPU e 32 GB de memória RAM	Instância / Hora	1,40600
88	Serviço Gerenciado de Banco de Dados ORACLE com 16 vCPU e 64 GB de memória RAM	Instância / Hora	2,81200
Código	Armazenamento de Banco de Dados	Métrica	Fator U
89	Armazenamento de Banco de Dados MySQL	Gigabyte / Mês	0,18325
90	Armazenamento de Banco de Dados PostgreSQL	Gigabyte / Mês	0,23100
91	Armazenamento de Banco de Dados SQLServer	Gigabyte / Mês	0,23100
92	Armazenamento de Banco de Dados Oracle	Gigabyte / Mês	0,12225
Código	Serviço de Cache Gerenciado	Métrica	Fator U
93	Serviço de Cache Gerenciado de memória RAM, com no mínimo 6 GB	Unidade / Hora	0,33235
94	Serviço de Cache Gerenciado de memória RAM, com no mínimo 26 GB	Unidade / Hora	1,01100
95	Serviço de Cache Gerenciado de memória RAM, com no mínimo 52 GB	Unidade / Hora	1,90035
Código	Serviços de Container (por demanda)	Métrica	Fator U
96	Serviço Gerenciado de Kubernetes	Instância / Hora	0,20000
Código	Serviço de Computação Sem Servidor - Serverless (por demanda)	Métrica	Fator U
97	Serverless - Requisições das funções	Milhão de requisições / Mês	0,25000
98	Serverless - Tempo de Execução das funções	Gigabyte / Segundo	0,00001
Código	Serviço de Distribuição de Conteúdo (CDN)	Métrica	Fator U
99	Tráfego de rede do CDN	Gigabyte / Mês	0,14435

(*) Valores Médios levantados pelo TJES (0238467).

(**) O Serviço de balanceamento de carga deverá ser prestado na métrica definida no código 41 ou no código 42 a ser indicada pela CONTRATADA proposta de preços para cada provedor ofertado.

(***) Os serviços de Web Application Firewall deverão ser prestados na métrica definida nos códigos 53, 54 ou 55 a ser indicada pela CONTRATADA proposta de preços para cada provedor ofertado.

1.3.7. Descrição dos Serviços de Computação em Nuvem - tabela 1

1.3.7.1. A CONTRATADA deverá disponibilizar os recursos computacionais descritos na tabela 1 por intermédio dos provedores de serviços de computação em nuvem ofertados.

1.3.7.2. A CONTRATADA deverá apresentar uma composição de serviços da tabela 1 que atendam a todas as condições seguintes:

1.3.7.2.1. Ao menos um provedor deverá atender integralmente (100% - cem por cento) todos os serviços da tabela 1.

1.3.7.2.2. O segundo provedor deverá atender ao menos 50% (cinquenta por cento) dos serviços da tabela 1.

1.3.7.2.3. Não será aceita a combinação de provedores distintos para alcance dos limites mínimos citados nos itens 1.3.7.2.1 e 1.3.7.2.2.

1.3.8. (código 01 ao 30) - Máquinas Virtuais

1.3.8.1. As máquinas virtuais consistem na disponibilização de recursos de processamento de dados a serem provisionados com diferentes capacidades em termos de vCPU e Memória RAM;

1.3.8.2. As máquinas virtuais poderão ser provisionadas nas modalidades "reservada por 1 (um) ano" ou por "demanda" (modalidade de pagamento *upfront*); na modalidade por demanda, os serviços são alocados sem um período pré-determinado de faturamento periódico, de acordo com a Ordem de Serviço;

1.3.8.3. As máquinas virtuais, cujo propósito é de uso geral, deverão ser demandadas respeitando a seguinte relação vCPU/memória RAM: 2x8; 4x16; 8x32; 16x64 e 32x128.

1.3.8.4. Não será admitido o uso de máquinas *burstable*, ou seja, máquinas virtuais que fornecem o seu desempenho máximo por apenas um curto período de tempo.

1.3.8.5. Os processadores utilizados nas vCPU devem ser, no mínimo: Intel Xeon família E5 2673 v3, Xeon Scalable Proc Xeon Platinum 8167, GOLD, Silver Scalable e AMD EPYC 7000;

1.3.8.6. A razão vCPU:pCPU máxima admitida deve ser de 3:1;

1.3.8.7. As máquinas virtuais serão ofertadas com, no mínimo, os seguintes sistemas operacionais instalados:

1.3.8.7.1. Máquinas Virtuais Linux: CentOS 7 ou superior; Ubuntu Server 16.04.2 ou superior; Debian 11 ou superior;

1.3.8.7.2. Máquinas Virtuais Linux Corporativo: Linux com suporte do fabricante, como por exemplo Red Hat Enterprise Linux 6 ou superior, SuseEnterprise Server 15 ou superior, Oracle Linux 6/7 ou superior;

1.3.8.7.3. Máquinas Virtuais Windows: Windows Server 2012 ou superior.

1.3.8.8. Os sistemas operacionais devem estar devidamente licenciados e aptos para uso, salvo nos casos de aplicação de condições de uso de licenciamento próprio BYOL descritas no item 1.3.21 deste documento.

1.3.8.9. As máquinas virtuais devem ser fornecidas com disco destinado ao *boot* e hospedagem do sistema operacional. A capacidade mínima do disco deve ser de 10GB para Linux e 100GB para Windows.

1.3.8.10. Todas as máquinas virtuais devem ser confiáveis, ou seja, a CONTRATADA deverá demonstrar que tais máquinas virtuais estão em conformidade com as políticas e práticas de segurança e de qualidade de redes exigidas pelo provedor.

1.3.8.11. As máquinas virtuais disponibilizadas devem prover mecanismos de *backup* recorrentes, incluindo *snapshot* (sazonais), a fim de mitigar os riscos de perda de dados.

1.3.9. (código 31 e 32) - Serviço de Hospedagem de VMware SDDC

1.3.9.1. Serviço de Data Center Definido como Software (SDDC) para gerência de plataforma da VMware na nuvem sob a forma de cluster de hardwares físicos dedicados.

1.3.9.2. O serviço de hospedagem de VMware SDDC poderá ser provisionado na modalidade reservada por 1 (um) ano ou por 3 (três) anos. Em ambos os casos, os recursos são previamente reservados pelo período especificado na Ordem de Serviço e o faturamento é mensal (sem pagamento *upfront*).

1.3.9.3. O cluster VMware será composto de pelo menos 2 hosts, cada um com a seguinte especificação de hardware: 36 núcleos físicos (Intel Xeon Platinum 8000 series Skylake-SP ou Cascade Lake, Intel Xeon Gold 6000 Series, Intel Xeon Platinum 8000 Series v4 Broadwell), memória RAM de 512 GB, armazenamento NVMe disponível de 10 TB e Cache NVMe de 32 GB, largura de banda de rede de 25 Gbps.

1.3.9.4. A solução deverá fornecer vSphere, vCenter, vSAN, NSX-T e HCX;

1.3.9.5. Deverá incluir licenças para ESXi, vCenter, vSAN, NSX-T e HCX;

- 1.3.9.6. Deverá ser compatível com migração por meio de HCX e vMotion por meio de link dedicado ou serviço de VPI comunicação entre os clusters;
- 1.3.9.7. O provedor de nuvem ou a VMware, conforme parceria firmada com o provedor, será responsável pela administração da pilha VMware, devendo garantir seu correto funcionamento e atendimento ao SLA, bem como aplicar periodicamente patches lançados pela VMware para correções de bugs e de problemas de segurança, e atualizações de versões componentes da pilha de VMware.
- 1.3.10. (código 33 ao 36) - Armazenamento (por demanda)
- 1.3.10.1. Serviços de armazenamento em blocos ou objetos para serem acessados pelas Máquinas Virtuais e/ou aplicações, que serão provisionados na modalidade por demanda.
- 1.3.10.2. (código 33) - Serviço de armazenamento de blocos SSD.
- 1.3.10.2.1. Serviços para utilização de volume de armazenamento *block-level*;
- 1.3.10.2.2. Deverá ser baseado em discos de estado sólido (SSD) ou tecnologia superior em termos de performance;
- 1.3.10.2.3. Deverá possibilitar que o volume criado seja anexado às máquinas virtuais e reconhecido pelo SO cor dispositivo físico e local;
- 1.3.10.2.4. Deverá permitir a definição de nomes ou identificadores de volume de armazenamento;
- 1.3.10.2.5. Deverá possuir função de criptografia do volume com mudança de chave gerenciada pela CONTRATADA pelo CONTRATANTE;
- 1.3.10.2.6. O desempenho informado pela CONTRATADA para o volume provisionado deve se manter ao longo do contrato, podendo ser comprovado por meio de *benchmark* definido a critério do CONTRATANTE.
- 1.3.10.3. (código 34) - Serviço de armazenamento de blocos HDD
- 1.3.10.3.1. Serviços para utilização de volume de armazenamento *block-level*;
- 1.3.10.3.2. Deverá ser baseado em discos magnéticos (HDD) ou superior;
- 1.3.10.3.3. Deverá possibilitar que o volume criado seja anexado às máquinas virtuais e reconhecido pelo SO cor dispositivo físico e local;
- 1.3.10.3.4. Deverá permitir a definição de nomes ou identificadores de volume de armazenamento;
- 1.3.10.3.5. Deverá possuir função de criptografia do volume com mudança de chave gerenciada pela CONTRATADA pelo CONTRATANTE;
- 1.3.10.3.6. O desempenho informado pela CONTRATADA para o volume provisionado deve se manter ao longo do contrato, podendo ser comprovado por meio de *benchmark* definido a critério do CONTRATANTE.
- 1.3.10.4. (código 35) - Serviço de armazenamento de objetos
- 1.3.10.4.1. Serviço para utilização de volume de armazenamento de objetos;
- 1.3.10.4.2. Deverá ser durável, escalável e seguro;
- 1.3.10.4.3. Deverá possuir recurso de versionamento ou de *snapshot*;
- 1.3.10.4.4. Deverá possuir interface web para inclusão, exclusão e consultas de informações;
- 1.3.10.4.5. Deverá possuir função de criptografia do volume com mudança de chave gerenciada pela CONTRATADA pelo CONTRATANTE;
- 1.3.10.4.6. Deverá possuir API para upload de arquivos via aplicações desenvolvidas por terceiros.
- 1.3.10.5. (código 36) - Serviço de armazenamento em rede compatível com NFS
- 1.3.10.5.1. Serviço de compartilhamento de arquivos compatível com protocolo NFS (Network File System) na sua versão 3 ou superior;
- 1.3.10.5.2. Deverá ter suporte a pontos de montagem em mais de uma máquina simultaneamente;
- 1.3.10.5.3. Deverá ter suporte a alta disponibilidade (*High Availability - HA*), com cópia dos dados em mais de uma zona;
- 1.3.10.5.4. Deverá ter suporte a criptografia em repouso.
- 1.3.11. (código 37 ao 51) - Rede (por demanda)
- 1.3.11.1. (código 37) - Tráfego de saída da rede
- 1.3.11.1.1. Serviço de transmissão de dados de saída da rede, cuja origem é o datacenter do provedor de nuvem e o destino é a Internet ou a rede local do CONTRATANTE, no caso de utilização de porta de conexão de fibra (código 43). Será considerada como saída de rede o tráfego entre regiões.
- 1.3.11.1.2. O tráfego de dados entre máquinas virtuais e entre as áreas de armazenamento de dados do provedor de nuvem não devem ser contabilizados como tráfego de saída de rede;
- 1.3.11.1.3. O tráfego de entrada de dados deverá ser ilimitado e sem custos para o CONTRATANTE.
- 1.3.11.2. (código 38) - Tráfego de rede interna entre zonas
- 1.3.11.2.1. Serviço de transmissão de dados entre zonas do provedor quando as estruturas utilizadas estiverem separadas geograficamente.
- 1.3.11.3. (código 39) - Tráfego de rede do balanceador de carga
- 1.3.11.3.1. Serviço de transmissão de dados do balanceador de carga.
- 1.3.11.4. (código 40) - Serviço de balanceamento de carga
- 1.3.11.4.1. Serviço para utilização de balanceador de carga, que distribuirá o tráfego de entrada para as máquinas virtuais;
- 1.3.11.4.2. Deverá ser escalável, de maneira a crescer ou diminuir seu poder de processamento, em função do fluxo de dados que por ele trafega;
- 1.3.11.4.3. A CONTRATADA deverá definir as regras de escalabilidade de acordo com as necessidades do CONTRATANTE.
- 1.3.11.5. (código 41) - Serviço de balanceamento de carga utilizando gerenciador de tráfego por consultas DNS
- 1.3.11.5.1. Serviço para controlar a distribuição do tráfego do usuário para pontos de extremidade da aplicação;
- 1.3.11.5.2. Deverá fornecer *failover* automático quando um ponto de extremidade ficar inativo;
- 1.3.11.5.3. Deverá permitir a melhoria da capacidade de resposta do aplicativo direcionando o tráfego para o ponto de extremidade com a menor latência de rede para o cliente, em nível de região;

- 1.3.11.5.4. Deverá permitir operações de manutenção planejada nas aplicações sem tempo de inatividade;
- 1.3.11.5.5. Deverá suportar o tráfego para pontos de extremidade externos de outras nuvens, habilitando seu us implantações locais, inclusive de nuvem híbrida.
- 1.3.11.6. (código 42) - Serviço de balanceamento de carga utilizando gerenciador de tráfego por endpoint
 - 1.3.11.6.1. Serviço para controlar a distribuição do tráfego do usuário para pontos de extremidade da aplicação cor as mesmas características do serviço previsto no código 41 e sendo contabilizado por *endpoint*.
- 1.3.11.7. (código 43) - Porta de conexão de fibra 1Gbps
 - 1.3.11.7.1. Serviço de conexão de fibra dedicada entre a infraestrutura de rede local do CONTRATANTE e uma po interface do provedor ou entre provedores visando à interconexão segura e rápida entre os dois, sem tráfeg internet;
 - 1.3.11.7.2. A porta do provedor deverá estar localizada em território nacional, quando se tratar de conexão dir ambiente do CONTRATANTE.
- 1.3.11.8. (código 44) - Porta de conexão de fibra 5 Gbps
 - 1.3.11.8.1. Serviço de conexão de fibra dedicada entre a infraestrutura de rede local do CONTRATANTE e uma po interface do provedor ou entre provedores visando à interconexão segura e rápida entre os dois, sem tráfeg internet;
 - 1.3.11.8.2. A porta do provedor deverá estar localizada em território nacional, quando se tratar de conexão dir ambiente do CONTRATANTE.
- 1.3.11.9. (código 45) - Serviço de DNS – Hospedagem de zonas
 - 1.3.11.9.1. O serviço consiste em um espaço de gerenciamento no qual é possível criar, alterar e excluir entradas ni Cada zona DNS representa um limite de autoridade sujeito à gestão por determinadas entidades.
- 1.3.11.10. (código 46) - Serviço de DNS – Consultas
 - 1.3.11.10.1. O serviço consiste em realizar consultas DNS que representa a ação de um host buscar um registro esp que está exposto na zona DNS. Para realizar essa consulta o host percorre toda a árvore hierárquica até achar o r específico.
 - 1.3.11.10.2. Deverá ser possível realizar buscas nos registros disponíveis, quais sejam do tipo A, AAAA, CNAME, M; NS, SOA, SRV e TXT, sendo cada um específico para cada finalidade.
- 1.3.11.11. (código 47) - Serviço de VPN
 - 1.3.11.11.1. Serviço para uso de Rede Privada Virtual (Virtual Private Network – VPN);
 - 1.3.11.11.2. Deve permitir a criação de conexões site-to-site e client-to-site entre as mesmas redes locais e na nu fornecer *scripts* e/ou software para a criação dessas conexões.
 - 1.3.11.11.3. Somente o tráfego de saída será contabilizado para cobrança do serviço.
 - 1.3.11.11.4. O tráfego de saída para o serviço de VPN não se confunde nem poderá ser cobrado em duplicidade tráfego de saída de rede descrito no código 37.
 - 1.3.11.11.5. O tráfego de dados através da conexão deve ser por túnel VPN utilizando o protocolo IPSec para cor site-to-site e client-to-site. Alternativamente, as conexões client-to-site poderão ser realizadas por túnel VPN utiliz protocolo SSL.
- 1.3.11.12. (código 48) - VPN Gateway
 - 1.3.11.12.1. A CONTRATADA deverá prover um gateway de VPN para a rede do CONTRATANTE;
 - 1.3.11.12.2. Possibilitar o envio do tráfego criptografado em uma conexão pública;
 - 1.3.11.12.3. Permitir a criação de VPN conforme descrito no Serviço de VPN;
 - 1.3.11.12.4. Estão inclusos nesse serviço os custos do gateway por hora de conexão da VPN.
- 1.3.11.13. (código 49) NAT Gateway
 - 1.3.11.13.1. Serviço que fornece um gateway de Network Address Translation (NAT - Conversão de endereços de rec
 - 1.3.11.13.2. Deve permitir que máquinas virtuais ou outros serviços dentro de uma rede privada possam se cone serviços externos a esta rede e, ainda e simultaneamente, não permitir que serviços externos iniciem conexão com máquinas virtuais;
 - 1.3.11.13.3. A cobrança será por hora que o serviço estiver ativo.
- 1.3.11.14. (código 50) NAT Gateway – Tráfego
 - 1.3.11.14.1. Tráfego de dados que passam pelo NAT Gateway (código 49);
 - 1.3.11.14.2. O tráfego de dados de saída que passe pelo NAT Gateway não se confunde nem poderá ser cobra duplicidade com o tráfego de saída de rede (código 37);
 - 1.3.11.14.3. A cobrança será feita pelo consumo em gigabytes por mês.
- 1.3.11.15. (código 51) - IP Público
 - 1.3.11.15.1. Serviço de atribuição de endereço IP público (estático ou dinâmico), dedicado, até que seja liberad CONTRATADA a pedido do CONTRATANTE ou até que o recurso seja desligado, no caso de ser dinâmico.
- 1.3.12. (código 52 ao 58) Segurança (por demanda)
 - 1.3.12.1. (código 52) - Serviço de Cofre de Senhas
 - 1.3.12.1.1. Serviço para controle de chaves criptográficas e outros segredos usados por aplicativos e serviços;
 - 1.3.12.1.2. Deverá criptografar chaves e segredos, como chaves de autenticação, chaves de conta de armazenar chaves de criptografia de dados, arquivos .PFX e senhas;
 - 1.3.12.1.3. Deverá permitir a criação ou importação de uma chave ou segredo;
 - 1.3.12.1.4. Deverá permitir usuários ou aplicativos a acessar o cofre da chave para que eles possam gerenciar o suas chaves e segredos;
 - 1.3.12.1.5. Deverá fornecer o log de uso do Cofre da Chave.
 - 1.3.12.1.6. Cada chave deverá permitir no mínimo 10.000 operações.
 - 1.3.12.2. (código 53) - Serviço Web Application Firewall adquirido por ACL
 - 1.3.12.2.1. Serviço para fornecer proteção centralizada dos aplicativos Web contra vulnerabilidades e eventuais atac

