

DIRETORIA DE LOGISTICA E GESTÃO DOCUMENTAL

Termo de Referência 107/2025

Informações Básicas

Número do artefato

UASG

Editado por

HUGO DO PRADO FELIX

Atualizado em

17/04/2026 16:06 (v 0.11)

107/2025

110792-DIRETORIA DE LOGISTICA E GESTÃO DOCUMENTAL

Status

ASSINADO

Outras informações

Categoria

VII - contratações de tecnologia da informação e de comunicação/Bens de TIC

Número da Contratação

00590.000832/2025-90

Processo Administrativo

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Registro de Preços para o fornecimento de Solução de Hiperconvergência para a ESAGU, incluindo a aquisição de hardware e softwares integrados e serviços necessários para garantir a gestão, segurança e escalabilidade da infraestrutura, além de serviços de instalação e implementação, pelo período de 12 (doze) meses, para atender as necessidades da Advocacia-Geral da União, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

GRUPO	ITEM	ESPECIFICAÇÃO	CATSER/ CATMAT	MÉTRICA OU UNIDADE DE MEDIDA	CÓD. PMC- TIC	QUANTIDADE	VALOR UNIT.	VALOR TOTAL
1	1	Appliance para Solução de Hiperconvergência	626070	UNIDADE	N/A	6	R\$ 1.895.918,92	R\$ 11.375.513,51
	2	Armazenamento Unificado de Arquivos e Objetos	476654	UNIDADE	N/A	1	R\$ 7.133.799,87	R\$ 7.133.799,87
	3	Instalação do Appliance para Solução de Hiperconvergência	27111	SERVIÇO	N/A	6	R\$ 23.886,12	R\$ 143.316,72
	4	Instalação do Armazenamento Unificado de Arquivos e Objetos	27111	SERVIÇO	N/A	1	R\$ 74.507,15	R\$ 74.507,15
VALOR TOTAL								R\$ 18.727.137,24

Classificação do objeto quanto à heterogeneidade ou complexidade

1.2. Os bens objetos desta contratação são caracterizados como comuns, uma vez que se enquadram na definição de bens e serviços comuns do inciso XIII do art. 6º da Lei nº 14.133/2021, cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado.

Classificação do objeto como bem de luxo

1.3. O objeto desta contratação não se enquadra como bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

Classificação do objeto quanto ao modelo de execução

1.4. O objeto desta contratação não possui natureza continuada, pois envolve o fornecimento e implantação de solução de hiperconvergência, incluindo instalação e configuração, cuja execução ocorrerá de forma pontual e conclusiva resultando na entrega e operacionalização dos equipamentos. Os serviços associados são considerados acessórios à aquisição, por serem necessários à plena utilização do bem principal, mantendo-se, assim, predominantemente de fornecimento com serviços continuados acessórios.

Prazo de vigência

1.5. O prazo de vigência da contratação é de 12 (doze) meses contados da data de assinatura do contrato, na forma do artigo 105 da Lei nº 14.133, de 2021.

1.6. A ata de registro de preços terá vigência de 1 (um) ano, podendo ser prorrogável por igual período, desde que comprovado o preço mais vantajoso, nos termos do art. 15 do Decreto nº 11.462/2023.

1.6.1. O quantitativo da ata de registro de preços poderá ser renovado quando da prorrogação da ata, nos termos do art. 84 da Lei nº 14.133/2021, do art. 22 do Decreto nº 11.462/2023, e consonante a NOTA JURÍDICA n. 00003/2024/CNLCA/CGU/AGU, devendo esta informação constar do Edital e da Ata de Registro de Preços.

1.7. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A presente contratação justifica-se por ser uma necessidade estratégica da Advocacia-Geral da União (AGU) a contratação de uma solução, a fim de prover infraestrutura física/virtual completa para Hospedagem de Portal da Escola Virtual da AGU (EVA) da Escola Superior da AGU (ESAGU).

2.2. Atualmente, a ESAGU conta com 587 cursos disponíveis em canal no YouTube, contendo cerca de 4.953 vídeos, totalizando cerca de 445.770 minutos e 22,16TB, além de perspectiva de crescimento. Esses cursos não atendem apenas à AGU, mas também servidores de diversos órgãos e cidadãos brasileiros, contribuindo para a disseminação de conhecimento em nível nacional. Isso demonstra a importância estratégica no investimento de uma solução que hospede o Portal da Escola, garantindo escalabilidade, instâncias dedicadas ao seu Moodle, que auxiliem as experiências de ensino-aprendizagem, com garantia de armazenamento, disponibilidade e segurança.