- 1.3.12.2.2. O serviço será remunerado por Regra de ACL (Access Control List);
 - 1.3.12.2.3. Deverá fornecer proteção sem modificar o código de *back-end*;
 - 1.3.12.2.4. Deverá proteger vários aplicativos Web ao mesmo tempo por trás de um gateway de aplicativo;
 - 1.3.12.2.5. Deverá fornecer monitoramento das aplicações Web contra ataques usando um log em tempo real;
 - 1.3.12.2.6. Deverá permitir personalização de regras e grupos de regras, a fim de atender as necessidades das aplicações e eliminar falsos positivos.
- 1.3.12.3. (código 54) - Serviço Web Application Firewall adquirido por Regra
- 1.3.12.3.1. Serviço para fornecer proteção centralizada dos aplicativos Web contendo as mesmas características do serviço previsto no código 53 e sendo contabilizado por regra ativada.
- 1.3.12.4. (código 55) - Serviço Web Application Firewall adquirido por hora
- 1.3.12.4.1. Serviço para fornecer proteção centralizada dos aplicativos Web contendo as mesmas características do serviço previsto no código 54 e sendo contabilizado por hora;
 - 1.3.12.4.2. O serviço será remunerado por hora de utilização do gateway.
- 1.3.12.5. (código 56) - Serviço de Backup
- 1.3.12.5.1. Serviço para fornecer backup (ou proteção) e restauração de dados na nuvem;
 - 1.3.12.5.2. Deverá alocar e gerenciar automaticamente o armazenamento de backup;
 - 1.3.12.5.3. Deverá permitir a transmissão segura e o armazenamento dos dados criptografados;
 - 1.3.12.5.4. Deverá fornecer backups consistentes, garantindo que correções adicionais não sejam necessárias para restaurar os dados;
 - 1.3.12.5.5. Deverá permitir a retenção dos backups durante a vigência do contrato;
 - 1.3.12.5.6. Deverá permitir transferência de dados ilimitada, tanto para backup quanto para *restore*, dentro da rede do próprio datacenter do provedor;
 - 1.3.12.5.7. Deverá fornecer sistema de alertas para falhas no processo de backup, ou consistência dos arquivos.
- 1.3.12.6. (código 57) - Serviço de armazenamento de Backup
- 1.3.12.6.1. Serviço de armazenamento em nuvem de cópias de segurança;
 - 1.3.12.6.2. O serviço de armazenamento de backup em nuvem deve prover escala ilimitada e proporcionar disponibilidade, sem necessidade de manutenção ou sobrecarga de monitoramento;
 - 1.3.12.6.3. Os dados devem ser persistidos com redundância em equipamentos de hardware diferentes, de forma a prevenir perda de dados com falhas de hardware;
 - 1.3.12.6.4. Deverá permitir a retenção de dados limitado ao prazo de vigência do contrato.
 - 1.3.12.6.5. Deverá permitir a criptografia dos dados.
- 1.3.12.7. (código 58) - Serviço de Auditoria e Análise de Logs.
- 1.3.12.7.1. Serviço de coleta e análise de dados de monitoramento;
 - 1.3.12.7.2. Deverá permitir a construção de consultas para analisar os dados coletados;
 - 1.3.12.7.3. Deverá permitir o armazenamento dos logs por períodos superiores a 1 (um) ano.
- 1.3.13. (código 59 ao 88) - Serviços Gerenciados de Banco de Dados
- 1.3.13.1. Os serviços de banco de dados devem fornecer plataformas de bancos de dados escaláveis, com dimensionamento dinâmico e automação da administração, provisionamento, configuração, atualização e backup.
 - 1.3.13.2. Os serviços de banco de dados consistem na disponibilização da console da nuvem pública capaz de:
 - 1.3.13.2.1. Permitir a criação de instâncias de banco de dados;
 - 1.3.13.2.2. Atribuir o tipo de recurso computacional que suportará o banco de dados;
 - 1.3.13.2.3. Implementar recursos de segurança relacionados ao controle de acesso;
 - 1.3.13.2.4. Atribuir o tipo de banco de dados (MySQL, PostgreSQL, Microsoft SQL Server e Oracle);
 - 1.3.13.2.5. Implementar recursos de detecção de falhas e recuperação dos recursos computacionais e aplicações;
 - 1.3.13.2.6. Permitir o monitoramento do banco de dados.
 - 1.3.13.3. Os sistemas de gerenciamento de banco de dados devem estar devidamente licenciados (edição Standard ou superior) e aptos para uso;
 - 1.3.13.4. Os serviços gerenciados de banco de dados devem ser providos diretamente e integralmente pelos provedores de nuvem;
 - 1.3.13.5. Os serviços gerenciados de banco de dados são independentes dos serviços de gerenciamento e operação de recursos de nuvem (item 2 da contratação).
 - 1.3.13.6. Os serviços de banco de dados poderão ser provisionados nas modalidades reservada por 1 (um) ano ou sob demanda. Na modalidade reservada (código 59 ao 73), os recursos são previamente reservados pelo período de 1 ano com faturamento mensal; na modalidade sob demanda (código 74 ao 88), os serviços são alocados sem um prazo predeterminado e com faturamento periódico, de acordo com a Ordem de Serviço.
- 1.3.14. (código 89 ao 92) - Serviço de Armazenamento de Banco de Dados
- 1.3.14.1. Serviço para armazenamento dos Bancos de Dados MySQL, PostgreSQL, Microsoft SQL Server e Oracle.
- 1.3.15. (código 93 ao 95) - Serviço de Cache gerenciado (por demanda)
- 1.3.15.1. O Serviço de cache gerenciado deverá implementar uma solução baseada em estrutura de dados em memória, por exemplo de tecnologias Redis, MemCache ou equivalente.
 - 1.3.15.2. O serviço deverá conter no mínimo um nó principal e outro secundário ou réplica.
 - 1.3.15.3. Deverá ser possível implementar por meio do serviço de cache gerenciado:
 - 1.3.15.3.1. Criação de memória cache em banco de dados para aumento de desempenho, redução de latência de acesso e aumento de *throughput*;
 - 1.3.15.3.1.1. O serviço de cache gerenciado deverá ser ofertado nas seguintes configurações de memória mínima: 6, 26 e 52 GB.

- 1.3.15.3.2. Gerenciamento de sessões; e
- 1.3.15.3.3. Implementar mecanismos de limitação de consumo de recursos de memória.
- 1.3.16. (código 96) - Serviços de Container (por demanda) - Plataforma como Serviço de Kubernetes
 - 1.3.16.1. Serviço para orquestração e gerenciamento de aplicações em containers através de múltiplos clusters.
 - 1.3.16.2. O serviço é mensurado por instância de cluster por hora. As instâncias relacionadas aos nós, bem como armazenamento e recursos de redes consumidos pelos clusters são contabilizados nos respectivos itens de IaaS, não há contabilização na métrica associada ao serviço de Container (código 96).
 - 1.3.16.3. Deverá permitir no mínimo 50 (cinquenta) nós por cluster.
 - 1.3.16.4. Deverá permitir o gerenciamento do Kubernetes via console.
 - 1.3.16.5. Deverá permitir o monitoramento dos recursos.
- 1.3.17. (Código 97 e 98) - Serviços de Computação sem Servidor – Serverless (por demanda)
 - 1.3.17.1. Os serviços de computação sem servidor (Serverless) consistem no fornecimento de uma plataforma de função serviço capaz de construir código que utilize e integre os diversos serviços de infraestrutura do provedor sem a necessidade de configuração, provisionamento e gerenciamento de infraestrutura.
 - 1.3.17.2. Os serviços são contabilizados por número de chamadas (requisições) das funções e pela duração da execução das funções, ressalvadas as condições de gratuidade de cada provedor em que não haverá ônus ao CONTRATANTE.
 - 1.3.17.3. Cada função deverá permitir no mínimo a alocação de 128 MB.
- 1.3.18. (código 97) - Requisições das funções
 - 1.3.18.1. A unidade para cálculo da quantidade de solicitações será contabilizada em milhões de requisições.
- 1.3.19. (código 98) - Tempo de Execução das funções
 - 1.3.19.1. A duração do tempo de execução deve ser calculada a partir do momento do início de execução até o encerramento ou retorno do resultado.
 - 1.3.19.2. Não deve ser considerado o tempo ocioso do código para fins de contabilização do tempo de execução.
- 1.3.20. (código 99) Serviços de Distribuição de Conteúdo (por demanda) - Tráfego de rede do CDN
 - 1.3.20.1. Serviço de transmissão de dados de Rede de Distribuição de Conteúdo (Content Delivery Network – CDN).
- 1.3.21. Do uso de licenciamento próprio (Bring Your Own License -BYOL)
 - 1.3.21.1. O uso de licenciamento próprio é uma prática que permite implantar ou utilizar no ambiente de nuvem determinado software já licenciado originalmente no ambiente do CONTRATANTE.
 - 1.3.21.2. Somente será aplicado a política de BYOL sobre aqueles produtos cujo licenciamento do fabricante permita previsão na política de licenciamento do provedor de nuvem.
 - 1.3.21.3. Os produtos abrangidos pela política de BYOL do provedor e declarados como isento de pagamento deverão ser prestados sem ônus pela CONTRATADA.
 - 1.3.21.4. Os produtos abrangidos pela política de BYOL do provedor e que possuam descontos em seu preço final deverão ser prestados com o mesmo desconto pela CONTRATADA. Para efetivação do repasse do desconto, a CONTRATADA deverá aplicar a mesma redução percentual concedida pelo provedor em sua política de BYOL no fator de USN associado ao objeto a política de BYOL.
 - 1.3.21.5. O CONTRATANTE será o responsável pela aquisição das licenças dos fabricantes de software, enquanto a CONTRATADA, conforme demanda, será a responsável pela instalação e configuração das licenças na máquina virtual.

1.4. REQUISITOS TÉCNICOS DOS SERVIÇOS FORNECIDOS PELO BROKER

1.4.1. DOS SERVIÇOS DE GERENCIAMENTO E OPERAÇÃO DE NUVEM

- 1.4.1.1. Os serviços de gerenciamento de recursos em nuvem consistem no planejamento, projeto, construção, execução, operação, monitoramento e otimização dos recursos computacionais mantidos em nuvem.
- 1.4.1.2. A execução dos serviços de gerenciamento de recursos em nuvem possui escopo definido na Ordem de Serviço que deverá abranger uma ou mais instâncias de computação e de banco de dados.
- 1.4.1.3. O serviço de gerenciamento e operação de nuvem relacionados às instâncias de computação e instâncias de banco de dados que integram o escopo da ordem de serviço, doravante denominado de Solução Gerenciada, será aferido mensal por Instância de Computação e por Instância de Banco de Dados.
- 1.4.1.4. O escopo das atividades de gerenciamento deve abranger todos os recursos de rede, de segurança e armazenamento utilizados pelas instâncias identificadas na ordem de serviço.
- 1.4.1.5. A CONTRATADA deverá providenciar os recursos tecnológicos e humanos necessários à execução dos serviços de gerenciamento dos recursos em nuvem, que incluem no mínimo as seguintes ações:
 - 1.4.1.5.1. Elaboração de Projeto e Design da arquitetura da solução gerenciada.
 - 1.4.1.5.2. Provisionamento de recursos e serviços de computação em nuvem constantes da tabela 1, incluindo dimensionamento, alocação, automação, parametrização no provedor, atribuição de tags, catalogação e elaboração de scripts necessários para a disponibilização em produção.
 - 1.4.1.5.3. Atualização dos recursos e serviços de computação em nuvem conforme necessidades de negócio do CONTRATANTE.
 - 1.4.1.5.4. Otimização dos recursos e serviços de computação em nuvem no tocante ao desempenho operacional e consumo financeiro.
 - 1.4.1.5.5. Documentação da solução gerenciada incluindo a disponibilização ao CONTRATANTE dos registros, o mapeamento e outros insumos necessários à identificação dos recursos em relação à necessidade de negócio com o provedor de serviço.
 - 1.4.1.5.6. Realizar a configuração e o gerenciamento das aplicações, soluções e softwares em relação aos recursos computacionais alocados na solução gerenciada.
 - 1.4.1.5.7. Apoio na implantação (*deployment*) de aplicações, softwares e soluções de acordo com as melhores práticas disponibilizadas pelo provedor de nuvem adotado.
 - 1.4.1.5.8. Gerenciamento de mudanças nas cargas de trabalhos (*workloads*) relacionadas à solução gerenciada por meio do uso de metodologias ágeis e de recursos de automação capazes de implementar um processo de contínuo desenvolvimento de mudanças compatíveis aos cenários de frequentes modificações e otimizações.

- 1.4.1.5.9. Garantia da segurança lógica dos recursos da solução gerenciada.
- 1.4.1.5.10. Criação e implantação de ambiente de integração contínua.
- 1.4.1.5.11. Automatizar o processo de gerenciamento dos recursos em nuvem por meio de ferramentas (Infraestrutura como Código).
- 1.4.1.5.12. Gerenciamento proativo baseado em monitoramento 24x7 com registro e resolução de problemas durante período contratado.
- 1.4.1.5.13. Implementar mecanismo de detecção e resposta de incidentes no ambiente da solução gerenciada.
- 1.4.1.6. A CONTRATADA deverá executar ações preventivas e proativas com vistas à otimização e garantia da disponibilidade e eficiência da solução gerenciada.
- 1.4.1.7. O registro diário das ações executadas com vistas a manutenção da saúde da solução gerenciada deverá ser disponível mensalmente e adicionalmente quando solicitado pelo CONTRATANTE.
- 1.4.1.8. A CONTRATADA deverá executar ações sob demanda por meio de abertura de chamados com vistas a atender exigências de adequação dos recursos às necessidades do CONTRATANTE.
- 1.4.1.9. Os profissionais da CONTRATADA que atuarão nos serviços de gerenciamento e operação em nuvem deverão utilizar solução de gerenciamento de chamados do CONTRATANTE.
- 1.4.1.10. A solução de gerenciamento de chamados do CONTRATANTE será utilizada para o acionamento, registro de informações, tratamento de incidentes, acompanhamento e verificação de cumprimento dos SLAs para os serviços de gerenciamento e operação em nuvem.
- 1.4.1.11. A CONTRATADA deverá utilizar os recursos tecnológicos necessários para execução dos serviços de gerenciamento sem ônus adicional ao CONTRATANTE.
- 1.4.1.12. Os recursos do provedor utilizados exclusivamente para a prestação dos serviços de gerenciamento deverão ser fornecidos pela CONTRATADA, sem ônus adicional ao CONTRATANTE.
- 1.4.1.13. Os recursos tecnológicos utilizados pela CONTRATADA exclusivamente para gerenciamento não estão limitados pelos recursos constantes da tabela 1.
- 1.4.1.14. A execução dos serviços de Gerenciamento e Operação deverá observar os seguintes prazos máximos:

Tabela 2 – Prazos máximos para execução de serviços de gerenciamento e operação

Ação	Prazo Máximo
Criação de instâncias de computação	30 (trinta) minutos
Criação de instâncias de banco de dados	1 (uma) hora
Configuração ou alteração de atributos em instâncias de computação	15 (quinze) minutos
Configuração ou alteração de atributos em instâncias de banco de dados	30 (trinta) minutos
Criação ou configuração de recurso de rede relacionado à solução gerenciada	30 (trinta) minutos
Criação ou configuração de recurso de armazenamento	1 (uma) hora
Criação ou configuração de recurso de segurança	1 (uma) hora
Criação ou configuração de serviços de <i>analytics</i> relacionados à solução gerenciada	2 (duas) horas
Criação ou configuração de ambiente de integração continuada	2 (duas) horas

- 1.4.1.15. A CONTRATADA deverá assegurar a alta disponibilidade, a segurança das soluções, o pleno funcionamento dos mecanismos de backup e de recuperação de desastres.
- 1.4.1.16. Os serviços de gerenciamento deverão ser executados por profissionais especializados no provedor de nuvem contratado conforme critérios definidos nas seções de requisitos de experiência profissional e de formação de equipe.
- 1.4.1.17. A CONTRATADA deverá disponibilizar, por meio do serviço de gerenciamento e operação, as instâncias em regime 24x7 e adotar o processo de registro e execução de demandas descrito no modelo de execução do Termo de Referência.
- 1.4.1.18. O gerenciamento de instâncias de banco de dados consiste na operação, configuração, automação, otimização e monitoramento dos bancos de dados, incluindo no mínimo as seguintes ações:
- 1.4.1.18.1. Gerenciamento das configurações da plataforma de banco de dados.
 - 1.4.1.18.2. Gerenciamento e aplicação da política de backup.
 - 1.4.1.18.3. Execução de rotinas de desempenho e tuning.
 - 1.4.1.18.4. Atualização e gerenciamento de patches e versões.
 - 1.4.1.18.5. Resolução de problemas e incidentes.
 - 1.4.1.18.6. Redimensionamento de capacidade.
 - 1.4.1.18.7. Gerenciamento dos recursos associados aos bancos de dados.
- 1.4.2. DO SERVIÇO DE MIGRAÇÃO DE MÁQUINAS VIRTUAIS OU IMAGEM DE INSTÂNCIAS
- 1.4.2.1. O escopo do serviço abrange a migração de ambiente de datacenter do CONTRATANTE (*on-premises to cloud*) para outro ambiente em nuvem utilizado pelo CONTRATANTE diferente da nuvem fornecida pela CONTRATADA (*cloud to cloud*).
- 1.4.2.2. O serviço de migração de máquinas virtuais ou imagens de instâncias deverá ser executado pela CONTRATADA preferencialmente de forma remota e sob demanda por meio de ordem de serviço específica, com escopo previamente definido.
- 1.4.2.3. A migração envolve ao menos as seguintes ações: diagnóstico, planejamento, identificação das máquinas e/ou imagens de instâncias, avaliação, preparação dos ambientes, execução, *backup* ou criação de condição de retorno em caso de falhas e estabilização do ambiente migrado em nuvem.
- 1.4.2.4. A métrica adotada para o serviço de migração é a instância migrada para o ambiente de nuvem, cujo valor é fixo independentemente da quantidade ou configuração de máquinas adotadas no ambiente original.
- 1.4.2.5. São consideradas instâncias migradas para efeitos de contabilização da métrica associada ao serviço, as instâncias de computação criadas resultantes do processo de migração, independentemente da quantidade de ambientes, aplicadas às soluções.
- 1.4.2.6. Deverá integrar o custo da unidade de serviço de migração das instâncias de computação: os recursos humanos

tecnológicos e de processos da CONTRATADA. As ferramentas e recursos de nuvem utilizados pela CONTRA exclusivamente para a realização do processo de migração deverão ser utilizados sem ônus ao CONTRATANTE.

- 1.4.2.7. O processo de migração deverá observar ao menos as seguintes etapas a serem conduzidas pela CONTRATADA:
- 1.4.2.7.1. Etapa de Avaliação do ambiente para migração (*Assessment*): Consiste na determinação do estado at escopo de recursos a serem migrados em relação ao grau de compatibilidade ou aptidão para migração. A CONTRA deverá apresentar como resultado da avaliação do ambiente um relatório técnico descrevendo as aplicações elegíveis não elegíveis. No caso das não elegíveis, deverão ser apontadas as restrições técnicas encontradas;
 - 1.4.2.7.2. Etapa de planejamento da migração: Consiste na construção de um plano de migração abrangendo no n as seguintes dimensões (construção da estrutura de recebimento dos recursos em nuvem, adoção de um n operacional padronizado e automatizado, preservação dos aspectos de segurança e conformidade);
 - 1.4.2.7.3. Etapa de execução da migração: Consiste na execução do plano de migração por meio da preparaçã ambientes a serem migrados, movimentação das cargas de trabalho, criação e configuração da estrutura de recebi dos ambientes na nuvem, operação do processo de migração, teste e validação da conclusão bem sucedida da migr;
- 1.4.2.8. A CONTRATADA deverá adotar a estratégia de migração “Lift and Shift”, também conhecida como “Rehosting tocante às aplicações e sistemas. Essa estratégia consiste na retirada do aplicativo inteiro da infraestrutura *on-prem* movimentação para o ambiente de nuvem, sem realizar alterações ou ajustes no código da aplicação.
- 1.4.2.9. Caso seja verificado na etapa de avaliação do ambiente que a aplicação não possui grau de compatibilidad migração em nuvem, será de responsabilidade do CONTRATANTE providenciar os ajustes técnicos.
- 1.4.2.10. Os serviços de migração devem observar os prazos máximos definidos a seguir, que constarão expressos na t de Serviço.

Tabela 3 – Prazos máximos para execução de serviços de migração de máquinas virtuais ou imagem de instâncias

Quantidade de instâncias de computação estimadas da OS	Prazo máximo em dias de execução da OS
1 a 5 instâncias	10 (dez) dias úteis
6 a 20 instâncias	20 (vinte) dias úteis
21 a 50 instâncias	35 (trinta e cinco) dias úteis

- 1.4.2.11. A critério do CONTRATANTE, os prazos de migração poderão ser superiores aos definidos na tabela acima, desde esteja previsto na Ordem de Serviço de forma justificada.
- 1.4.2.12. A Ordem de Serviço deverá conter a identificação da quantidade de instâncias a serem migradas, sendo limitad (cinquenta) instâncias por ordem de serviço.
- 1.4.2.13. O CONTRATANTE deverá observar o limite de 50 (cinquenta) instâncias em processo de migração concorrenten admitindo-se quantidade superior desde que em comum acordo com a CONTRATADA.

1.4.3. DO SERVIÇO DE MIGRAÇÃO DE MÁQUINAS VIRTUAIS VMWARE

- 1.4.3.1. O escopo do serviço abrange a migração de máquinas virtuais instaladas no VMware do ambiente de datacen CONTRATANTE (*on-premises to cloud*), ou de outro ambiente em nuvem utilizado pelo CONTRATANTE diferente da r fornecida pela CONTRATADA (*cloud to cloud*), para um ambiente de VMware SDDC no provedor de nuvem.
- 1.4.3.2. A migração deverá ocorrer com a utilização das tecnologias HCX vMotion e/ou HCX Cold Migration.
- 1.4.3.3. Os endereços MAC e IP das máquinas virtuais não deverão ser alterados no processo de migração.
- 1.4.3.4. O serviço de migração de máquinas virtuais VMware deverá ser executado pela CONTRATADA, preferencialmer forma remota e sob demanda por meio de ordem de serviço específica, com escopo previamente definido.
- 1.4.3.5. A migração envolve ao menos as seguintes ações: diagnóstico, planejamento, identificação das máquinas e/ou ir de instâncias, avaliação, preparação dos ambientes, execução, *backup* ou criação de condição de retorno em caso de testes e estabilização do ambiente migrado em nuvem.
- 1.4.3.6. A métrica adotada para o serviço de migração é a instância migrada para o ambiente de nuvem, cujo valor é fi instância independentemente da quantidade ou configuração de máquinas adotadas no ambiente original.
- 1.4.3.7. São consideradas instâncias migradas para efeitos de contabilização da métrica associada ao serviço, as instânc computação criadas resultantes do processo de migração, independentemente da quantidade de ambientes, aplicaç soluções.
- 1.4.3.8. Deverá integrar o custo da unidade de serviço de migração das instâncias de computação: os recursos hur tecnológicos e de processos da CONTRATADA. As ferramentas e recursos de nuvem utilizados pela CONTRA exclusivamente para a realização do processo de migração deverão ser utilizados sem ônus ao CONTRATANTE.
- 1.4.3.9. O processo de migração deverá observar ao menos as seguintes etapas a serem conduzidas pela CONTRATADA:
- 1.4.3.9.1. Etapa de Avaliação do ambiente para migração (*Assessment*) - Consiste na determinação do estado at escopo de recursos a serem migrados em relação ao grau de compatibilidade ou aptidão para migração. A CONTRA deverá apresentar como resultado da avaliação do ambiente um relatório técnico descrevendo as aplicações elegíveis não elegíveis. No caso das não elegíveis, deverão ser apontadas as restrições técnicas encontradas;
 - 1.4.3.9.2. Etapa de planejamento da migração - Consiste na construção de um plano de migração abrangendo no n as seguintes dimensões (construção da estrutura de recebimento dos recursos em nuvem, adoção de um n operacional padronizado e automatizado, preservação dos aspectos de segurança e conformidade);
 - 1.4.3.9.3. Etapa de execução da migração - Consiste na execução do plano de migração por meio da preparaçã ambientes a serem migrados, movimentação das cargas de trabalho, criação e configuração da estrutura de recebi dos ambientes na nuvem, operação do processo de migração, teste e validação da conclusão bem sucedida da migr;
- 1.4.3.10. A CONTRATADA deverá adotar a estratégia de migração “Lift and Shift”, também conhecida como “Rehosting tocante às aplicações e sistemas. Essa estratégia consiste na retirada do aplicativo inteiro da infraestrutura *on-prem* movimentação para o ambiente de nuvem, sem realizar alterações ou ajustes no código da aplicação.
- 1.4.3.11. Caso seja verificado na de etapa de avaliação do ambiente que a aplicação não possui grau de compatibilidad migração em nuvem, será de responsabilidade do CONTRATANTE providenciar os ajustes técnicos.
- 1.4.3.12. Os serviços de migração devem observar os prazos máximos definidos a seguir, que constarão expressos na t de Serviço.

Tabela 4 – Prazos máximos para execução de serviços de migração de máquinas virtuais VMware

Quantidade de instâncias de computação estimadas da OS	Prazo máximo em dias de execução da OS
1 a 5 instâncias	10 (dez) dias úteis
6 a 20 instâncias	15 (quinze) dias úteis
21 a 50 instâncias	25 (vinte e cinco) dias úteis

1.4.3.13. A critério do CONTRATANTE, os prazos de migração poderão ser superiores aos definidos na tabela acima, desde que esteja previsto na Ordem de Serviço de forma justificada.

1.4.3.14. A Ordem de Serviço deverá conter a identificação da quantidade de instâncias a serem migradas, sendo limitada a quantidade de instâncias por ordem de serviço.

1.4.3.15. O CONTRATANTE deverá observar o limite de 50 instâncias em processo de migração concorrentemente, admitindo-se quantidade superior desde que em comum acordo com a CONTRATADA.

1.4.4. DO SERVIÇO DE MIGRAÇÃO DE RECURSOS DE BANCO DE DADOS

1.4.4.1. O escopo do serviço abrange a migração de bancos de dados hospedados em ambientes de datacenter (*on-prem cloud*) ou de outro ambiente em nuvem utilizado pelo CONTRATANTE diferente da nuvem fornecida pela CONTRATADA (*cloud*).

1.4.4.2. O serviço de migração de banco de dados deverá ser executado pela CONTRATADA, preferencialmente de forma remota, sob demanda, por meio de ordem de serviço específica com escopo previamente definido.

1.4.4.3. A migração envolve ao menos as seguintes ações:

1.4.4.3.1. Diagnóstico e descoberta: identificação das cargas de trabalho e aplicações constantes do escopo da migração, incluindo a realização de processos de *Assessment*, inventário automatizado e mapeamento da relação entre recursos e aplicações;

1.4.4.3.2. Planejamento: definição da estratégia de migração observando custos, prazos e riscos;

1.4.4.3.3. Identificação dos bancos de dados e recursos de computação e infraestrutura necessários para as necessidades de negócio associadas à demanda;

1.4.4.3.4. Levantamento da arquitetura dos bancos de dados, estruturas de dados e metadados;

1.4.4.3.5. Realização de processos de conversão, tratamento e exportação de dados quando necessário;

1.4.4.3.6. Provisionamento, dimensionamento e alocação de estrutura em nuvem para recepção das cargas de trabalho envolvendo quaisquer recursos e serviços de computação constantes da Tabela 1;

1.4.4.3.7. Realização da migração e de testes e verificações das cargas de trabalho;

1.4.4.3.8. Monitoramento das cargas de trabalho durante o período de estabilização dos serviços; e

1.4.4.3.9. Realização de processos de *backup* e criação de condições de retorno, caso haja situações não previstas no planejamento, que impeçam o funcionamento adequado das cargas de trabalho.

1.4.4.4. A migração deverá envolver também a adaptação ou ajustes de objetos de banco de dados para utilização no ambiente de nuvem, bem como a devida conexão com as respectivas aplicações que utilizam as bases de dados migradas.

1.4.4.5. A métrica adotada para o serviço de migração é a instância migrada para o ambiente de nuvem, cujo valor é fixado independentemente da quantidade ou configuração de máquinas adotadas no ambiente original.

1.4.4.6. São consideradas instâncias migradas de banco de dados para efeitos de contabilização da métrica associada ao serviço, as instâncias de banco de dados gerenciado criadas, resultantes do processo de migração, independentemente da quantidade de ambientes, aplicações e soluções.

1.4.4.7. Deverá integrar o custo da unidade de serviço de migração das instâncias de banco de dados: os recursos tecnológicos e de processos da CONTRATADA. As ferramentas e recursos de nuvem utilizados pela CONTRATADA exclusivamente para a realização do processo de migração deverão ser utilizados sem ônus adicional ao CONTRATANTE.

1.4.4.8. O processo de migração das instâncias de banco de dados deverá observar ao menos as seguintes etapas a serem conduzidas pela CONTRATADA:

1.4.4.8.1. Etapa de Avaliação do ambiente para migração (*Assessment*) - Consiste na determinação do estado do ambiente de recursos a serem migrados em relação ao grau de compatibilidade ou aptidão para migração. Essa avaliação de compatibilidade ao ambiente de nuvem deve abranger no mínimo as seguintes dimensões: construção da estrutura de dados, recebimento dos recursos em nuvem, adoção de um modelo operacional padronizado e automatizado, preservação dos aspectos de segurança e conformidade. A CONTRATADA deverá apresentar como resultado da avaliação do ambiente relatório técnico descrevendo as aplicações elegíveis e as não elegíveis. No caso das não elegíveis, deverão ser apontadas as restrições técnicas encontradas;

1.4.4.8.2. Etapa de planejamento da migração - Consiste na construção de um plano de migração abrangendo no mínimo as seguintes dimensões: construção da estrutura de recebimento dos recursos em nuvem, adoção de um modelo operacional padronizado e automatizado, preservação dos aspectos de segurança e conformidade;

1.4.4.8.3. Etapa de preparação do ambiente de banco de dados - Consiste no transporte para o ambiente em nuvem, incluindo ao menos preparação e conversão de dados e objetos, atualização de *patches* ou versões, resolução de incompatibilidades, ajustes e correções de esquemas e de objetos; e

1.4.4.8.4. Etapa de execução da migração - Consiste na execução do plano de migração por meio da preparação das cargas de trabalho e dados a serem migradas, movimentação das cargas de trabalho e dados, criação e configuração da estrutura de recebimento dos ambientes na nuvem, operação do processo de migração, teste e validação da migração bem sucedida da migração.

1.4.4.9. A CONTRATADA deverá adotar as medidas necessárias de segurança para assegurar a integridade, autenticidade, confidencialidade e disponibilidade dos dados, estruturas e metadados em todo o processo de migração.

1.4.4.10. A CONTRATADA deverá adotar, preferencialmente, a distribuição sob o modelo de plataforma como serviço (PaaS) como critério do CONTRATANTE, ou em casos de incompatibilidades a estratégia de migração "Lift and Shift", também conhecido como "Rehosting", no tocante às aplicações e sistemas (sem realizar alterações ou ajustes no código da aplicação).

1.4.4.11. Caso seja verificado na etapa de avaliação do ambiente que a aplicação não possui grau de compatibilidade para migração em nuvem, será de responsabilidade do CONTRATANTE providenciar os ajustes técnicos.

1.4.4.12. Os serviços de migração devem observar os prazos máximos definidos a seguir, que constarão expressos na Ordem de Serviço:

Tabela 5 - Prazos máximos para execução de serviços de migração de recursos de banco de dados

Quantidade de instâncias de computação estimadas da OS	Prazo máximo em dias de execução da OS
1 a 5 instâncias	30 (trinta) dias úteis

1.4.4.13. A critério do CONTRATANTE, o prazo de migração poderá ser superior ao definido na tabela acima, desde que previsto na Ordem de Serviço de forma justificada.

1.4.4.14. A Ordem de Serviço deverá conter a identificação da quantidade de instâncias a serem migradas, sendo limitada (cinco) instâncias por ordem de serviço.

1.4.4.15. O CONTRATANTE deverá observar o limite de 5 instâncias em processo de migração concorrentemente, admitir quantidade superior desde que em comum acordo com a CONTRATADA.

1.5. REQUISITOS DE ARQUITETURA TECNOLÓGICA

1.5.1. A arquitetura das soluções de TI, objeto deste documento, deverá observar ao menos os seguintes princípios de excelência em operação em nuvem:

1.5.1.1. Permitir o uso de operações como código (*Operations as Code*): Ser capaz de prover e definir uma carga de trabalho (aplicações e infraestrutura) como código e atualizá-la como código.

1.5.1.2. Permitir o uso de documentação baseada em anotações (*Annotate Documentation*): Anotações são utilizadas para as operações via código.

1.5.1.3. Permitir mudanças constantes, pequenas e frequentes: O design das cargas de trabalho deve permitir que componentes sejam atualizados com frequência.

1.5.1.4. Permitir a antecipação de falhas: Ser capaz de permitir a simulação de cenários, realização de teste e validação de requisitos antes de entrada em produção.

1.5.2. As arquiteturas criadas em ambiente de nuvem devem:

1.5.2.1. Ser precedidas de planejamento.

1.5.2.2. Possuir cotas que limitem o consumo de determinado recurso de acordo com as necessidades do CONTRATANTE.

1.5.2.3. Permitir o gerenciamento de capacidade das cargas de trabalho com antecedência com vistas a evitar a limitação inesperada do consumo de recursos.

1.5.2.4. Prever mecanismos de controle de custos por meio de alertas relacionados a situações em que os gastos atingiram determinados limites.

1.5.2.5. Ser projetadas observando padrões mínimos de segurança, incluindo: controle de acesso, uso de mecanismos de monitoramento, gestão de credenciais, segmentação de rede, entre outros recomendados pelo provedor.

1.6. REQUISITOS DE PROJETO E DE IMPLEMENTAÇÃO

1.6.1. Os Serviços de Computação em nuvem (Item 1 da contratação), de Gerenciamento e Operação de recursos em nuvem (Item 2 da contratação) e de migração (Itens 3, 4 e 5 da contratação) deverão ser executados observando um projeto definido pela CONTRATADA e aprovado pelo CONTRATANTE com no mínimo:

1.6.1.1. Arquitetura da solução prevista em nuvem.

1.6.1.2. Identificação das cargas de trabalho e recursos computacionais previstos.

1.6.1.3. Considerações sobre segurança da informação.

1.6.1.4. Estimativa de custos para os próximos três meses, no mínimo.

1.6.2. As integrações e os desenvolvimentos de soluções de interoperabilidade, sempre que possível, serão pautados em plataformas livres, na arquitetura orientada a modelos e utilizando *frameworks* disponibilizados no Portal do Software Livre Brasileiro.

1.6.3. O desenvolvimento dos produtos deverá utilizar *frameworks*, bibliotecas, componentes, ferramentas, códigos-fonte e utilitários que sejam portáteis para outros ambientes de nuvem.

1.6.4. As prospecções tecnológicas deverão evitar propostas que dependam somente de plataformas proprietárias e que dependam de único fornecedor, salvo quando autorizado pelo CONTRATANTE.

1.7. REQUISITOS DE IMPLANTAÇÃO

1.7.1. A CONTRATADA deverá adotar mecanismos de automação e de implantação contínua.

1.7.2. Deverão ser adotadas práticas ágeis pela CONTRATADA na operação, implantação e automação de processos e cargas de trabalho no ambiente de nuvem.

1.8. REQUISITOS DE GARANTIA E ASSISTÊNCIA TÉCNICA

1.8.1. A CONTRATADA deverá reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios ou defeitos nos recursos e serviços de computação em nuvem.

1.9. REQUISITOS DE FORMAÇÃO DA EQUIPE

1.9.1. No âmbito da solução (quaisquer itens), o planejamento e projeto dos serviços de computação em nuvem deverão ser supervisionados por um arquiteto de nuvem e por um especialista em segurança da informação da CONTRATADA.

1.9.2. No âmbito dos serviços de computação em nuvem (item 1 da contratação), o provisionamento, configuração e monitoramento dos recursos de computação em nuvem deverão ser operacionalizados por um administrador de nuvem.

1.9.3. No âmbito dos serviços de gerenciamento de nuvem (item 2 da contratação), as atividades deverão ser realizadas por um administrador de nuvem e supervisionada por um arquiteto de nuvem e por um especialista em segurança da informação.

1.9.4. No âmbito dos serviços de migração (itens 3, 4 e 5 da contratação), as atividades deverão ser executadas por ao menos um administrador de nuvem, um arquiteto em nuvem e um especialista em segurança da informação. Para aquelas cargas de trabalho que envolvem banco de dados, deve ser apoiada por um especialista em banco de dados.

1.9.5. No âmbito dos serviços de treinamento (Item 6 da contratação), as atividades deverão ser executadas por ao menos um instrutor de serviços de nuvem.

1.10. REQUISITOS DE METODOLOGIA DE TRABALHO

1.10.1. Os papéis e responsabilidades da CONTRATADA e os diferentes serviços previstos neste documento são descritos na m seguir. São utilizados os seguintes elementos para caracterizar a forma de relação entre o ator e o respectivo papel ou função:

1.10.1.1. Responsável (R): executor da função.

1.10.1.2. Avaliador (A): instância de aprovação prévia.

1.10.1.3. Consultado (C): possui informações e capacidade necessária à conclusão do serviço.

1.10.1.4. Informado (I): deve ser notificado após a conclusão do serviço.

1.10.2. Há dois cenários de execução dos serviços de computação em nuvem previstos neste documento: a oferta de recur: computação por intermédio do provedor de nuvem (Cenário 1 - uso dos serviços dos Item 1 da contratação) e a oferta de re de computação em nuvem, incluindo uma camada de gerenciamento total dos recursos (Cenário 2 - uso dos serviços do Item Item 2 da contratação).

1.10.3. O modelo proposto nesta contratação admite a coexistência de ambos cenários durante a execução do contrato. exemplo, o CONTRATANTE pode adotar três modelos distintos:

1.10.3.1. Parcialmente gerenciado: Demandar apenas os serviços de computação em nuvem (Item 1 da contratação) e n o provisionamento, gerenciamento e operação dos recursos utilizando a plataforma de gestão de recursos do provedor.

1.10.3.2. Totalmente gerenciado: Demandar os serviços de computação em nuvem (Item 1 da contratação) e adicional requerer os serviços de gerenciamento completo desses recursos (Item 2 da contratação). Neste caso, a CONTRATADA a a responsabilidade total pelo provisionamento, gerenciamento e operação dos serviços de computação em nuvem.

1.10.3.3. Híbrido: Adotar para parte dos recursos de computação em nuvem o modelo parcialmente gerenciado e para parte dos recursos (geralmente aqueles com maior criticidade) adotar o modelo totalmente gerenciado.

1.10.4. Em um modelo parcialmente gerenciado, a CONTRATADA atua provendo os serviços por intermédio do provedor de n cenário em que se utiliza apenas os serviços constantes do Item 1 da contratação, conforme tabela a seguir. Dessa forma, ter seguinte distribuição de responsabilidades para o modelo de governança:

Tabela 6 - Distribuição de responsabilidades em um modelo parcialmente gerenciado

Função na prestação dos Serviços de Computação em Nuvem	CONTRATANTE (Órgão/Entidade)	CONTRATADA (Integrador)
Planejamento/Demanda	A/I	R
Projeto/Design	A/I	R
Execução/Provisionamento	I	R
Operação/Gerenciamento	R	I
Monitoramento	R	R
Gerenciamento de Custos	A/I	R
Suporte técnico	I	R

1.10.5. O modelo é denominado parcialmente gerenciado porque apesar da responsabilidade de projeto, execução e monitora serem da CONTRATADA, o CONTRATANTE realiza a operação e gerenciamento do ambiente.

1.10.6. Em um modelo totalmente gerenciado, a CONTRATADA atua provendo os serviços de gerenciamento complet intermédio dos provedores de nuvem. Neste modelo são demandados serviços constantes do Item 1 da contrataç adicionalmente, os serviços do Item 2 da contratação. Dessa forma, tem-se a seguinte distribuição de responsabilidades | modelo de governança:

Tabela 7 - Distribuição de responsabilidades em um modelo totalmente gerenciado

Função na prestação dos Serviços de Computação em Nuvem	CONTRATANTE (Órgão/Entidade)	CONTRATADA (Integrador)
Planejamento/Demanda	A/I	R
Projeto/Design	A/I	R
Execução/Provisionamento	I	R
Operação/Gerenciamento	I	R
Monitoramento	I	R
Gerenciamento de Custos	A/I	R
Suporte técnico	I	R

1.10.7. Neste modelo, uma vez incluídas as instâncias de computação (Item 1 da contratação) no escopo de gerencia completo (Item 2 da contratação), todos os recursos associados aquelas instâncias, incluindo as próprias instâncias, são geren pela CONTRATADA. O gerenciamento abarca o controle total de custos de acordo com as diretrizes, limites e alçadas constant ordens de serviço. O papel do CONTRATANTE está mais centrado em aprovação de certas atividades ou de receber inform prestadas pela CONTRATADA.