2.3. O público-alvo estimado abrange aproximadamente 15.000 (quinze mil) membros das carreiras jurídicas, servidores administrativos da AGU, parceiros institucionais distribuídos nacionalmente e cidadãos. Para cumprir adequadamente sua função enquanto Escola de Governo, a ESAGU necessita investir em instrumentos que possibilitem ampliar o alcance das ações de desenvolvimento, atendendo simultaneamente grande número de usuários, democratizando o acesso ao conhecimento e observando os princípios da eficiência e sustentabilidade.

2.4. Nesse contexto, as ferramentas de ensino a distância são essenciais para permitir o avanço das instituições, impulsionadas pela popularização da internet e pela crescente necessidade de flexibilização nas formas de ensino e de aprendizado. Esse modelo EaD tem se consolidado globalmente, atendendo a diferentes perfis de estudantes e contextos de aprendizagem, inclusive, o corporativo.

2.5. Atenta a esse cenário, a ESAGU vem, desde 2021, estruturando-se para ofertar cursos nessa modalidade, tendo desenvolvido internamente a Escola Virtual da AGU (EVA), baseada na plataforma Moodle.

2.6. Desde sua implementação, em 2022, a EVA tem hospedado centenas de ações de desenvolvimento, incluindo os Cursos de Pós-Graduação Lato Sensu da ESAGU, ofertados integralmente em EaD. Todavia, apesar dos esforços internos, a unidade tem conseguido atender apenas de forma limitada às demandas de capacitação da AGU, devido a restrições técnicas que dificultam a evolução da estrutura e do funcionamento da plataforma.

2.7. Um exemplo de limitação do EaD da ESAGU é que atualmente as transmissões ao vivo e as aulas gravadas dos cursos ocorrem e ficam hospedadas na plataforma externa, o YouTube, sendo ele o atual servidor de mídia da ESAGU, o que fragiliza a segurança, além de inviabilizar o controle pormenorizado por parte da ESAGU no que diz

respeito aos acessos e visualização das videoaulas. Assim, o acompanhamento dos discentes fica prejudicado, para não dizer inviável.

2.8. Embora o YouTube seja plataforma de hospedagem e streaming, seu foco é a divulgação ampla de conteúdo audiovisual, não oferecendo funcionalidades de interatividade, controle, personalização ou integração pedagógica essenciais ao adequado desenvolvimento do processo de ensino-aprendizagem.

2.9. Além dessas limitações, outros fatores tornam urgente a adoção de melhorias estruturais na EVA, destacando-se:

- a) aumento significativo das demandas por capacitação EaD ou híbrida no âmbito da AGU;
- b) interesse da alta administração em permitir acesso contínuo de servidores públicos federais à plataforma;
- c) necessidade de aprimorar a organização das informações e a gestão discente, diante do elevado volume de conteúdo disponível;
- d) necessidade de aplicar design instrucional e modelos pedagógicos adequados, superando o atual uso de recursos básicos (vídeos e apostilas sem estrutura instrucional);
- e) necessidade de provimento de armazenamento em nuvem e servidor de mídia, frente às limitações da plataforma externa atualmente utilizada;
- f) necessidade de criação de turmas com datas de início e fim, sem duplicação indevida de conteúdos, o que requer mecanismo de Rede de Entrega de Conteúdo (CDN);
- g) necessidade de aprimoramento da configuração da plataforma, com catálogo de cursos, interfaces adequadas e criação de secretaria escolar digital para disponibilização de cursos, notas, históricos e certificados;
- h) necessidade de implementação e/ou revisão de políticas de segurança da informação;
- i) necessidade de ampliar e qualificar o atendimento ao usuário, especialmente diante da expansão prevista.

2.10. Do ponto de vista técnico, a nova infraestrutura deve consolidar recursos de processamento, armazenamento e virtualização, simplificando a gestão e elevando a disponibilidade do ambiente que sustenta o Portal EVA. A solução deve reduzir a complexidade decorrente da atual estrutura fragmentada, acelerar o provisionamento e padronizar políticas de segurança e conformidade, assegurando qualidade de serviço ao crescente número de usuários.