1.11. REQUISITOS TÉCNICOS DE SEGURANÇA

1.11.1. A CONTRATADA deverá adotar todas as medidas necessárias para assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações a serem tratadas na nuvem.

1.11.2. A CONTRATADA deverá implementar medidas para garantir a proteção dos dados, antecipando ameaças à privacidade, segurança e à integridade, prevenindo acesso não autorizado às informações.

1.11.3. A CONTRATADA deverá disponibilizar os recursos de computação em provedor que possua ao menos as certificações: NBR ISO/IEC27001:2013 (Segurança Cibernética); ISO/IEC 27017:2016 (Segurança para Computação em Nuvem) ou CSA Certification (Certificado independente de auditoria externa para provedores de computação em nuvem) LEVEL TWO ou supe ISO/IEC 27018:2014 (Proteção de Dados Pessoais em Nuvem), com validade vigente durante a execução do contrato, refere infraestrutura de datacenter onde os serviços em nuvem estarão hospedados.

1.11.4. As certificações ABNT NBR ISO/IEC 27001:2013, ISO/IEC 27017:2016 e ISO/IEC 27018:2014 e deverão ser apresent: serão aceitas nas suas versões originais em inglês.

- 1.11.5. Os provedores de serviços em nuvem, deverão demonstrar através da CONTRATADA estar em conformidade com os padrões de segurança de nuvem através de auditoria anual do tipo SOC 2, ou superior, conduzida por um auditor independente, apresentação dos relatórios de tipo I ou tipo II.
- 1.11.6. A CONTRATADA deverá apresentar, anualmente, a auditoria citada no item anterior, o que será essencial para garantir que o PROVEDOR continue em conformidade com os padrões de segurança durante a vigência do contrato.
- 1.11.7. São requisitos exigidos com relação à Política de Segurança da Informação, devendo a CONTRATADA:
- 1.11.7.1. Obedecer aos critérios, padrões, normas e procedimentos operacionais adotados pelo TRF6;
 - 1.11.7.2. Manter sigilo, sob pena de responsabilidades civis, penais e administrativas, sobre todo e qualquer assunto de interesse do TRF6 ou de terceiros de que tomar conhecimento em razão da execução do objeto do Contrato, devendo o provedor manter seus empregados nesse sentido;
 - 1.11.7.3. Promover o afastamento, no prazo máximo de 24 (vinte e quatro) horas após o recebimento da notificação por escrito de qualquer dos seus recursos humanos que não correspondam aos critérios de confiança ou que perturbe a ação da equipe de fiscalização do TRF6;
 - 1.11.7.4. O pedido de afastamento será motivado e justificado pelo TRF6;
 - 1.11.7.5. Responsabilizar-se pelos materiais, produtos, ferramentas, instrumentos e equipamentos eventualmente disponibilizados para a execução dos serviços, não cabendo ao TRF6 qualquer responsabilidade por perdas decorrentes de roubo, furto ou outros fatos que possam vir a ocorrer, cabendo à CONTRATADA o ressarcimento de quaisquer dos itens mencionados, em quantidade e qualidade, sem prejuízo das penalidades cabíveis;
 - 1.11.7.6. Não veicular publicidade acerca dos serviços contratados, sem prévia autorização, por escrito, do TRF6;
 - 1.11.7.7. Manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações relativas:
 - 1.11.7.7.1. à política de segurança adotada pelo TRF6 e as configurações de hardware e de softwares decorrentes;
 - 1.11.7.7.2. ao processo de instalação, configuração e adaptações de produtos, ferramentas e equipamentos;
 - 1.11.7.7.3. ao processo de implementação, no ambiente do TRF6, dos mecanismos de criptografia e autenticação;
- 1.11.8. A equipe técnica da CONTRATADA deverá assinar o Anexo III - Modelo de Termo de Ciência antes de iniciar suas atividades junto ao TRF6, bem como na substituição de integrante de equipe, nos casos especificados;
- 1.11.9. Submeter seus recursos humanos aos regulamentos de segurança e disciplina instituídos pelo TRF6 durante a execução dos serviços, e, principalmente, durante a permanência nas suas dependências.
- 1.11.10. Dos planos e procedimentos
- 1.11.10.1. A Solução ofertada pela CONTRATADA deverá dispor de plano de comunicação de incidentes, devendo a CONTRATADA informar 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 terem acarretado dano à confidencialidade, disponibilidade, integridade ou autenticidade dos dados do CONTRATANTE.
 - 1.11.10.2. Os serviços ofertados deverão contemplar análise e gestão de riscos de segurança de informação. A análise de riscos deve ter periodicidade, no mínimo, trimestral 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, plano de tratamento e monitoramento dos riscos, assunção ou não dos riscos e outras informações pertinentes.
 - 1.11.10.3. A CONTRATADA deve possuir e manter disponíveis ao CONTRATANTE:
 - 1.11.10.3.1. O plano de continuidade com as ações de recuperação de desastres e contingência de negócio;
 - 1.11.10.3.2. Os resultados dos testes trimestrais de análise de riscos de segurança da informação;
 - 1.11.10.3.3. Plano de resposta a incidentes com os procedimentos relacionados à prevenção e resposta aos incidentes referentes aos serviços objetos do Termo de Referência;
 - 1.11.10.3.4. Os resultados das respostas a incidentes relacionados com os serviços.
- 1.11.11. Da segurança de identidades
- 1.11.11.1. Os serviços de nuvem ofertados deverão dispor de mecanismo de garantia de identidade realizada previamente à execução das requisições dos usuários.
 - 1.11.11.2. Os serviços de nuvem ofertados devem permitir a criação e gerenciamento de perfis e credenciais de segurança para o CONTRATANTE e para seus usuários.
 - 1.11.11.3. Os serviços de nuvem ofertados deverão permitir que somente os usuários autorizados pelo CONTRATANTE tenham acesso aos recursos em conformidade aos respectivos perfis de uso.
 - 1.11.11.4. Os serviços de nuvem ofertados deverão permitir autenticação de usuário para controlar o acesso aos dados, mecanismos de controle de acesso, como políticas de permissões e listas de controle de acesso para conceder seletiva permissões para usuários e grupos de usuários.
 - 1.11.11.5. Os serviços de nuvem ofertados deverão permitir a realização de forma segura de *upload/download* de arquivos utilizando protocolos SSL e HTTPS.
 - 1.11.11.6. Os serviços de nuvem ofertados deverão permitir a definição de regras que se aplicam, em geral, a todas as solicitações para seus recursos, tais como a concessão de privilégios de gravação para um subconjunto dos recursos contratados.
- 1.11.12. Da segurança dos dados e requisições
- 1.11.12.1. Os serviços de nuvem ofertados deverão permitir ou negar uma requisição baseada no endereço IP de origem do requisitante.
 - 1.11.12.2. Os serviços de nuvem ofertados deverão permitir que o CONTRATANTE restrinja o acesso a determinados recursos com base em aspectos da requisição.
 - 1.11.12.3. Os serviços de nuvem ofertados deverão utilizar protocolos seguros para autenticar as requisições, por exemplo, HMAC (*Hash Message Authentication Code*) - SHA1, conforme RFC 2104, utilizando codificação Base 64.
 - 1.11.12.4. Os serviços de nuvem ofertados 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 ou para um objeto.
 - 1.11.12.5. Os serviços de nuvem ofertados deverão permitir a autenticação de sequência de caracteres da requisição de usuário, por exemplo, os clientes poderão criar uma URL para um objeto que só é válida por um tempo limitado.
- 1.11.13. Das chaves de segurança

- 1.11.13.1. Os serviços de nuvem ofertados deverão dispor de mecanismo para gestão integrada de chaves de segurança permita tratar, gerenciar e proteger chaves usando várias camadas de segurança.
- 1.11.13.2. Os serviços de nuvem ofertados deverão permitir que os dados e objetos sejam criptografados e descriptografados sem perda de desempenho substancial.
- 1.11.13.3. Os serviços de nuvem ofertados deverão permitir recursos para trilha de auditoria, permitindo visualizar quem determinada chave para acessar um objeto, qual objeto foi acessado e quando ocorreu esse acesso.
- 1.11.13.4. Os serviços de nuvem ofertados deverão permitir visualizar tentativas mal sucedidas de acesso por usuário sem permissão para descriptografar os dados.
- 1.11.13.5. Os serviços de nuvem ofertados deverão permitir que os usuários criptografem seus dados e objetos antes de serem armazenados para o serviço de armazenamento.
- 1.11.13.6. Os serviços de nuvem ofertados deverão permitir que cada objeto ou recurso protegido seja criptografado com uma chave exclusiva.
- 1.11.13.7. Os serviços de nuvem ofertados deverão permitir que a própria chave de objeto ou recurso seja criptografada com uma chave separada.
- 1.11.13.8. Os serviços de nuvem ofertados deverão permitir que dados criptografados, chaves de criptografia e chaves de descriptografia sejam armazenadas e protegidas em hosts separados e protegidos por várias camadas de proteção.
- 1.11.13.9. Os serviços de nuvem ofertados deverão permitir que eventos relativos à segurança de chaves sejam registrados para a auditoria da segurança de chaves.
- 1.11.14. Da disponibilidade e continuidade dos serviços
- 1.11.14.1. Os serviços de nuvem ofertados pela CONTRATADA deverão dispor de sistema de hardware e dados para recuperação crítica com política de "Disaster Recovery", balanceamento, conectividade e *backup/restore* durante toda a vigência do contrato com garantia de *Recovery Time Objective* (RTO) em até 3 horas e de *Recovery Point Objective* (RPO) de 1 hora.
- 1.11.15. Da segurança dos dados e informações
- 1.11.15.1. É vedado o tratamento em ambiente de nuvem de informações não autorizadas pelo CONTRATANTE.
- 1.11.15.2. É vedada à CONTRATADA ou ao provedor acesso aos dados hospedados na infraestrutura de nuvem, sem prévia autorização formal por parte do CONTRATANTE.
- 1.11.15.3. Os serviços de nuvem ofertados deverão prover mecanismo de acesso protegido aos dados por meio de criptografia, garantindo que apenas aplicações e usuários autorizados tenham acesso.
- 1.11.15.4. Os serviços de nuvem ofertados deverão permitir a criptografia automática de dados e objetos armazenados com o padrão AES (*Advanced Encryption Standard*) de no mínimo 256 bits ou outro algoritmo com força de chave equivalente ou superior neste último caso desde que aprovado pelo CONTRATANTE.
- 1.11.15.5. Os serviços de nuvem ofertados deverão possibilitar comunicação criptografada e protegida para transferência de dados.
- 1.11.15.6. Os serviços ofertados 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.
- 1.11.15.7. A CONTRATADA deve implementar controles para isolamento e segurança de sistema operacional.
- 1.11.15.8. A CONTRATADA deve utilizar soluções de virtualização de servidores que sejam padrões ou referências de mercado.
- 1.11.15.9. A CONTRATADA deverá criar uma política de atualização de versão de software, indicando sua criticidade e acordando junto ao CONTRATANTE qual a melhor data para ser aplicada.
- 1.11.15.10. A CONTRATADA comprometer-se-á a preservar os dados do CONTRATANTE contra acessos indevidos e abster-se 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.
- 1.11.15.11. 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.
- 1.11.15.12. A partir do ponto de entrada/saída da Internet nos datacenters dos provedores ofertados, deverão ser observadas as seguintes disposições:
- 1.11.15.12.1. Inviolabilidade e sigilo do fluxo de suas comunicações pela rede, salvo por ordem judicial, na forma da legislação aplicável.
- 1.11.15.12.2. Inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial.
- 1.11.15.12.3. 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.
- 1.11.15.12.4. Fornecer ao CONTRATANTE, sempre que solicitado, informações claras e completas sobre coleta, armazenamento, tratamento e proteção de dados do CONTRATANTE.
- 1.11.15.13. A quebra do sigilo das informações restritas reveladas, devidamente comprovada, sem autorização expressa do CONTRATANTE, possibilitará a imediata rescisão de contrato firmado entre o CONTRATANTE e a Contratada sem que qualquer tipo de ressarcimento a esta. Nesse caso, a CONTRATADA estará sujeita, por ação ou omissão, ao ressarcimento das perdas e danos sofridos pelo CONTRATANTE, inclusive os de ordem moral, bem como as de responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.
- 1.11.16. Da localização dos dados e informações
- 1.11.16.1. A CONTRATADA deverá assegurar que os dados, metadados, informações e conhecimento, produzidos e armazenados pelo CONTRATANTE, bem como suas cópias de segurança, residam em território brasileiro.
- 1.11.16.2. Todos os provedores ofertados pela CONTRATADA deverão possuir ao menos 1 (um) datacenter em território nacional.

1.12. REQUISITOS DE SEGURANÇA INSTITUCIONAL

- 1.12.1. O CONTRATANTE deverá cientificar a CONTRATADA sobre as normas internas vigentes relativas à segurança, incluindo aquelas relacionadas ao controle de acesso de pessoas e veículos, bem como sobre a Política de Segurança da Informação.
- 1.12.2. Para que a CONTRATADA atenda aos requisitos exigidos com relação à Política de Controle de Acesso, deverá:
- 1.12.2.1. Responsabilizar-se pelo credenciamento e descredenciamento de acesso às dependências do TRF6, assuando quaisquer prejuízos porventura causados por dolo ou culpa de seus profissionais.

1.12.2.2. Solicitar, por escrito, credenciamento e autorização de acesso para os recursos humanos da CONTRATADA.

1.12.2.3. Informar e solicitar ao GESTOR ou FISCAL TÉCNICO do CONTRATANTE, no prazo máximo de 24 (vinte e quatro) horas, o credenciamento dos recursos desvinculados da prestação de serviços com o CONTRATANTE.

1.12.2.4. Devolver para o CONTRATANTE todos os recursos e equipamentos eventualmente disponibilizados, como cartões certificadores, "pen drives" e outros, de propriedade do CONTRATANTE, juntamente com a solicitação de credenciamento.

1.13. REQUISITOS TÉCNICOS DOS LINKS DE DADOS DEDICADOS

1.13.1. Link de Dados Primário Dedicado ao Provedor de Nuvem (LDP) - Item 7 da contratação

1.13.1.1. Trata-se de conjunto de softwares, hardwares, licenciamentos e serviços necessários para implementar uma conexão direta e dedicada entre a rede interna da CONTRATANTE (Datacenter - localizado fisicamente em Belo Horizonte / MG) e a rede interna do Provedor de Nuvem disponibilizada para a CONTRATANTE.

1.13.1.2. O LDP deverá ser do tipo exclusivo e dedicado para o CONTRATANTE, não sendo admitidos compartilhamentos de recursos com outros clientes.

1.13.1.3. O LDP não poderá utilizar nenhum tipo de recurso de Internet, mesmo que na forma de túneis VPN ou tecnologia de abstração de transporte de dados.

1.13.1.4. O LDP deverá funcionar de forma contínua e ininterrupta, durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e durante todos os dias do ano.

1.13.1.5. O LDP deverá ser do tipo full duplex (comunicação simultânea nos dois sentidos de fluxo de dados), com capacidade de 5 Gbps (cinco gigabits por segundo), possuir latência máxima de 30 ms (trinta milissegundos), possuir taxa máxima de pacotes de 0,5% (zero vírgula cinco por cento) e ser simétrica (mesmas capacidades e características nos dois sentidos de fluxo de dados).

1.13.1.6. Para fins práticos de medição de latência e perda de pacotes, para aceitação do objeto, deverá ser utilizado o envio de pacotes ICMP *echo request* de 1500 bytes de "payload" por equipamento IPv4 da CONTRATANTE (equipamento físico conectado diretamente na extremidade da ligação instalada no centro de dados da CONTRATANTE, em direção ao equipamento IPv4 da CONTRATANTE, conectado diretamente no outro lado da ligação (máquina virtual executando o Provedor de Nuvem), que deverá transmitir de volta os correspondentes pacotes ICMP *echo response*. A medição deverá ocorrer durante um período contínuo de 15 (quinze) minutos, onde o fluxo de pacotes será o de envio de um pacote ICMP de 1500 bytes de "payload", a cada 30 ms (trinta milissegundos).

1.13.1.7. Todos os equipamentos (físicos ou virtuais) existentes entre a máquina virtual no Provedor de Nuvem e a máquina física no centro de dados da CONTRATANTE serão tratados apenas como parte do meio de comunicação que provê o LDP.

1.13.1.8. Por latência máxima de 30 ms (trinta milissegundos), entenda-se o tempo decorrido entre o momento do envio do primeiro bit dos dados em uma extremidade da ligação e o momento do recebimento do último bit dos dados na outra extremidade da ligação, tendo sido o dado transmitido de volta na outra extremidade, conforme medição realizada anteriormente. Ao final dos testes, nenhuma das latências medidas no fluxo de pacotes (tempo de trânsito de ida e volta de cada pacote) poderá ser maior do que 30 ms (trinta milissegundos).

1.13.1.9. Por perda máxima de pacotes de 0,5% (zero vírgula cinco por cento), entenda-se a perda máxima de 0,5% (zero vírgula cinco por cento) dos pacotes transmitidos em um fluxo contínuo ICMP, conforme medição descrita anteriormente.

1.13.1.10. A CONTRATADA deverá, a critério da CONTRATANTE, prover conexão simultânea através do mesmo LDP aos provedores de nuvem ofertados para prestação do serviço de nuvem, utilizando-se o mesmo ponto de presença.

1.13.1.11. O LDP deverá ser capaz de trafegar/rotear as famílias de protocolos TCP/IP, tanto IPv4 quanto IPv6, nativamente sem a utilização de túneis (6to4 ou 4to6, por exemplo) e sem a utilização de conversão de pacotes.

1.13.1.12. Os pacotes que trafegarão no LDP poderão utilizar endereços privados e não privados, tanto IPv4 quanto IPv6, sem que haja problemas de conflito ou colisões com outros clientes.

1.13.1.13. Os endereços privados serão de fornecimento exclusivo da CONTRATANTE.

1.13.1.14. O LDP deverá adotar endereços IPv4 e IPv6 válidos em seus componentes, todos fornecidos pelo Provedor de Nuvem para uso exclusivo do CONTRATANTE.

1.13.1.15. Em caso de não haver a possibilidade de fornecimento deste endereçamento pelo Provedor de Nuvem, o LDP deverá adotar endereçamento IPv4 (privados - RFC1918) e IPv6 (Unique Local Address) fornecidos exclusivamente pela CONTRATANTE, sem limitações ou restrições de operação.

1.13.1.16. Todos os componentes da LDP serão de responsabilidade exclusiva da CONTRATADA, devendo a mesma estabelecer acordos de nível de serviços (ANSS / SLAs) com seus parceiros ou subcontratados que atendam aos requisitos de disponibilidade do CONTRATANTE.

1.13.1.17. A CONTRATADA deverá possuir telefone do tipo 0800 para abertura de chamados em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e durante todos os dias do ano.

1.13.1.18. Em caso de interrupção, falha ou degradação do funcionamento do LDP, a CONTRATADA tem os seguintes prazos máximos, contados a partir do momento do início do evento:

1.13.1.18.1. 15 (quinze) minutos para detecção do evento e para iniciar os procedimentos de reparo, independentemente de notificação ou ciência da CONTRATANTE.

1.13.1.18.2. 20 (vinte) minutos para notificação (via email) da CONTRATANTE.

1.13.1.18.3. 4 (quatro) horas para restabelecer o funcionamento normal da LDP.

1.13.1.18.4. Caso haja indisponibilidade simultânea da LDP e LDS (primário e secundário), o prazo máximo de restabelecimento do serviço será reduzido para 1 (uma) hora.

1.13.1.19. O LDP será composto pelos seguintes componentes mínimos, cada um com as suas respectivas características:

1.13.1.19.1. Ponto de Presença Autorizado para Conexão Direta ao Provedor de Nuvem (PP).

1.13.1.19.1.1. Trata-se de instalação localizada em território nacional (construído e operado fisicamente dentro do Brasil), do tipo Centro de Dados (Datacenter), devidamente autorizada pelo Provedor de Nuvem para receber a conexão.

1.13.1.19.1.2. Deve ser mantido e operado por empresa devidamente autorizada pelo Provedor de Nuvem para a prestação de serviço de disponibilização/hospedagem de Ligação Direta e Dedicada ao Provedor de Nuvem.

1.13.1.19.2. Ligação dedicada entre o datacenter do CONTRATANTE e o Ponto de Presença (LDC)

1.13.1.19.2.1. Conjunto de softwares, hardwares, licenciamentos e serviços, que implementam todos os meios físicos e serviços necessários para prover a ligação direta e dedicada da rede interna da CONTRATANTE a um ponto de presença do Provedor de Nuvem.

1.13.1.19.2.2. A LDC será entregue em uma extremidade no PP e em outra extremidade no centro de (Datacenter) da CONTRATANTE.

1.13.1.19.2.3. A LDC utilizará apenas a rede interna da empresa especializada em telecomunicações e não utilizará Internet ou tráfegará dados pela Internet (mesmo que seja dentro de túneis VPN ou tecnologias similares de abstração de transporte de dados), sob nenhuma hipótese, para sua implementação.

1.13.1.19.2.4. A LDC será de uso exclusivo da CONTRATANTE, não podendo compartilhar nenhum tipo de recurso (seja ele qual for) com outro cliente.

1.13.1.19.2.5. A LDC deverá ser do tipo full-duplex (permitir tráfego simultâneo nos dois sentidos), ter capacidade mínima de 5 Gbps (cinco gigabits por segundo), ser simétrica (ter as mesmas capacidades e características nos dois sentidos de fluxo de dados) e, como irá compor a Ligação de Dados com o Provedor de Nuvem, deve suprir todos os requisitos indicados em sua especificação.

1.13.1.19.2.6. A LDC, deverá utilizar apenas enlaces de fibra ótica em toda a sua extensão.

1.13.1.19.2.7. A conexão final entre o equipamento da CONTRATANTE e a extremidade da LDC implantada no centro de dados da CONTRATANTE poderá ser realizada através de *patch cord* duplex fibra OM4 LC em interface Base-SR LC.

1.13.1.19.3. Ligação Direta e Dedicada ao Provedor de Nuvem (LPN)

1.13.1.19.3.1. Conjunto de softwares, hardwares, licenciamentos e serviços providos diretamente pelo Provedor de Nuvem, que implementam a interconexão da rede interna do Provedor de Nuvem à rede privada de cliente.

1.13.1.19.3.2. A LPN será entregue em Ponto de Presença autorizado para conexão direta junto ao provedor;

1.13.1.19.3.3. Para fins de efetivação da LPN, a CONTRATANTE deverá utilizar o serviço de computação em nuvem "Porta de conexão de fibra 5 Gbps" da Tabela 1 deste documento.

1.13.1.19.4. Interconexão entre o LDC e o LPN (IDCPN)

1.13.1.19.4.1. Conjunto de softwares, hardwares, licenciamentos e serviços, disponibilizados e implantados fisicamente dentro do PP, que implementam todos os mecanismos e serviços necessários para prover a interconexão entre a LPN e a LDC.

1.13.1.19.4.2. Esta Interconexão utilizará apenas a rede interna da empresa autorizada (para a prestação do serviço sendo vedada a utilização, sob qualquer hipótese, de tráfego de dados através da Internet, ainda que a conexão seja através de túneis de VPN ou tecnologias similares de abstração de transporte de dados).

1.13.1.19.4.3. Esta Interconexão será de uso exclusivo da CONTRATANTE, não podendo compartilhar nenhum tipo de recurso (seja ele qual for) com outro cliente do Provedor de Nuvem ou com outro cliente da empresa mantendo esta Interconexão.

1.13.1.19.4.4. Esta Interconexão deverá ser do tipo full-duplex (permitir tráfego simultâneo nos dois sentidos), ter capacidade mínima de 5 Gbps (cinco gigabits por segundo), ser simétrica (ter as mesmas capacidades e características nos dois sentidos de fluxo de dados) e, como irá compor o LDP, deve superar os demais requisitos indicados em sua especificação.

1.13.1.19.4.5. Esta Interconexão deverá utilizar apenas enlaces de fibra ótica em toda a sua extensão.

1.13.2. Link de Dados Secundário com o Provedor de Nuvem (LDS) - Item 8 da contratação

1.13.2.1. Deverá atender a todas as características e especificações do LDS, exceto as referentes à capacidade, uma vez que o LDS deverá ter a capacidade mínima de 1 Gbps (um gigabit por segundo).

1.13.2.2. Deverá atender aos seguintes requisitos especiais, por se tratar de conexão com objetivo de redundância e balanceamento de carga.

1.13.2.3. O PP deverá estar localizado em Estado da Federação diferente daquele utilizado para o LDP.

1.13.2.4. Para a LDC:

1.13.2.4.1. A operadora de telecomunicações deverá ser diferente daquela utilizada para implantar o LDP.

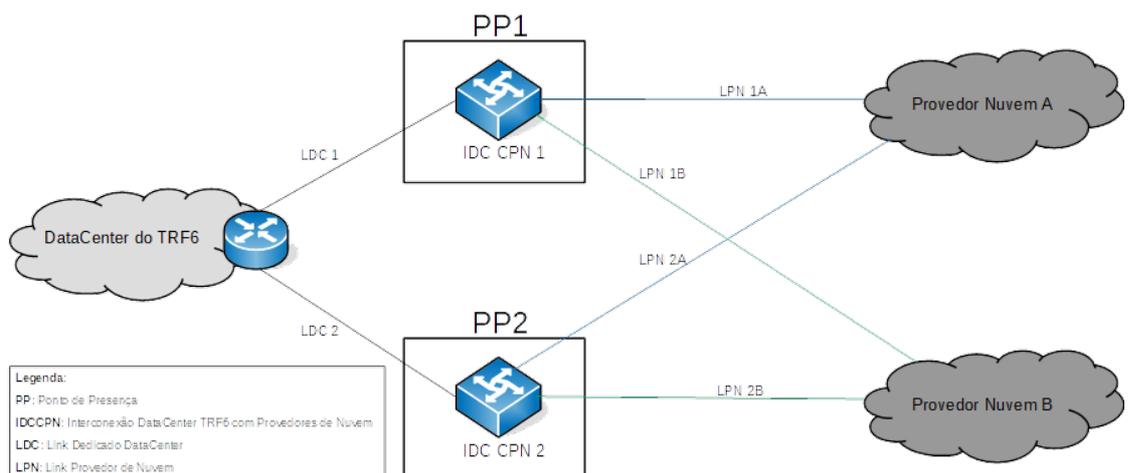
1.13.2.4.2. A operadora de telecomunicações não poderá compartilhar recursos com aquela contratada para implementar o LDP.

1.13.2.4.3. Os caminhos utilizados pelos cabos e enlaces, tanto externamente (ruas e quarteirões), quanto internamente ao prédio do centro de dados da CONTRATANTE, deverão ser completamente distintos daqueles utilizados no LDP.

1.13.3. A critério da CONTRATANTE, o LDP e o LDS poderão ser utilizados em modo de balanceamento de carga ou failover.

1.13.4. A CONTRATADA deverá realizar a implantação do LDP e do LDS em até 60 (sessenta) dias corridos após a emissão da Cotação de Serviço.

1.13.5. A figura abaixo representa a arquitetura de referência para os links de dados dedicados, onde o Link de Dados Primário (LDP) é composto pelos subcomponentes LDC 1, PP 1, LPN 1A, LPN 1B e IDCCPN1 e o Link de Dados Secundário (LDS) é composto pelos subcomponentes LDC 2, PP 2, LPN 2A, LPN 2B e IDCCPN2:



1.14. REQUISITOS DE SUPORTE TÉCNICO DO PROVEDOR

1.14.1. A solução deve incluir um suporte técnico do provedor contendo no mínimo as seguintes características:

1.14.1.1. O suporte técnico deve estar disponível para acionamento em regime 24x7, incluindo feriados e finais de se com quantidade ilimitada de acionamentos por meio telefone, e-mail ou sistema web próprio do provedor para contr chamados.

1.14.1.2. Não pode haver limites à adição de usuários para interagir com o suporte técnico.

1.14.1.3. O idioma do suporte técnico deve ser em português.

1.14.1.4. O tempo de resposta inicial do suporte técnico para falhas que causem indisponibilidade nos sistemas de pr deve ser de, no máximo, 1 (uma) hora para atendimento de acionamentos pelo CONTRATANTE.

1.14.1.5. Suporte diferenciado para 1 (um) evento programado, de curta duração, que exija excepcional ajust infraestrutura de nuvem do CONTRATANTE que exijam, por exemplo, maior desempenho computacional ou aumen capacidade de tráfego de dados.

1.14.1.6. Deve incluir serviço de gestão técnica de contas (*Technical Account Manager - TAM*), com um ou mais ge designados, que forneça monitoramento proativo e suporte reativo, auxiliando na otimização e orientando sobre p recomendadas, auxiliando também na otimização da carga de trabalho, custos e tratamento de eventos.

1.14.1.7. A CONTRATADA poderá registrar chamados junto ao provedor de nuvem, desde que devidamente autorizad CONTRATANTE.

1.14.1.8. O CONTRATANTE deverá possuir todos os acessos necessários de modo a manter a autonomia necessári registrar todo e qualquer tipo de chamado junto ao provedor de nuvem, independente do nível de prioridade.

1.14.1.9. O CONTRATANTE se reserva no direito de delegar a abertura, o acompanhamento e a validação da resoluçã chamados junto ao provedor de nuvem à CONTRATADA, acompanhando o fluxo da ocorrência, atuando de m supervisorar o andamento.

1.14.1.9.1. O fechamento de quaisquer ocorrências que tenham sido delegadas à CONTRATADA só poderá ocorre anuência do CONTRATANTE.

1.15. DOS NÍVEIS MÍNIMOS DE SERVIÇO EXIGIDOS (NMS)

1.15.1. A verificação da adequação da prestação do serviço deverá ser realizada com base em Níveis de Serviço definidos seção.

1.15.2. Níveis de serviço são indicadores mensuráveis, estabelecidos pelo CONTRATANTE, capazes de aferir objetivamer resultados pretendidos com a respectiva contratação.

1.15.3. A auditoria dos níveis de serviço será realizada mensalmente pelos fiscais do contrato, com base no relatório men serviço fornecido pela CONTRATADA referente ao mês anterior.

1.15.4. O não cumprimento dos valores mínimos/máximos exigidos nos indicadores ensejará na possível aplicação de m glosas previstas neste documento.

1.15.5. Para os serviços de computação em nuvem (Item 1 da contratação), serão considerados os seguintes indicadores:

1.15.5.1. INDICADOR DE DISPONIBILIDADE DOS SERVIÇOS DE COMPUTAÇÃO EM NUVEM (IDSCN)

Tabela 8 - Indicador de Disponibilidade dos Serviços de Computação em Nuvem (IDSCN)

INDICADOR DE DISPONIBILIDADE DOS SERVIÇOS DE COMPUTAÇÃO EM NUVEM (IDSCN)	
Tópico	Descrição
Finalidade	O IDSCN visa a aferir o percentual do tempo em que os serviços da Nuvem Pública estiveram disponíveis no mês.
Meta a cumprir	IDSCN >= 99,90% O serviço objeto desta contratação deverá ser prestado 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, durante todo o período de vigência do contrato, salvaguardados os casos de interrupções programadas.
Instrumento de medição	Através da plataforma de gerenciamento de nuvem e por controle próprio do CONTRATANTE na constatação de indisponibilidade dos serviços.
Forma de acompanhamento	Durante a execução dos serviços, a disponibilidade será monitorada e o tempo de indisponibilidade dos serviços serão descontados do tempo total de disponibilidade esperado no mês. Entende-se como serviços aqueles constantes dos catálogos do item 1 da contratação em execução.
Periodicidade	Aferida mensalmente por serviço
Mecanismo de Cálculo (métrica)	IDSCN (%) = (TDM / TTM) x 100 Onde: IDSPN = Disponibilidade dos Serviços TDM = Total de tempo com disponibilidade no mês TTM = Total do tempo no mês
Observações	Serão utilizados dias corridos na medição.
Início da Apuração	A partir da execução dos serviços previstos no Item 1 da contratação.

1.15.6. Para os serviços de gerenciamento e operação de recursos de computação em nuvem (Item 2 da contratação) considerados os seguintes indicadores:

1.15.6.1. INDICADOR DE RESPONSABILIDADE A INCIDENTES (IRI)

Tabela 9 - Indicador de Responsividade a Incidentes (IRI)

INDICADOR DE RESPONSABILIDADE A INCIDENTES (IRI)	
Tópico	Descrição
Finalidade	O indicador de resposta a incidentes mensura a quantidade de incidentes ocorridos no mês relacionados às instâncias objeto do contrato. O objetivo deste indicador é incentivar uma atuação proativa e preventiva no gerenciamento dos recursos.
Meta a cumprir	IRI >= 90% Promover uma resposta com proposta de resolução ou medida de contorno do incidente em até 90 (noventa) minutos.
Instrumento de medição	Através da plataforma de gerenciamento e acompanhamento de chamados e por controle próprio do CONTRATANTE
Forma de acompanhamento	Durante a execução dos serviços, a ocorrência de incidentes será monitorada e o tempo de resposta será contabilizado.
Periodicidade	Aferida mensalmente.

Mecanismo de Cálculo (métrica)	$IRI = (TI90 / TIM) \times 100$ Onde: IRI = Percentual de Incidentes Tratados em até 90 (noventa) minutos. TI90 = Total de incidentes tratados em até 90 (noventa) minutos. TIM = Total de incidentes ocorridos no mês.
Observações	Serão utilizados dias corridos na medição.
Início da Apuração	A partir da execução dos serviços previstos no Item 2 da contratação.

1.15.6.2. INDICADOR DE TEMPESTIVIDADE NA OPERAÇÃO (ITO)

Tabela 10 - Indicador de Tempestividade na Operação (ITO)

INDICADOR DE TEMPESTIVIDADE NA OPERAÇÃO (ITO)	
Tópico	Descrição
Finalidade	Mensurar a execução dos serviços de gerenciamento e operação nos prazos máximos estabelecidos.
Meta a cumprir	ITO \geq 90% Executar as operações e atividades dentro dos prazos para a execução previstos na tabela 2 e na ordem de sei
Instrumento de medição	Através da plataforma de gerenciamento e acompanhamento de chamados e por controle próprio do CONTRATANTE.
Forma de acompanhamento	Após a execução dos serviços, os fiscais analisarão individualmente cada execução de serviço verificando a conclusão no prazo definido neste documento.
Periodicidade	Aferida mensalmente.
Mecanismo de Cálculo (métrica)	$ITO = (TCSA / TC) \times 100$ Onde: ITO = Percentual de serviços entregues tempestivamente. TCSA = Total de chamados sem atraso. TC = Total de chamados ocorridos no mês.
Observações	Serão utilizados dias corridos na medição.
Início da Apuração	A partir da execução dos serviços previstos no Item 2 da contratação.

1.15.6.3. INDICADOR DE CONFORMIDADE NA OPERAÇÃO (ICO)

Tabela 11 - Indicador de Conformidade na Operação (ICO)

INDICADOR DE TEMPESTIVIDADE NA OPERAÇÃO (ITO)	
Tópico	Descrição
Finalidade	Assegurar que os serviços de operação e gerenciamento dos recursos em nuvem sejam executados em conformidade aos requisitos técnicos e funcionais esperados.
Meta a cumprir	ICO = 100% Executar as operações e atividades de gerenciamento para aferição da QUALIDADE dos serviços previstos na tabela 2 e na ordem de serviço.
Instrumento de medição	Através da plataforma de gerenciamento e acompanhamento de chamados e por controle próprio do CONTRATANTE.
Forma de acompanhamento	Após a execução dos serviços, os fiscais analisarão individualmente cada execução de serviço verificando a conformidade no prazo definido neste documento.
Periodicidade	Aferida mensalmente.
Mecanismo de Cálculo (métrica)	$ICO = (TCC / TC) \times 100$ Onde: ICO = Percentual de serviços entregues de acordo com os requisitos definidos neste documento. TCC = Total de chamados entregues de acordo com os requisitos definidos neste documento. TC = Total de chamados ocorridos no mês.
Observações	Serão utilizados dias corridos na medição.
Início da Apuração	A partir da execução dos serviços previstos no Item 2 da contratação.

1.15.7. Para os serviços relacionadas aos itens MIGRAÇÃO DE MÁQUINAS VIRTUAIS, MIGRAÇÃO DE MÁQUINAS VIRTUAIS VMV, MIGRAÇÃO DE BANCO DE DADOS (ITENS 3, 4 e 5 da contratação), serão considerados os seguintes indicadores:

1.15.7.1. INDICADOR DE TEMPESTIVIDADE NA MIGRAÇÃO (ITM)

Tabela 12 - Indicador de Tempestividade na Migração (ITM)

INDICADOR DE TEMPESTIVIDADE NA MIGRAÇÃO (ITM)	
Tópico	Descrição
Finalidade	Mensurar a execução dos serviços de migração nos prazos máximos estabelecidos.
Meta a cumprir	ITM = 0 Executar a migração das cargas de trabalhos dentro dos prazos para a execução previstos nos itens 3, 4 e 5.
Instrumento de medição	Relatório de execução.
Forma de acompanhamento	Após a execução dos serviços de migração, os fiscais verificarão a conformidade entre o prazo realizado e o prazo previsto.
Periodicidade	Aferida mensalmente.
Mecanismo de Cálculo (métrica)	$ITM = PR - PMP$ Onde: ITM = Dias de entrega do serviço dentro do prazo previsto. PR = Prazo realizado. PMP = Prazo Máximo previsto para migração.
Observações	Serão utilizados dias corridos na medição. O período cuja pendência dependa do CONTRATANTE será descontado da forma de cálculo.
Início da Apuração	A partir da execução dos serviços previstos nos itens 3, 4 e 5.

1.15.7.2. INDICADOR DE EFETIVIDADE NA MIGRAÇÃO (IFM)

Tabela 13 - Indicador de Efetividade na Migração (IFM)

INDICADOR DE EFETIVIDADE NA MIGRAÇÃO (IFM)	
Tópico	Descrição
Finalidade	Assegurar que a migração das cargas de trabalho ocorra em conformidade aos requisitos técnicos e de negócio esperados.

Meta a cumprir	IFM = 100%	Quantidade de instâncias migradas cujas cargas de trabalhos foram estabilizadas no ambiente de nuvem.
Instrumento de medição	Relatório de execução e plataforma de gerenciamento dos recursos de nuvem.	
Forma de acompanhamento	Após a execução dos serviços de migração, os fiscais verificarão a conformidade funcionais das cargas de trabalho mantidas instâncias.	
Periodicidade	Sob demanda	
Mecanismo de Cálculo (métrica)	IFM = TIMS / TIM x 100 Onde: IFM = Instâncias migradas em conformidade funcional aos requisitos técnicos e de negócio esperados. TIMS = Total de instâncias migradas em conformidade funcional. TIM = Total de instâncias migradas	
Observações	Serão consideradas instâncias de computação, máquinas virtuais VMware e instâncias de banco de dados.	
Início da Apuração	A partir da execução dos serviços previstos nos itens 3, 4 e 5.	