2.11. Quanto à escalabilidade, a solução deve permitir expansão de capacidade sem interrupção dos serviços. Para o Moodle e componentes adjacentes (banco de dados, cache, balanceadores, multimídia), elevada conectividade leste-oeste é essencial para mitigar latência e aprimorar a experiência dos usuários.

2.12. A alta disponibilidade deve ser intrínseca ao desenho que atenda as necessidades da ESAGU e com política de proteção adequada, possibilitando tolerância a falhas. A solução deve evitar janelas de indisponibilidade. Também são necessárias tecnologias para manter o desempenho e a resiliência frente a incidentes.

2.13. A solução de armazenamento deve garantir performance, segurança e flexibilidade, habilitando os principais casos de uso do Portal (bancos de dados, repositórios de curso, mídia e relatórios). É necessário suportar os formatos habituais de consumo de dados (blocos, arquivos e objetos), além de manter espaço local para preparação de conteúdos (staging), transcoding, cópias de preservação e eventuais migrações, considerando o volume atual e seu crescimento previsto.

2.14. Quanto à conectividade, deve assegurar acesso contínuo, rápido e confiável ao Portal, com redundância para evitar interrupções e com isolamento lógico entre ambientes (aplicação, dados e administração). A integração com mecanismos de distribuição e proteção de tráfego deve contribuir para manter a qualidade de serviço mesmo em picos de demanda.

2.15. A solução também precisa aderir à LGPD e às diretrizes de segurança do setor público, com controles de acesso por função, autenticação forte, registros de auditoria e criptografia de dados. Backups imutáveis e políticas de retenção compatíveis com requisitos legais e acadêmicos, acompanhados de testes regulares de restauração, reduzem riscos operacionais e reputacionais.

2.16. É recomendável, ainda, operar tudo por um console unificado, com visibilidade de capacidade, uso e tendências, suporte à detecção de anomalias e apoio a decisões de otimização de custos. Processos de atualização coordenados e automação para reduzir esforço operacional, acelerar provisionamento e dirimir risco de erros.

2.17. Para preservar a competitividade e evitar dependência tecnológica, a solução deve ser compatível com os principais hipervisores e oferecer trajetória clara de evolução. Os critérios de contratação devem ser objetivos, considerando métricas de desempenho, eficiência de dados e níveis de serviço.

2.18. A configuração inicial deve assegurar desempenho adequado para as cargas do Portal, com margem para crescimento e sem restrições de licenciamento atreladas à capacidade adquirida. A expansão deve ser modular e previsível, sem impacto aos usuários.

2.19. A infraestrutura atual da ESAGU baseia-se em arquitetura tradicional de três camadas (servidores, SAN e storage dedicado), a qual tem se mostrado inadequada frente às demandas crescentes devido à complexidade, à fragmentação e à rigidez desse modelo. Tais limitações comprometem a escalabilidade, dificultam a automação e reduzem a capacidade de resposta a falhas.

2.20. Diante da relevância da ESAGU para a AGU, órgãos parceiros, Poder Judiciário e cidadãos, faz-se necessária solução tecnológica que evolua em capacidade e serviços, ampliando o valor entregue à sociedade.

2.21. Em relação ao suporte, deve ser adotado modelo compatível com a criticidade do Portal, incluindo atendimento 24x7 para incidentes graves, documentação, apoio à migração e validação pós-implantação, com testes de desempenho e resiliência.

2.22. Por fim, a solução deve contribuir para reduzir complexidade, otimizar o uso de recursos e conferir previsibilidade de custos ao longo do ciclo de vida, alinhando investimentos ao crescimento real da demanda e ao impacto social das ações educacionais da AGU.

Justificativa para a utilização de Sistema de Registro de Preços (SRP)

2.23. A solução a ser contratada visa atender a todas as unidades da AGU, garantindo a continuidade operacional da infraestrutura da AGU, preservando o mesmo formato, padrão arquitetural e modelo de operação já consolidado. A escolha por esse modelo assegura total compatibilidade com os ambientes e processos atualmente em produção, mitigando riscos relacionados à interoperabilidade, tempo de adaptação e eventuais indisponibilidades. O modelo de consumo é mais flexível, com opções de escalabilidade conforme demanda, evitando superdimensionamento, o que justifica a adoção do Sistema de Registro de Preços (SRP) para assegurar a flexibilidade na contratação.