1.15.8. Para os serviços relacionados ao item TREINAMENTO (ITEM 6 da contratação), serão considerados os seguintes indica
1.15.8.1. INDICADOR DE QUALIDADE DO TREINAMENTO (IQT)

Tabela 14 - Indicador de Qualidade do Treinamento (IQT)

INDICADOR DE QUALIDADE DO TREINAMENTO (IQT)	
Tópico	Descrição
Finalidade	A execução dos serviços de treinamento com a qualidade mínima esperada.
Meta a cumprir	IQT >= 60% Avaliação positiva do treinamento por no mínimo 60% dos treinandos.
Instrumento de medição	Formulário de avaliação preenchido por cada treinando após realização do curso
Forma de acompanhamento	Ao término do treinamento cada aluno responderá um formulário com um indicador de avaliação geral do treinamento. Consi se positiva a avaliação superior a 60%.
Periodicidade	Por treinamento
Mecanismo de Cálculo (métrica)	$IQT (\%) = (TAP / TA) \times 100$ Onde: IQT = Índice de avaliações positivas sobre o treinamento. TA = Total de avaliações. TAP = Total de avaliações positivas
Observações	Serão considerados apenas os participantes com no mínimo 70% de frequência.
Início da Apuração	A partir da execução do serviço previsto no item 6.

1.15.9. Para os serviços relacionados aos itens de Link de Dados Dedicado (ITENS 7 e 8 da contratação), serão consider
seguintes indicadores:

1.15.9.1. INDICADOR DE DISPONIBILIDADE DO LINK DE DADOS

Tabela 15 - Indicador de Disponibilidade do Link de Dados (IDL D)

INDICADOR DE DISPONIBILIDADE DO LINK DE DADOS (IDL D)	
Tópico	Descrição
Finalidade	Avaliar a disponibilidade do link de dados
Meta a cumprir	IDL D >= 99,95% Disponibilidade apurada para o link de dados
Instrumento de medição	Relatório de disponibilidade para o link de dados dedicado.
Forma de acompanhamento	Após a entrega do serviço de fornecimento de link de dados, os fiscais verificarão a disponibilidade apurada para o período.
Periodicidade	Mensal
Mecanismo de Cálculo (métrica)	$D = (T0 - Ti) / T0 \times 100$ Onde: NC = Não conformidade D = disponibilidade; T0 = período de operação (1 mês), em minutos; Ti = tempo total de indisponibilidade do circuito de acesso ocorrida no período de operação (1 mês), em minutos. Caso a Disponibilidade seja maior ou igual a 98% e menor do que 99,95%: $NC = (100\% - Disponibilidade)$. Caso a Disponibilidade seja menor do que 98%: $NC = ((100\% - Disponibilidade) \times 2)$.
Observações	Será considerado o link de dados em uso no mês corrente.
Início da Apuração	A partir da autorização da execução do serviço previsto nos itens 7 e 8.

1.15.9.2. INDICADOR DE PERDA DE PACOTES DO LINK DE DADOS

Tabela 16 - Indicador de Perda de Pacotes do Link de Dados (IPPLD)

INDICADOR DE PERDA DE PACOTES DO LINK DE DADOS (IPPLD)	
Tópico	Descrição
Finalidade	Avaliar a latência do link de dados
Meta a cumprir	IPPLD <= 30ms Latência apurada para os pacotes de dados.
Instrumento de medição	Relatório de qualidade apurada para os pacotes de dados que trafegam no link dedicado.
Forma de acompanhamento	Após a entrega do serviço de fornecimento de link de dados, os fiscais verificarão a perda de pacotes apurada para o período.
Periodicidade	Mensal
Mecanismo de Cálculo (métrica)	<ul style="list-style-type: none"> Serão realizados testes de ping de 2 em 2 minutos, lançando 10 pings em cada teste. Cada ping deverá ser um pacote de 32 bytes encaminhado da infraestrutura do TRF6 até a infraestrutura da nuvem pública. Para efeito de cálculo, será considerada a perda de pacotes para os 2 minutos posteriores ao teste. A razão entre os pa que não tiveram respostas sobre a quantidade de pings, que, neste caso, são 10 (dez). Perda de Pacotes Mensal será a média de todos os resultados, ou seja, o somatório da razão de todos os testes sobre a quantidade de testes realizados no mês. <p>NC = Não conformidade Caso a Perda de Pacotes seja maior do que 0,5% e menor ou igual a 3%. NC = Perda de Pacotes. Caso a Perda de Pacotes seja maior do que 3%. NC = (Perda de Pacotes x 2).</p>

Observações	Será considerado o link de dados em uso no mês corrente.
Início da Apuração	A partir da autorização da execução do serviço previsto nos itens 7 e 8.

1.15.9.3. INDICADOR DE LATÊNCIA DO LINK DE DADOS

Tabela 17 - Indicador de Latência do Link de Dados (ILLD)

INDICADOR DE LATÊNCIA DO LINK DE DADOS (ILLD)	
Tópico	Descrição
Finalidade	Avaliar a qualidade do link de dados
Meta a cumprir	IPPLD \leq 0,5% Latência apurada para os pacotes de dados.
Instrumento de medição	Relatório de latência apurada para os pacotes de dados que trafegam no link dedicado.
Forma de acompanhamento	Após a entrega do serviço de fornecimento de link de dados, os fi scais verifi carão a latência apurada para o período.
Periodicidade	Mensal
Mecanismo de Cálculo (métrica)	<ul style="list-style-type: none"> Para efeito de contabilização da Latência, considera-se uma Avaliação de Latência como sendo um procedimento de te com pings realizado a cada 2 (dois) minutos, ao longo do período de medição mensal onde, em cada Avaliação de Latência, serão lançados 10 pings ping deverá ser um pacote de 32 bytes encaminhado da infraestrutura do TRF6 até à infraestrutura da nuvem pública. Para efeito de cálculo, será considerada a média do tempo de resposta dos 10 (dez) pings, ou seja, a Latência será o v; da razão entre o somatório dos tempos de resposta de todos os 10 (dez) pings sobre a quantidade de pings que, neste caso, são 10 (dez). O valor da Latência obtido para cada Avaliação de Latência, será enquadrada em três categorias: normal (menor ou igt 15 ms), alta (maior do que 15ms e menor ou igual do que 75 ms) e muito alta (maior do que 75 ms). A Latência do Mês será o somatório das Latências obtidas para cada uma das Avaliações de Latência ao longo de um n discriminada por categoria. Será tolerada que a Latência do Mês Alta seja menor ou igual a 20 minutos e a Latência do Mês Muito Alta seja menor (igual a 10 minutos. <p>NC = Não conformidade $NC = (Latência\ Alta \times 0,45 / Tempo\ Total\ do\ Mês) + (Somatório\ da\ Latência\ Muito\ Alta \times 0,9 / Tempo\ Total\ do\ Mês)$. Tolerância:</p> <ul style="list-style-type: none"> Será tolerado até 20 minutos por mês de Latência Alta Será tolerado até 10 minutos por mês de Latência Muito Alta. Para fins de Cálculo do NC só deverão ser considerados valores de Latência do Mês Anterior conforme índices: Alta superiores a 20 minutos e Muito Alta superiores a 10 minutos <p>Considerando: Tempo Total do Mês do Anterior: Quantidade de Dias do Mês Anterior * 24 horas * 60 minutos. Mês com: 30 dias = 43.200; 31 dias = 44.640.</p>
Observações	Será considerado o link de dados em uso no mês corrente.
Início da Apuração	A partir da autorização da execução do serviço previsto nos itens 7 e 8.

1.15.9.4. INDICADOR DE SUPORTE PARA LINK DE DADOS

Tabela 18 - Indicador de Suporte para Link de Dados (ISLD)

INDICADOR DE SUPORTE PARA LINK DE DADOS (ISLD)	
Tópico	Descrição
Finalidade	Avaliar a responsividade do suporte para o link de dados
Meta a cumprir	ISLD \leq 4 horas Atendimento dentro do prazo para suporte ao link de dados
Instrumento de medição	Relatório de SLA apurado para suporte do link dedicado.
Forma de acompanhamento	Tempo decorrido entre o pedido de suporte do CONTRATANTE e a resolução da solicitação de problema/questionamento.
Periodicidade	Sob demanda
Mecanismo de Cálculo (métrica)	Somatório das Horas Extrapoladas de cada solicitação que tenha ultrapassado o SLA. NC= Não conformidade $NC = 0,05\% \times Somatório\ das\ Horas\ Extrapoladas\ do\ Mês\ Anterior$.
Observações	Serão considerados os links de dados em uso no mês corrente.
Início da Apuração	A partir da autorização da execução do serviço previsto nos itens 7 e 8.

1.16. DOS REQUISITOS DE QUALIFICAÇÃO TÉCNICA

1.16.1. DA COMPROVAÇÃO DE ATENDIMENTOS AOS REQUISITOS TÉCNICOS

1.16.1.1. Para fins de demonstração da conformidade do serviço apresentado pela licitante em relação às especificações técnicas previstas neste documento, a LICITANTE deverá apresentar a seguinte Documentação Técnica:

1.16.1.1.1. A identificação dos provedores de nuvem ofertados e seus respectivos catálogos de serviços, associados aos serviços mínimos constantes dos catálogos do item 1 deste documento, conforme Anexo V - MODELO DE TABELA DE CONFORMIDADE TÉCNICA DOS CATÁLOGOS DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM;

1.16.1.1.2. A descrição de cada produto ofertado, incluindo os prospectos técnicos, referência ao endereço eletrônico do provedor e outros materiais necessários para se demonstrar a compatibilidade aos requisitos mínimos constantes dos serviços exigidos neste documento.

1.16.2. DA QUALIFICAÇÃO TÉCNICO-OPERACIONAL

- 1.16.2.1. A licitante deverá apresentar Atestado de Capacidade Técnica, expedido por pessoa jurídica de direito público ou privado, devidamente assinado do prestador ou órgão tomador do serviço, comprovando, no mínimo:
- 1.16.2.1.1. O provisionamento, gerenciamento e operação de, no mínimo, 200 instâncias de máquina virtual e instâncias de banco de dados em ambiente de nuvem pública;
 - 1.16.2.1.2. O fornecimento de painel ou portal web de gestão de recursos em nuvem pública capaz de real tempo de monitoramento e bilhetagem de recursos de computação em nuvem de um provedor;
 - 1.16.2.1.3. A realização de migração de ambiente de hospedagem próprio (*on-premises*) de organização pública ou privada com no mínimo 100 máquinas virtuais e de 10 instâncias de banco de dados para ambiente em nuvem pública.
- 1.16.2.2. Será permitido o somatório de atestados para fins de comprovação da qualificação técnica da licitante.
- 1.16.2.3. A Licitante deverá apresentar declaração dos PROVEDORES ofertados referente:
- 1.16.2.3.1. à capacidade de prover o escopo de serviços desta contratação.
 - 1.16.2.3.2. aos processos de recuperação de desastre, de gestão de continuidade de negócios e de gestão de mudanças, que garantam no mínimo:
 - 1.16.2.3.2.1. ter a capacidade de recuperar e de restaurar dados após incidentes de perda de dados;
 - 1.16.2.3.2.2. ter a capacidade de manter os mesmos níveis de segurança e de controles utilizados durante o modo de operação normal;
 - 1.16.2.3.2.3. garantir que a solução de recuperação de dados pertence e é gerenciada inteiramente pelo próprio provedor.
 - 1.16.2.3.3. às políticas e procedimentos para descarte de ativos de informação que garantam no mínimo:
 - 1.16.2.3.3.1. a sanitização ou a destruição segura de todos os dados existentes nos dispositivos descartados;
 - 1.16.2.3.3.2. a destruição segura de ativo em fim de ciclo de vida ou considerado inservível;
 - 1.16.2.3.3.3. o armazenamento seguro dos ativos a serem descartados.
- 1.16.2.4. A Documentação Técnica deverá ser encaminhada preferencialmente em formato digital.
- 1.16.2.5. Até a data de assinatura do contrato, a CONTRATADA deverá comprovar que os provedores constantes na proposta de prestação de serviço atendem ao menos as certificações: ABNT NBR ISO/IEC 27001:2013 (Segurança da Informação); ISO/IEC 27017:2016 (Segurança para Computação em Nuvem) ou CSA STAR Certification (Certificação independente de auditoria externa para provedores de computação em nuvem) LEVEL TWO ou superior ISO/IEC 27018:2014 (Proteção de Dados Pessoais em Nuvem), com validade durante a execução do contrato, referente à infraestrutura de datacenter onde os serviços em nuvem estarão hospedados.
- 1.16.2.5.1. As certificações de que tratam o item anterior poderão ser apresentadas na sua versão em inglês.

1.16.3. DA QUALIFICAÇÃO TÉCNICO- PROFISSIONAL

- 1.16.3.1. A CONTRATADA terá o prazo de 30 (trinta) dias corridos, a partir da emissão da Ordem de Serviço - OS, para a apresentação dos documentos comprobatórios da qualificação técnica dos profissionais;
- 1.16.3.2. Para aprovação dos profissionais da CONTRATADA, por parte do CONTRATANTE, a mesma deverá apresentar todos os documentos que comprovem o seu perfil;
- 1.16.3.3. O CONTRATANTE terá um prazo de até 05 (cinco) dias úteis para validar as documentações apresentadas, podendo solicitar a substituição do profissional que não atenda ao perfil mínimo indicado.

1.16.4. DA EXPERIÊNCIA PROFISSIONAL

- 1.16.4.1. A CONTRATADA deverá executar os serviços da presente contratação com ao menos os seguintes profissionais:
- 1.16.4.1.1. Administrador de Serviços de Nuvem
 - 1.16.4.1.1.1. Atribuições: Caberá ao Administrador de serviços de nuvem implementar, monitorar e manter as soluções em nuvem, incluindo os principais serviços relacionados a computação, armazenamento, rede e segurança.
 - 1.16.4.1.1.2. Experiência/Qualificação: Deverá ser comprovado experiência na operação/administração de serviços de computação em nuvem, podendo ser validado por meio de registro em carteira de trabalho ou contrato(s) executado(s) pelo profissional, atestados ou declarações, com a devida documentação necessária para que se comprove a participação do funcionário na execução das atividades.
 - 1.16.4.1.1.3. Formação: Curso superior completo na área de Tecnologia da Informação, ou qualquer outra formação de nível superior acrescida de especialização com no mínimo 360 horas na área de Tecnologia da Informação, devendo ser comprovado através de diploma, devidamente fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação - MEC.
 - 1.16.4.1.1.4. Certificação: O profissional deverá possuir certificação de Administrador de Soluções em Nuvem ou equivalente superior, relacionados ao provedor de nuvem adotado.
 - 1.16.4.1.2. Arquiteto de Nuvem
 - 1.16.4.1.2.1. Atribuições: Caberá ao Arquiteto de Soluções a análise e definição dos cenários apropriados para a execução dos procedimentos de configuração, migração/implantação, testes, colocação em produção e acompanhamento/monitoramento do serviço em produção.
 - 1.16.4.1.2.2. Experiência/Qualificação: Deverá ser comprovado experiência na elaboração e implementação de arquiteturas de serviços em computação em nuvem, podendo ser validado por meio de registro em carteira de trabalho, contrato(s) executado(s) pelo profissional, atestados ou declarações, com a devida documentação necessária para que se comprove a participação do funcionário na execução das atividades.
 - 1.16.4.1.2.3. Formação: Curso superior completo na área de Tecnologia da Informação, ou qualquer outra formação de nível superior acrescida de especialização com no mínimo 360 horas na área de Tecnologia da Informação, devendo ser comprovado através de diploma, devidamente fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação - MEC.
 - 1.16.4.1.2.4. Certificação: O profissional deverá possuir certificação de Arquiteto de Soluções em Nuvem ou equivalente superior, relacionados ao provedor de nuvem adotado.
 - 1.16.4.1.3. Especialista em Banco de Dados

1.16.4.1.3.1. Atribuições: Caberá ao especialista em banco de dados zelar pelo correto dimensionar arquitetura e operação das cargas de trabalho e recursos de computação associados aos bancos de utilizados pelas soluções e sistemas do CONTRATANTE.

1.16.4.1.3.2. Experiência/Qualificação: Deverá ser comprovado experiência na administração de banco de por meio de serviços de computação em nuvem, podendo ser validado por meio de registro em carteira trabalho, contrato(s) executado(s) pelo profissional, atestados ou declarações, com a devida documentação necessária para que se comprove a participação do funcionário na execução das atividades.

1.16.4.1.3.3. Formação: Curso superior completo na área de Tecnologia da Informação, ou qualquer outra formação de nível superior acrescido de especialização com no mínimo 360 horas na área de Tecnologia da Informação, devendo ser comprovado através de diploma, devidamente fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação - MEC.

1.16.4.1.3.4. Certificação: O profissional deverá possuir certificação de Administrador, engenheiro ou arquiteto de soluções, ou papel equivalente superior, relacionados ao provedor de nuvem adotado.

1.16.4.1.4. Especialista em Segurança da Informação

1.16.4.1.4.1. Atribuições: Caberá ao especialista em segurança da informação projetar, implementar, avaliar e recomendar, implantar e operar, do ponto de vista da segurança da informação, cargas de trabalho na nuvem, apoiando nas boas práticas de segurança da informação e tecnologias utilizadas pelos provedores, zelar pela confidencialidade, integridade e disponibilidade das informações, soluções e sistemas do CONTRATANTE.

1.16.4.1.4.2. Experiência/Qualificação: Deverá ser comprovado experiência na atuação na área de segurança da informação, com proteção de cargas de trabalho em nuvem, podendo ser validado por meio de registro em carteira trabalho, contrato(s) executado(s) pelo profissional, atestados ou declarações, com a devida documentação necessária para que se comprove a participação do funcionário na execução das atividades.

1.16.4.1.4.3. Formação: Curso superior completo na área de Tecnologia da Informação, ou qualquer outra formação de nível superior acrescido de especialização com no mínimo 360 horas na área de Tecnologia da Informação, devendo ser comprovado através de diploma, devidamente fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação - MEC.

1.16.4.1.4.4. Certificação: O profissional deverá possuir certificação de Especialista em Segurança da Informação, ou papel equivalente superior, relacionados ao provedor de nuvem adotado.

1.16.4.1.5. Instrutor de Serviços em Nuvem

1.16.4.1.5.1. Atribuições: Caberá ao instrutor ministrar os treinamentos previstos neste documento.

1.16.4.1.5.2. Experiência/Qualificação: Deverá ser comprovado experiência na realização de treinamentos corporativos e na operação de serviços em nuvem, podendo ser validado por meio de registro em carteira trabalho, contrato(s) executado(s) pelo profissional, atestados ou declarações, com a devida documentação necessária para que se comprove a participação do funcionário na execução das atividades.

1.16.4.1.5.3. Formação: Curso superior completo na área de Tecnologia da Informação, ou qualquer outra formação de nível superior acrescido de especialização com no mínimo 360 horas na área de Tecnologia da Informação, devendo ser comprovado através de diploma, devidamente fornecido por instituição de ensino superior reconhecido pelo Ministério da Educação - MEC.

1.16.4.1.5.4. Certificação: O profissional deverá possuir certificação de Administrador, Engenheiro ou Arquiteto de Soluções, ou papel equivalente superior, relacionados ao provedor de nuvem adotado.

1.16.4.2. Fica vedada a acumulação de perfis profissionais para um mesmo colaborador da CONTRATADA.

1.16.4.2.1. O perfil de instrutor poderá ser exercido por colaborador que atue como um dos outros perfis profissionais requeridos.

1.17. DA SUBCONTRATAÇÃO

1.17.1. A subcontratação de parcelas do objeto poderá ocorrer, considerando-se a sua especificidade e complexidade de execução, ou, em alguns casos, quando apresentarem grande simplicidade. Em ambos os casos, podem ser desempenhados por terceiros que isso acarrete prejuízos ao objeto contratado, sendo permitida apenas para serviços complementares ou acessórios, até o limite de 49% (quarenta e nove por cento).

1.17.2. A CONTRATADA não poderá, sob nenhum pretexto ou hipótese, subcontratar os itens principais do contrato, especialmente aqueles para os quais foram solicitados atestados de capacidade técnica operacional por ocasião da abertura do certame.

1.17.3. Será permitida a subcontratação dos serviços de link de dados MPLS.

1.17.4. Poderá a CONTRATADA solicitar a subcontratação de um serviço que não esteja acima relacionado, desde que justificado bem como analisado e aprovado previamente pelo CONTRATANTE. A não aprovação por parte da Administração do TRF6 em relação a uma subcontratação solicitada, de forma excepcional, não poderá ser utilizada como argumento para não execução de qualquer serviço.