2.24. Assim, a adoção do Sistema de Registro de Preços é justificada com base no art. 3º, inciso II, do Decreto nº 11.462/2023, que menciona o cabimento de registro de preços quando for conveniente a aquisição de bens com previsão de entregas parceladas. O SRP permite a formalização de Ata de Registro de Preços (ARP) sem a obrigatoriedade de contratação imediata da totalidade dos quantitativos estimados, possibilitando a realização de contratações futuras e sob demanda.

2.25. A equipe técnica realizou levantamento quanto à existência de Atas de Registro de Preços vigentes com objeto e modelagem compatíveis com a presente demanda, não tendo sido identificadas soluções aptas a atender às necessidades institucionais da AGU. Constatou-se que as atas analisadas apresentam divergências tecnológicas relevantes, incompatíveis com os requisitos técnicos estabelecidos, inviabilizando sua utilização como alternativa válida à contratação pretendida na forma registrada no Estudo Técnico Preliminar.

Justifica de não realização do procedimento de Intenção de Registro de Preços

2.26. O Sistema de Registro de Preços visa atender a necessidade de contratação de Solução de Hiperconvergência para atender as demandas específicas dos usuários da AGU, conforme requisitos e justificativas registradas no Estudo Técnico e no processo relacionado. Assim, a solução foi projetada para atender a demanda específica da AGU. Nesse contexto, entende-se pela não divulgação de Intenção de Registro de Preços (IRP) para participação de órgãos ou entidades externas, nos termos do art. 9º, § 2º, do Decreto nº 11.462/2023, considerando, sobretudo, a limitação de capacidade operacional para gerenciamento de uma ata compartilhada, bem como os riscos associados à ampliação do escopo da pretensa contratação.

2.27. A eventual adesão de múltiplos órgãos poderia acarretar aumento da complexidade administrativa, dificultando o controle da execução, o acompanhamento das demandas e a gestão dos quantitativos registrados, além de potencialmente impactar o planejamento originalmente estabelecido para atendimento das necessidades institucionais. Ademais, essa ampliação poderia gerar riscos à eficiência, à governança e à segurança do processo de contratação, especialmente em razão da natureza técnica e integrada da solução pretendida.

Utilização por órgão não participante

2.28. Diante do contexto apresentado, não será admitida a adesão de órgãos ou entidades não participantes à Ata de Registro de Preços (ARP), uma vez que a permissão implicaria aumento da complexidade operacional e administrativa, com potenciais impactos na gestão da ata, no controle dos quantitativos e na execução contratual. Nesse sentido, a vedação à adesão mostra-se necessária para preservar a aderência ao planejamento institucional, assegurar a adequada execução do objeto e mitigar riscos operacionais, garantindo o atendimento prioritário às demandas da instituição.

Parcelamento da Solução de TIC

2.29. O parcelamento não se mostra técnica e economicamente viável, visto tratar-se de uma única solução, que engloba a aquisição dos equipamentos e os serviços de instalação, configuração e garantia, os quais possuem alto grau de dependência entre si, sendo a instalação e configuração condições indispensáveis ao correto funcionamento do equipamento e da garantia contratada, mostrando-se inviável o parcelamento da contratação em itens separados, o que poderia comprometer tecnicamente o conjunto da solução.

2.30. Os itens que fazem parte do objeto da contratação são dependentes tecnicamente entre si. Logo, o parcelamento da aquisição em itens distintos comprometeria o conjunto da solução por separar fornecimento e serviços com alto grau de interdependência. Diante disso, fica assegurado o interesse público e justifica-se a inviabilidade do parcelamento do objeto conforme o inciso II do parágrafo 3º do art. 40 da lei nº 14.133/21 e a súmula nº 247 do TCU.