1.17.5. Qualquer subcontratação deverá ser previamente aprovada pelo CONTRATANTE.

1.17.6. As empresas subcontratadas deverão preencher os requisitos de habilitação jurídica, fiscal, trabalhista, bem como incorrer em qualquer tipo de vedação imposta à participação em licitações.

1.17.7. A CONTRATADA será integralmente responsável pela totalidade da prestação dos serviços perante o CONTRATANTE podendo isentar-se, sob nenhuma escusa, da responsabilidade sobre os atos e omissões da empresa SUBCONTRATADA;

1.17.8. Caberá à CONTRATADA a gestão dos serviços da SUBCONTRATADA e a interação com o CONTRATANTE na definição e execução dos serviços, sem prejuízo da possibilidade de o CONTRATANTE exigir, eventualmente, contato direto com representantes da SUBCONTRATADA para melhor definição das alternativas e ações necessárias à prestação dos serviços;

1.17.9. Não será estabelecido qualquer vínculo entre o CONTRATANTE e a empresa SUBCONTRATADA, permanecendo a CONTRATADA responsável pelo integral cumprimento das obrigações pactuadas no contrato.

1.18. REQUISITOS DA CAPACITAÇÃO

1.18.1. Será realizado treinamento pela CONTRATADA destinado aos técnicos do CONTRATANTE, visando a capacitação em gerenciamento e no uso dos serviços disponíveis na plataforma de serviços da CONTRATADA, conforme requisitos estabelecidos neste documento.

1.18.2. Cada trilha da capacitação terá carga horária de, no mínimo, 30 horas, para uma turma de até 15 (quinze) pessoas.

1.18.2.1. O treinamento ocorrerá em dias úteis consecutivos, respeitando-se o calendário nacional e regional de feriados do CONTRATANTE.

1.18.3. O treinamento deverá ser ministrado, preferencialmente, no formato digital (on-line) e poderá ser acessado pelas p designadas pelo CONTRATANTE.

1.18.4. O treinamento realizado no formato digital deve estar gravado e ficar disponível durante todo o período do contrato.

1.18.5. O treinamento não poderá ser meramente expositivo. Deve contemplar também o uso prático da solução desenvolvimento de estudos de caso no ambiente da CONTRATADA voltados a simulação do conteúdo lecionado, comu conhecido como "laboratórios".

1.18.6. O treinamento deve ser apresentado em língua portuguesa. O material didático deve ser fornecido em formato digita todos os participantes com o conteúdo abordado pelo treinamento em língua portuguesa.

1.18.7. A CONTRATADA deverá emitir, ao final do treinamento, o certificado de conclusão para cada participante, no qual de constar, no mínimo, o nome do aluno, assunto, entidade promotora, carga horária, período de realização, ministrante e cor programático.

1.18.8. O instrutor responsável pela execução do treinamento deverá ter qualificação técnica-profissional compatível c exigências de qualificação técnica profissional, na seção de Instrutor de Serviços em Nuvem.

1.18.9. A CONTRATADA poderá incluir a participação de representantes técnicos dos provedores ofertados, incluindo o fornecii de conteúdo e recursos de treinamento, caso seja necessário.

1.18.10. Requisitos da qualidade dos serviços de treinamento

1.18.10.1. A validação de cada capacitação será realizada em até 05 (cinco) dias úteis decorridos do encerramentc treinamento(s), mediante a verificação do atendimento mínimo aos critérios de avaliação.

1.18.10.2. Não atendidos os critérios mínimos de satisfação exigidos, conforme tabela abaixo, a CONTRATADA deverá r dentro do prazo de vigência do contrato, o(s) treinamento(s) para a respectiva Capacitação, estando a empresa su aplicação de penalidades em caso de persistência na insatisfação da Capacitação.

Tabela 19 - Método para aferição do nível de satisfação da capacitação (AVALIAR GLOSA)

Indicador	Nível de Satisfação (NS)
Aferição	Pelo TRF6 em pesquisa de satisfação pós treinamento.
Forma de cálculo	NS = Q/T*100 Onde: NS = Nível de Satisfação; Q = Somatório dos pontos avaliados; T = Total máximo de pontos da pesquisa.
Nível mínimo de serviço exigido	NS Desejável: acima de 60% (sessenta por cento); NS Inaceitável: menor que 60% (sessenta por cento).
Sanções	NS Desejável: nenhuma; NS Inaceitável: Refazer o treinamento sem custos adicionais. Caso o NS seja Inaceitável por 02 (duas) vezes consecutivas, a CONTRATADA poderá sofrer a(s) as penalidade(s) prevista(s) e bem como o contrato poderá ser rescindido.

1.18.10.3. Para a realização da capacitação, serão responsabilidades da CONTRATADA:

- 1.18.10.3.1. Preparação do ambiente com registros para demonstrações e exercícios necessários às capacitações;
- 1.18.10.3.2. Fornecimento, antes do início de cada treinamento, do material didático, incluindo todo o cor programático dos treinamentos;
- 1.18.10.3.3. Fornecimento da lista de presença nominal com a identificação do curso e do período de aplicação, ord alfabeticamente pelo nome;
- 1.18.10.3.4. Assegurar o cumprimento do conteúdo programático do curso;
- 1.18.10.3.5. Fornecer, ao final do curso, o certificado de conclusão do curso aos servidores que tiverem compare pelo menos 80% (oitenta por cento) do tempo demandado, contendo, no mínimo, título do treinamento, conteúdo, horária, período da realização e identificação do treinando e da empresa;
- 1.18.10.3.6. Se durante o treinamento verificar-se o aproveitamento insatisfatório do(s) instrutor(es) da Contratada uso completo da solução, tal fato deverá ser comunicado à Contratada que deverá providenciar a substituição c profissional, no prazo máximo de 10 (dez) dias corridos após a solicitação.
- 1.18.10.3.7. Coordenar, acompanhar e supervisionar as atividades acadêmicas e operacionais do curso, garant atendimento aos requisitos de qualidade exigidos.

1.18.10.4. Para a realização das capacitações, serão responsabilidades do CONTRATANTE:

- 1.18.10.4.1. Fornecer os recursos de apoio necessários ao desenvolvimento dos cursos, tais como: acesso à equipamentos multimídia, flip-chart e quadro branco, no caso de treinamento na forma presencial;
- 1.18.10.4.2. Indicar os participantes do curso, juntamente com seus nomes completos e demais dados dos partici para emissão do certificado de conclusão;
- 1.18.10.4.3. Realizar a avaliação de reação de cada treinamento, por meio das características técnicas e níveis de s estabelecidos neste documento.

1.18.10.5. São requisitos exigidos da CONTRATADA com relação ao Padrão de Qualidade dos Serviços de Capacitação:

Tabela 20 - Padrão de Qualidade de Serviços de Capacitação

Variáveis	Indicadores	Nível de Satisfação (NS)
Instrutor	Domínio do assunto; Métodos didáticos; Clareza na exposição; Facilidade de comunicação e objetividade; Esclarecimento de dúvidas; Atenção e estímulo à participação do grupo; Administração de imprevistos; Foco na apresentação do tema; Administração do tempo previsto.	Mede o nível de satisfação dos treinandos. Caso o nível de satisfação dos treinandos não atinja 60% (sessenta por cento), o treinamento deverá ser refeito

Conteúdo do treinamento	Clareza e facilidade de compreensão; Balanceamento entre teoria e prática; Adequação do conteúdo à realidade do trabalho; Completude do Conteúdo; Facilidade de aplicação prática.	integralmente para aqueles que se manifestarem insatisfeitos. Deverá ter aferição de satisfação mesmo para o treinamento refeito.
Avaliação geral	Alcance das expectativas; Coerência entre o proposto e o realizado; Qualidade geral do curso.	

1.18.11. Do escopo de treinamento

1.18.11.1. A CONTRATADA deverá ministrar um curso de capacitação que habilite os servidores do CONTRATANTE administração de todos os serviços fornecidos pelo provedor de nuvem escolhido.

1.18.11.2. As trilhas elencadas abaixo deverão ser segmentadas pela CONTRATADA em cursos diferentes, com o intuito otimizar a participação dos servidores em seu respectivo ramo de atuação.

1.18.11.3. A CONTRATADA deverá abordar, no mínimo, os seguintes tópicos:

1.18.11.3.1. Administração da Nuvem

Tabela 21 - Escopo de treinamento de Administração da Nuvem

Tópico	Conteúdo
Gerenciamento de identidades	Administração de usuários e grupos; Administração de unidades administrativas; Configurar e gerenciar limitações de uso de recursos; Configurar reset self-service de senha; Configurar políticas de senha; Gerenciamento de usuários protegidos; Administração de perfis e políticas de acesso; Outros tópicos relevantes para o serviço fornecido pelo provedor de nuvem.
Gerenciamento de storages	Configurar acesso à rede para contas com acesso ao storage; Configurar e criar links de compartilhamento; Gerenciamento de chaves de acesso; Gerenciar e configurar replicação de objetos e backups; Apresentar os diferentes tipos de armazenamento do provedor; Configurar a integração de aplicações com o storage; Outros tópicos relevantes para o serviço fornecido pelo provedor de nuvem.
Deploy e gerenciamento de recursos computacionais	Configurar templates gerenciáveis de recursos computacionais; Criar, configurar e gerenciar VMs (Virtual Machines); Configurar VHD (Virtual Hard Disk); Realizando deploys a partir de templates; Configurar funcionalidade responsável por criptografar discos virtuais; Configurar e movimentar VMs (Virtual Machines) entre os grupos de recursos; Gerenciamento de tamanho das VMs e adição de data disks; Configurações avançadas de rede; Redeploy de VMs; Configuração de alta disponibilidade de VMs; Configuração de rede para Kubernetes; Configuração e dimensionamento de grupos para o serviço de Kubernetes ou equivalente; Implantar e configurar containers; Monitorar servidores on-premises e IaaS Virtual machines utilizando serviço de monitoramento do provedor de nuvem; Implantar política de failover cluster, em estrutura <i>on-premises</i> , híbridas ou nativamente cloud; Configuração e implementação de elasticidade rápida para os serviços do provedor; Utilizar console de gerenciamento e deploy fornecido pelo provedor; Outros tópicos relevantes para o serviço fornecido pelo provedor de nuvem.
Configuração e Gerenciamento de redes	Criar e configurar redes virtuais, incluindo <i>peering</i> ; Configurar endereços de IP privados e públicos; Configurações personalizadas de rotas de rede; Implantação e gerenciamento de subnets; Configuração e gerenciamento de endpoints privadas; Configuração do serviço de DNS do provedor, incluindo configurações personalizadas, sejam elas para zonas de DNS públicas ou privadas; Criação de regras de segurança; Associação de Grupos de Segurança de rede (NSG - Network Security Group) uma subnet ou interface de rede; Avaliar a efetividade do uso das regras de segurança; Implantação e gerenciamento do serviço de Firewall do provedor de nuvem; Configuração de acesso remoto protegido às máquinas virtuais, sem exposição de IPs públicos; Configuração de gateways de aplicativos do provedor de nuvem; Configurar um balanceador de carga interno ou público; Monitorar e configurar conectividade com a infraestrutura on-premises; Configuração de um monitor de rede, que verifique a conectividade das redes destinadas ao serviço; Depuração de problemas externos de rede; Depuração de conectividade de redes virtuais; Criar e configurar um serviço de gateway para VPN; Criar e otimizar rotas de acesso à rede; Configuração de redes WAN virtuais; Outros tópicos relevantes para o serviço fornecido pelo provedor de nuvem.

Backup e recuperação de dados	<p>Criar um serviço cofre de backups; Criar e configurar políticas de execução de backups; Ser capaz de realizar o backup e a restauração de serviços usando a ferramenta de backup fornecida pelo provedor de nuvem; Realizar recuperação site-to-site utilizando a ferramenta de backup do provedor de nuvem; Configurar e revisar relatórios de execução de backup; Realizar o backup e restauração de arquivos e pastas utilizando o serviço de recuperação de dados do provedor de nuvem; Instalar e gerenciar servidores de backup fornecidos pelo provedor de nuvem; Gerenciar os backups contidos no serviço de cofre para recuperação de dados; Recuperar máquinas virtuais utilizando snapshots temporários; Recuperar dados de uma VM e transferi-los para novas máquinas virtuais; Configurar políticas de site Recovery; Configurar planos de recuperação de dados; Implantar replicação de dados para um datacenter secundário, localizado na mesma região; Outros tópicos relevantes para o serviço fornecido pelo provedor de nuvem.</p>
Gerenciamento e monitoramento de recursos	<p>Configurar e interpretar métricas utilizadas pelos monitores de recursos do provedor de nuvem; Configurar o monitor de logs do provedor de nuvem; Demandar e analisar logs; Configurar alertas e ações com base nas informações do monitor do provedor de nuvem; Configurar e interpretar recomendações de otimização emitidas de forma automática pelo monitor de recursos do provedor de nuvem; Configuração de gerenciamento de custos do provedor de nuvem, assinatura de grupos de recursos [remanejado].</p>
Migração de servidores on-premises para nuvem	<p>Compartilhamento e transferência de dados; Utilização do Serviço de Migração de Dados para máquinas virtuais; Configurar e implantar um dispositivo de migrações para a estrutura do provedor de nuvem; Configurar e migrar <i>workloads</i> da VM para a IaaS do provedor; Configurar e migrar <i>workloads</i> físicos para a IaaS do provedor; Realizar a migração de todos os itens acima para containers, quando possível.</p>

1.18.11.3.2. Segurança da Informação

Tabela 22 – Escopo de Treinamento de Segurança da Informação

Tópico	Conteúdo
Resposta a incidentes	<p>Avaliar reports de uso abusivo nos serviços fornecidos pelo provedor; Identificar e avaliar uso indevido de instâncias computacionais; Isolar instâncias computacionais suspeitas para investigação do problema; Analisar logs de forma direcionada nas instâncias em que há fundada suspeita incluindo a coleta dos dados correspondentes; Capturar <i>dumps</i> de instâncias suspeitas para análise aprofundada para fins legais ou para análise forense; Determinar e avaliar configurações básicas de segurança que tenham sido alteradas recentemente; Avaliar as configurações dos serviços automatizados de alerta de incidentes de segurança; Automatizar todas as principais verificações de segurança disponíveis no provedor de nuvem, indicando os pontos de melhoria; Ser capaz de automatizar a criação, a verificação, o aumento da proteção, a manutenção e o gerenciamento de patches de imagens de contêiner; Recomendar soluções de segurança e gerenciamento de identidade mais utilizadas na nuvem, de modo a prevenir as falhas mais conhecidas.</p>
Ferramentas de Governança e Monitoramento	<p>Recomendar o uso dos recursos fornecidos pelo provedor de nuvem, dividindo hierarquicamente; Recomendar soluções que fortaleçam as ferramentas de auditoria e compliance; Recomendar soluções que armazenem senhas e chaves de segurança de forma segura; Descrever, analisar e gerenciar alertas e incidentes de segurança nas <i>workloads</i> do provedor de nuvem; Identificar, planejar e configurar solução de monitoramento que esteja disponível no provedor de nuvem, conectando-o, inclusive, a fontes de dados externas; Configurar e implantar regras de análise para ferramenta de monitoramento do provedor de nuvem; Realizar triagem de incidentes utilizando o serviço de monitoramento do provedor de nuvem; Configurar consultas e verificações de segurança agendadas de auditoria.</p>

Segurança de Infraestrutura	<p>Limitar ataques direcionados às workloads, identificando-os e limitando o período de ataque;</p> <p>Ser capaz de escolher serviços de segurança do provedor de nuvem ou de terceiros, que abranja, ao menos, serviços edge de WAF (Web Application Firewall), serviços de CDN (Content delivery network), serviços que automatizem a escolha da rota rápida para o serviço requisitado, proteção contra ataques DDoS, dentre outros;</p> <p>Avaliar e implantar mecanismos de prevenção e detecção de intrusão, validando relatórios apresentados pelas aplicações;</p> <p>Testar e depurar regras de WAF, assegurando que elas bloqueiam todo o tráfego indesejado;</p> <p>Ser capaz de avaliar e desabilitar quaisquer protocolos de rede e portas desnecessárias para o pleno funcionamento dos sistemas;</p> <p>Avaliar e implantar grupos de segurança que segmentem a rede, permitindo apenas os acessos estritamente necessários para o pleno funcionamento dos serviços;</p> <p>Avaliar e implantar o funcionamento de VPNs ou conexão via link dedicado, conforme o tipo de serviço fornecido pelo provedor de nuvem;</p> <p>Ser capaz de descrever a infraestrutura de nuvem, analisando o uso das sub-gateways para que estejam habilitadas de forma correta e segura;</p> <p>Ser capaz de identificar o motivo pelo qual um determinado tráfego de rede está sendo negado;</p> <p>Assegurar que a implantação de grupos de segurança e demais ACLs foram implantados de forma correta e segura;</p> <p>Ser capaz de decidir quando utilizar firewalls host-based, como iptables;</p> <p>Ser capaz de configurar controles de perímetro de rede;</p> <p>Ser capaz de configurar o balanceamento de carga (balanceadores de carga de rede, https, proxy SSL e proxy TCP);</p> <p>Ser capaz de avaliar as propriedades de segurança de uma rede VPC, incluindo peering de VPC, VPC compartilhada e regras de firewall.</p>
Políticas de Controle de Acesso	<p>Desenhar e implantar o gerenciamento e autorização de acesso aos recursos do provedor em nuvem, de modo individual e em grupos;</p> <p>Avaliar as workloads em uso na nuvem, analisando as configurações de nível de acesso e ajustando-as, quando necessário;</p> <p>Verificar o uso da conta do provedor de nuvem, avaliando possíveis riscos de exposição de senhas de administrador, dentre outros;</p> <p>Avaliar as configurações de políticas de segurança aplicadas para usuários, grupos e roles;</p> <p>Monitorar as políticas estabelecidas para assegurar que os usuários e sistemas estão acessando apenas o que é necessário para o desempenho de suas atribuições, sugerindo, quando necessário, a segmentação de tarefas.</p>
Proteção de Dados	<p>Desenhar e implantar o uso de chaves de segurança;</p> <p>Analisar e sugerir cenários onde o uso das chaves de segurança assegurará a confiabilidade dos dados;</p> <p>Ser capaz de avaliar e realizar o isolamento de falhas de segurança relacionadas a chaves de segurança, sugerindo e solucionando a falha identificada;</p> <p>Ser capaz de solucionar problemas gerais no gerenciamento das chaves de segurança;</p> <p>Assegurar que as diferentes políticas de segurança não estejam conflitantes com outras existentes;</p> <p>Realizar a revogação das permissões de um usuário ou serviço para conteúdo de falha, quando identificada;</p> <p>Desenhar e implementar a criptografia dos dados em repouso e dados <i>in transit</i>;</p> <p>Ser capaz de avaliar a tecnologia criptográfica mais aderente ao caso de uso;</p> <p>Ser capaz de determinar os requisitos regulamentares para a nuvem, incluindo limitação de computação e dados para conformidade regulatória;</p> <p>Avaliar o modelo de responsabilidade compartilhada de segurança;</p> <p>Configuração de controles de segurança em ambientes de nuvem que não foram abordados nos tópicos anteriores.</p>

2. DEMAIS REQUISITOS

2.1. REQUISITOS LEGAIS

O Projeto será executado em conformidade com:

- Lei nº 14.133, de 1º de abril de 2021, que a lei de licitações e contratos administrativos;
- Plano Estratégico de Tecnologia da Informação da Justiça Federal - PETI 2021/2026, aprovado pela Resolução CJF n. 685/2020;
- Resolução CNJ 370/2021, que estabelece a Estratégia Nacional de Tecnologia da Informação do Poder Judiciário (ENTIC-JUD) | período 2021/2026;
- Resolução CNJ 468/2022, que dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça;
- Lei nº 8.248, de 23 de outubro de 1991, regulada pelo Decreto nº 7.174/2010. Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União;
- Instrução Normativa ME 01/2019, que dispõe o processo de contratação de soluções de tecnologia da informação e comunicação em TIC;
- Instrução Normativa GSI 05/2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de serviços de computação em nuvem pelos órgãos e pelas entidades da administração pública federal;
- Decreto nº 10.024, de 20 de setembro de 2019, que regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências;
- Lei nº 10.520, de 17 de julho de 2002, regulada pelo Decreto nº 10.024, de 20 de setembro de 2019, que regulamenta o pregão na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências;
- Decreto nº 3.555/2000, que aprova o Regulamento para a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns.

2.2. DO SIGILO

2.2.1. São consideradas confidenciais informações ou dados armazenados a que a CONTRATADA tenha acesso, e também ac transmitidos oralmente, por escrito ou eletronicamente, em razão da execução deste objeto, independentemente de ex menção à sua confidencialidade.

2.2.2. A CONTRATADA, para fins de sigilo, se obriga por seus administradores, empregados, prepostos a qualquer título, suce e comissários.

2.2.3. A CONTRATADA deverá seguir os protocolos de segurança e envidará os melhores esforços para evitar backdc vulnerabilidades nos serviços objeto deste contrato. Na hipótese de vazamento de informações, a CONTRATADA se responsab por eventuais perdas e danos causados ao CONTRATANTE.

2.2.4. Sem prejuízo das disposições relativas à Segurança da Informação previstas neste documento, quaisquer inciden segurança, incluídos, mas não limitados aos ataques por hackers e/ou invasões de qualquer natureza e/ou vulnerabilidades té que exponham ou tenham o potencial de expor o ambiente onde se encontram hospedados informações e dados do TRF6, d ser imediatamente comunicados pela CONTRATADA ao CONTRATANTE, mesmo que se trate de meros indícios, guardando tod registros (inclusive logs, metadados e outras evidências dos incidentes e providências correspondentes) visando subsi realização de eventual auditoria.

2.2.5. Caso a CONTRATADA receba uma solicitação de acesso emitida por uma autoridade governamental, do Brasil ou do ex aos dados do TRF6 armazenados em decorrência da execução deste objeto, a CONTRATADA deverá dar ciência imedia CONTRATANTE, ressalvadas as hipóteses legais de sigilo na investigação e desde que expressamente exigido, por escrito autoridade.

2.2.6. A CONTRATADA envidará seus melhores esforços para questionar, administrativa ou judicialmente, às suas próprias exp solicitações de acesso por autoridades governamentais que não possuam inequívoco respaldo legal, antes de conceder o i requerido.

2.2.7. Caso a CONTRATADA seja subsidiária brasileira de empresa estrangeira para prestar os serviços deste documento, de CONTRATADA apresentar acordo de sigilo celebrado com a respectiva holding estrangeira, estabelecendo que as informaçã TRF6 armazenadas na subsidiária são confidenciais, não devendo ser compartilhadas com outras empresas do mesmo econômico, que não poderão possuir posse, custódia, controle ou acesso às referidas informações. Além disso, deve const referido acordo de sigilo, que a empresa subsidiária declare que exerce a atividade econômica substantiva, possuindo capa operacional apropriada para os seus fins, pela existência de força de trabalho, instalações físicas, equipamentos e recursos pr adequados para o exercício da prestação de serviços, gestão e efetiva tomada de decisões.

2.2.8. O descumprimento pela CONTRATADA da obrigação de sigilo, revelando informações e dados confidenciais ou facilitanc revelação, poderá ensejar na rescisão do contrato.

2.3. REQUISITOS TEMPORAIS

2.3.1. A tabela abaixo prevê os prazos para execução das etapas desde a assinatura do contrato, bem como estipula os prazo cumprimento das ações subsequentes.

Tabela 23 – Requisitos Temporais

ETAPA	DESCRIÇÃO	INÍCIO DA ATIVIDADE	CONCLUSÃO (PRAZO ESTIMADO)	ENTREGÁVEIS
ETAPA 1	Reunião Inicial	A partir da notificação para tal fim	10 (dez) dias úteis a partir da notificação para tal fim.	1. Reunião de Kickoff; 2. Apresentação do Preposto da empresa pelo representante legal da CONTRATADA; 3. Recebimento dos termos de compromisso e manutenção de sigilo; 4. Comprovação da qualificação técnico-profissional.
ETAPA 2	Definição da estratégia do uso dos recursos em multivem	A partir da conclusão da ETAPA 1	10 (dez) dias úteis a partir da conclusão da ETAPA 1	1. Criação de Business Case, devidamente assinado pelos responsáveis contendo, no mínimo: a) A identificação e características gerais do perfil das workloads do CONTRATANTE; b) O Business Case deverá conter um projeto de implantação estruturado; c) Análise dos benefícios técnicos relacionados ao perfil de demanda do CONTRATANTE; d) Cenários de adoção dos recursos dos diferentes provedores, incluindo demonstrativos e projeções de custos durante o ciclo de vida de cada servidor; e) Alinhamento junto ao CONTRATANTE de qual provedor aloca em cada provedor, considerando a discricionariedade; f) Análise de riscos relacionados a cada estratégia de utilização dos recursos em nuvem dos diferentes provedores.
ETAPA 3	Da execução dos serviços	A partir da conclusão da ETAPA 2	Durante a vigência do contrato	1. Alinhamento junto ao CONTRATANTE acerca da prioridade de migração das aplicações, contendo no mínimo, as seguintes atividades: a) Emissão da ordem de início da prestação do serviço, respeitando o prazo acordado para cada tipo de serviço; b) Início da execução do Projeto de Implantação; c) Reapontamento de aplicações dependente da entrega; d) Validação da entrega e testes no ambiente de produção. 2. Para os serviços elencados na Tabela 2, de observar os prazos específicos para cada tipo de serviço. 3. Após a entrega dos serviços de computação em nuvem, a CONTRATADA deverá providenciar a atualização do projeto da arquitetura dos servidores de modo que o CONTRATANTE tenha uma representação gráfica do ambiente em nuvem.

ETAPA 4	Fase de Encerramento dos Serviços	Até 90 (noventa) dias corridos antes do término do contrato.	Término de vigência contratual	1. Plano de Encerramento dos Serviços; 2. Plano de Gerenciamento de Riscos, Plano de Contingência e Plano de Acompanhamento do Encerramento; 3. Transferência de conhecimentos e bases de dados para o TRF6 e/ou nova contratada; 4. Devolução dos recursos disponibilizados pelo CONTRATANTE.
---------	-----------------------------------	--	--------------------------------	---

2.4. REQUISITOS SOCIAIS E CULTURAIS

2.4.1. A CONTRATADA deverá orientar sua equipe técnica sobre as boas práticas voltadas ao consumo consciente, reduzir o desperdício dos recursos naturais e coleta seletiva, inclusive à adequada destinação dos resíduos porventura gerados na execução do contrato, com o objetivo de contribuir para a preservação do meio ambiente, quando aplicável;

2.4.2. Os profissionais da CONTRATADA que desempenharão as atividades em contato direto junto ao CONTRATANTE, deverão cumprir os seguintes requisitos:

2.4.2.1. Apresentar-se vestidos de forma adequada ao ambiente de trabalho físico ou virtual, evitando vestuário que comprometa a imagem institucional do CONTRATANTE ou que ofenda o senso comum de moral e bons costumes;

2.4.2.2. Respeitar todos os servidores e demais colaboradores, em qualquer posição hierárquica, preservando a comunicação e o relacionamento interpessoal construtivo;

2.4.2.3. Atuar nas dependências do CONTRATANTE, se necessário, com urbanidade e cortesia.

2.4.3. A presente contratação também visa a:

2.4.3.1. Alcançar melhoria sociocultural no relacionamento dos usuários com os recursos tecnológicos atuais, mediante comunicação e maior transparência nas atividades desenvolvidas pela SECTI;

2.4.3.2. Possibilitar a modernização do TRF6 para um melhor atendimento jurisdicional com agilidade, eficiência e eficácia;

2.4.3.3. Prover maior celeridade na administração das demandas apresentadas ao TRF6, assim como a diminuição dos custos dos serviços prestados.

3. MODELO DE EXECUÇÃO DO CONTRATO

3.1. DA INICIALIZAÇÃO DOS SERVIÇOS

3.1.1. Da Reunião Inicial

3.1.1.1. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial alinhando o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos e esclarecer possíveis dúvidas acerca da execução dos serviços.

3.1.1.2. A reunião ocorrerá em até 10 (dez) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério do CONTRATANTE.

3.1.1.3. A pauta desta reunião observará, pelo menos:

3.1.1.3.1. Apresentação do Preposto da empresa pelo representante legal da CONTRATADA.

3.1.1.3.2. Recebimento dos termos de compromisso e manutenção de sigilo.

3.1.1.3.3. Recebimento das comprovações relacionadas aos perfis profissionais que serão utilizados pela CONTRATADA.

3.1.1.4. A Carta de Apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário designado para acompanhar a execução do contrato e atuar como interlocutor principal junto ao CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual.

3.1.2. Da definição da estratégia do uso dos recursos em multinuvem

3.1.2.1. O CONTRATANTE deverá disponibilizar, após a reunião inicial, informações sobre as expectativas do uso dos recursos de nuvem, características gerais das cargas de trabalho a serem migradas e eventuais limitações tecnológicas.

3.1.2.2. Em até 10 (dez) dias úteis após o recebimento das informações do subitem anterior, a CONTRATADA deverá apresentar, sem ônus adicional, um ou mais Business Cases, assinado pelo arquiteto de nuvem e pelo especialista em banco de dados da CONTRATADA alocados para o projeto, contendo no mínimo:

3.1.2.2.1. a identificação e características gerais do perfil de cargas de trabalho do CONTRATANTE;

3.1.2.2.2. a análise dos benefícios técnicos relacionados ao perfil de demanda do CONTRATANTE;

3.1.2.2.3. cenários de adoção dos recursos dos diferentes provedores incluindo demonstrativos e projeções de custos durante o ciclo de vida de cada serviço;

3.1.2.2.4. riscos relacionados a cada estratégia de utilização dos recursos em nuvem dos diferentes provedores.

3.1.2.3. O CONTRATANTE, baseando-se nas informações apresentadas pela CONTRATADA e OBSERVANDO A SUA ESTRATÉGIA de uso dos recursos de computação em nuvem, DECIDIRÁ qual a estratégia de utilização dos recursos em nuvem oferecidos pelos diferentes provedores.

3.1.2.4. A indicação dos recursos de cada provedor deverá ser feita pelo CONTRATANTE por meio dos mecanismos formais de comunicação constante do Termo de Referência.

3.2. DA EXECUÇÃO DOS SERVIÇOS

3.2.1. Da formalização da demanda

3.2.1.1. A formalização para início da prestação dos serviços deve ser realizada por meio de Ordem de Serviço (OS) - Anexo 1.

3.2.1.2. A Ordem de Serviço deve ser encaminhada pelo Gestor do Contrato contendo no mínimo:

3.2.1.2.1. a definição e a especificação dos serviços a serem realizados;

3.2.1.2.2. o volume estimado de serviços a serem realizados;

3.2.1.2.3. os prazos para realização dos serviços;

3.2.1.2.4. a identificação dos responsáveis do CONTRATANTE pelo acompanhamento dos serviços.

3.2.1.3. Para os serviços de computação em nuvem e de gerenciamento de nuvem (itens 1 e 2 da contratação), a Ordem de Serviço poderá conter parcelas mensais, limitadas à vigência do contrato, previstas a serem executadas, com o necessário:

- 3.2.1.3.1. a identificação do escopo de serviços abrangidos por cada parcela,
 - 3.2.1.3.2. o limite máximo de gastos admitido com cada parcela, incluindo neste cálculo limitações relacionadas à elasticidade de computação em nuvem.
 - 3.2.1.4. Cada parcela deve estar associada a uma entrega mensal e será tratada de forma individual para efeito de contabilização de níveis de serviço e avaliação dos produtos entregáveis.
 - 3.2.1.5. Com vistas a subsidiar a construção da ordem de serviço, o CONTRATANTE poderá solicitar a qualquer momento a elaboração de plano de arquitetura que deverá ser realizado conforme item de Planejamento dos Serviços (3.2.2).
 - 3.2.1.6. A elaboração de plano de arquitetura deve ser realizada sem ônus adicional ao CONTRATANTE.
- 3.2.2. Do Planejamento dos Serviços:
- 3.2.2.1. Para os serviços que necessitem da realização de um planejamento (itens 01 e 02 da contratação), a CONTRATADA deverá agendar reunião com o CONTRATANTE em até 1 (um) dia útil após a abertura do chamado ou recebimento da ordem de serviço, para tratar da demanda solicitada.
 - 3.2.2.2. Após explicada a demanda solicitada pelo CONTRATANTE, a CONTRATADA terá até 10 (dez) dias úteis para apresentar o plano de arquitetura de solução para implementação dos serviços demandados pelo CONTRATANTE.
 - 3.2.2.3. O prazo para apresentação do plano de arquitetura poderá ser ampliado a critério do CONTRATANTE.
 - 3.2.2.4. O plano de arquitetura deverá conter, no mínimo, as seguintes informações:
 - 3.2.2.4.1. Descrição detalhada do serviço demandado;
 - 3.2.2.4.2. Arquitetura proposta pela CONTRATADA para implementação do serviço demandado;
 - 3.2.2.4.3. Orçamento detalhado dos serviços que serão usados pelo provedor para implementação do serviço demandado com o preço efetivamente cobrado pela CONTRATADA;
 - 3.2.2.4.4. Prazo para entrega dos serviços em perfeita operação;
 - 3.2.2.4.5. Descrição detalhada de restrições, dependências e quaisquer informações relevantes acerca do plano proposto.
 - 3.2.2.5. Os planos de serviços devem ser supervisionados e assinados por profissional com o perfil de arquiteto de nuvem.
 - 3.2.2.6. Após entrega do plano de arquitetura, o CONTRATANTE realizará a análise de modo a verificar a aderência técnica ao negócio.
 - 3.2.2.7. Havendo divergência, o CONTRATANTE solicitará à CONTRATADA que promova as adequações e/ou correções no plano de arquitetura, sem revisão do prazo e sem reinício de contagem de prazo, salvo quando o CONTRATANTE identificar fato impeditivo.
 - 3.2.2.8. Após o aceite do plano de arquitetura, o CONTRATANTE analisará o plano e decidirá se os serviços demandados foram implementados.
- 3.2.3. Da abertura de chamados:
- 3.2.3.1. Durante a execução dos serviços, a CONTRATADA deverá usar a plataforma de gerenciamento de chamados do CONTRATANTE.
 - 3.2.3.2. Os chamados abertos somente podem ser concluídos e fechados após autorização do CONTRATANTE.

Os itens pretendidos são sustentáveis? Indicar a resposta expressamente para cada item (SIM ou NÃO).

Em caso de resposta **afirmativa** para um ou mais itens: indicar os critérios de sustentabilidade adotados para cada item.

Em caso de resposta **negativa** para um ou mais itens: justificar o afastamento dos critérios de sustentabilidade para cada item.

E.2.1. Quanto aos critérios ambientais, a CONTRATADA deverá cumprir os seguintes requisitos de uso racional de recursos:

E.2.1.1. Deverá entregar os documentos solicitados na forma digital, com vistas a evitar ou reduzir o uso de papel e impressão, e atendimento ao Art. 9º da Política Nacional de Resíduos Sólidos (Lei nº 12.305, de 2 de agosto de 2010);

E.2.1.2. As configurações de hardware e software deverão ser realizadas visando ao alto desempenho com a utilização racional de energia, evitando-se a sobrecarga de equipamentos ou dispositivos elétricos e eletrônicos;

E.2.1.3. Utilizar de forma eficiente o espaço de armazenamento virtual e oferecer o máximo de desempenho de processamento com menor impacto ou comprometimento da capacidade de processamento dos recursos tecnológicos do CONTRATANTE.

E.3. Critérios de acessibilidade

A Contratada deverá atender os requisitos determinados pela Lei de Cotas (Lei 8.213 de 24 de julho de 1991) que concerne Portador de Necessidades Especiais (PNE). Essa lei arrola em seu inciso I, II, III e IV, art. 93 - "A empresa com 100 (cem) ou mais empregados obrigada a preencher de 2% (dois por cento) a 5% (cinco por cento) dos seus cargos com beneficiários reabilitados ou pessoas portadoras de deficiência, habilitadas, na seguinte proporção: I - até 200 empregados 2%; II - de 201 a 500 - 3%; III - de 501 a 1.000 - 4%; IV de 1.001 em diante 5%".

E.4. Demonstração de que o mercado atende aos requisitos mínimos

Requisito	ID da Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade Administração Pública Federal?	Solução 1	X		
	Solução 2			
	Solução 3			
	Solução 4			
	Solução 5			
	Solução 6			
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			
	Solução 5			
	Solução 6			
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			
	Solução 5			
	Solução 6			
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			
	Solução 5			
	Solução 6			
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			
	Solução 5			
	Solução 6			
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			
	Solução 5			
	Solução 6			

F. Descrição da solução como um todo**F.1. Resultados pretendidos com a solução escolhida**

- Obter serviços de alta disponibilidade e com suporte prestados em regime de atendimento 24 x 7 (vinte e quatro horas, sete dias por semana);
- Reduzir a necessidade de investimento de grande vulto com a aquisição de equipamentos e suas respectivas substituições em períodos médios de 04 a 05 anos;
- Terceirizar custos operacionais e reduzir custos de infraestrutura e serviços de TI por meio de aplicações hospedadas em infraestrutura em nuvem;
- Reduzir custos de licenciamento de *softwares* utilizados pelo TRF6;
- Otimizar a produtividade da equipe de TI do TRF6, que passa a se dedicar à qualidade do serviço e ao suporte especializado;
- Ampliar os mecanismos de segurança da informação através de recursos como: retenção de dados; sistema de prevenção contra perda de dados; controle de acesso e gerenciamento de dispositivos, aplicativos e auditoria;
- Disponibilidade dos serviços em produção;
- Redução de custos de manutenção e melhor eficiência pelo uso racional dos recursos;
- Possibilitar o ajuste, sob demanda, da capacidade dessas aplicações, sistemas e serviços;
- Possibilitar, ainda, a disponibilização de novas aplicações, sistemas e serviços.
- Agilizar o processo de aquisição, de forma a garantir o estabelecimento da infraestrutura necessária o mais rápido possível e, ainda, a manutenção do parque tecnológico atualizado com menor esforço;
- Terceirização dos custos para fornecimento de energia, refrigeração, monitoramento, segurança física, prevenção e combate a incêndio;
- Redução da dependência de pessoal interno qualificado, permitindo que os servidores possam focar na gestão do poder computacional contratado;
- Modernização de acesso à rede de modo ubíquo, conveniente e sob demanda, utilizando recursos computacionais configuráveis.

F.2. Contratações correlatas e/ou interdependentes

Não se aplica.

F.3. Adequações do ambiente do órgão impostas pela solução escolhida

Não se aplica.

F.4. Descrição integral da solução

Contratação de Infraestrutura como Serviço (*Infrastructure as a Service - IaaS*) para atender às necessidades de funcionamento dos sistemas do Tribunal Regional Federal da 6ª Região e das subseções judiciárias pelo período de 30 (trinta meses).

G. Declaração de viabilidade

Com base nas informações levantadas ao longo deste estudo técnico, declaramos que a solução apresentada é viável de prosseguir e ser concretizada, pois é a que melhor atende os requisitos técnicos e funcionais pretendidos pela área demandante.

H. Nome e assinatura dos responsáveis pela elaboração e pela revisão, supervisão e controle de qualidade do ETP

Responsável pela elaboração: (*servidor da unidade requisitante*)

Heli Lopes Rios - Diretor da SUINF

Responsável pela revisão, supervisão e controle de qualidade: (*diretor*)

Daniel Santos Rodrigues - Diretor da SECTI

Integrante Administrativo:

Bruno Vieira de Souza - Analista Judiciário



Documento assinado eletronicamente por **Heli Lopes Rios, Diretor(a) de Subsecretaria**, em 22/05/2023, às 20:18, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Daniel Santos Rodrigues, Diretor(a) de Secretaria**, em 22/05/2023, às 20:19, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site https://sei.trf6.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0266910** e o código CRC **705C5AC3**.