Resultados e Benefícios a Serem Alcançados

2.31. Os benefícios esperados com a contratação, são os seguintes:

- a) Alta disponibilidade contínua: tolerância a falhas de nós/discos e atualizações sem janelas, mantendo o EVA acessível sem interrupções significativas;
- b) Desempenho de baixa latência: SSDs NVMe, data locality e tráfego lesteoeste otimizado, que reduzirão tempos de resposta do Moodle, bancos e mídia e trarão maior estabilidade;
- c) Escalabilidade previsível e modular: crescimento linear por nó ("payasyougrow"), evitando superprovisionamento e alinhando recursos ao aumento de cursos, vídeos e acessos simultâneos;
- d) Simplificação operacional: console único, LCM coordenado e automação que diminuirão complexidade, esforço de gestão e erros operacionais, além de reduzir também o tempo de resolução de problemas;
- e) Serviços de dados integrados: thin provisioning, deduplicação, compressão, snapshots e clones eficientes serão utilizados para elevar a eficiência do armazenamento e acelerar cópias/migrações;
- f) Multiprotocolos no mesmo domínio: bloco, arquivo e objeto (iSCSI/NFS/SMB/S3 com WORM) atenderão bancos, repositórios, mídia/transcoding e relatórios sem gateways extras;
- g) Segurança de ponta a ponta: microsegmentação distribuída, RBAC, MFA, criptografia em trânsito/repouso, trilhas de auditoria e integração com SIEM/SOAR, trazendo conformidade com a LGPD e demais normas e orientações do serviço público;
- h) Resiliência e continuidade acadêmica: replicação síncrona/assíncrona, runbooks e testes de recuperação de desastres sem impacto, de modo a confluir para a restauração de serviços definidos para workloads críticos (principalmente o Moodle);

- i) Observabilidade fullstack: métricas, logs e traces correlacionados por máquina virtual/volume/rede sustentam métricas de experiência mais precisas, alertas acionáveis e resolução mais rápida de incidentes;
- j) Melhor qualidade de gastos e previsibilidade de custos: consolidação de contratos/licenças, menor consumo de energia/espço e menos integrações reduzindo chance de custos não previstos.

2.32. O objeto da contratação está previsto no Plano de Contratações Anual 2026, conforme detalhamento a seguir:

- 2.30.1. ID PCA no PNCP: 26994558000123-0-000007/2026
- 2.30.2. Data de publicação no PNCP: 22/05/2025
- 2.30.3. Id do item no PCA:
- 2.30.4. Classe/Grupo:
- 2.30.5. Identificador da Futura Contratação:

2.33. O objeto da contratação também está alinhado com a Estratégia de Governo Digital 2024-2027 (Decreto 12.069 /2024 e Portaria SGD/MGI 4.248/2024) e em consonância ao Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC (2024-2025) da AGU, conforme demonstrado abaixo:

PLANO ESTRATÉGICO 2024-2027 (Resolução CG-AGU nº 14/2024)	
Perspectiva	Objetivo Estratégico
Excelência dos Serviços Jurídicos	2. Aumentar a proteção do patrimônio e a recuperação de recursos públicos
Processos de Trabalho	4. Ampliar a capacidade de governança e gestão de riscos
Aprendizagem e crescimento sustentável	6. Promover a transformação digital inclusiva
	7. Incorporar práticas sustentáveis na gestão de recursos

Estratégia de Governo Digital 2024-2027 (Decreto 12.069/2024 e Portaria SGD/MGI 4.248/2024)	
Objetivos Gerais (Art. 8º)	Objetivos Específicos (Art. 9º)
I - da oferta de soluções que atendam às necessidades da sociedade e reconheçam as desigualdades sociais e as barreiras de acesso aos serviços públicos; II - da adaptação de seus processos às demandas atuais da sociedade, com inovação, uso adequado de tecnologias, reuso seguro de dados e melhor aplicação dos recursos públicos; e III - da transparência, do acesso à informação, da participação social na formulação de políticas públicas e da promoção do desenvolvimento sustentável.	I - qualificar a gestão e a governança das políticas de governo digital, de modo a promover a colaboração entre a União, os Estados, o Distrito Federal e os Municípios; IV - ampliar a resiliência e a maturidade das estruturas tecnológicas governamentais, com atenção à privacidade, à proteção de dados pessoais, à segurança da informação e à segurança cibernética; V - qualificar a tomada de decisões e a oferta de serviços nas organizações públicas com o reuso constante e ético dos dados disponíveis para análises, interoperabilidade e personalização; VI - dispor de infraestrutura moderna, segura, escalável e robusta, considerados os princípios de sustentabilidade, para a implantação e a evolução de soluções de governo digital, de modo a promover soluções estruturantes compartilhadas, o uso de padrões comuns e a integração entre os entes federativos; VII - estimular e promover o desenvolvimento do ecossistema de inovação e o uso de tecnologias emergentes de governo digital, com a participação dos entes federativos e da sociedade.

PDTIC 2023-2025 (Resolução CG-AGU nº 11/2023)			
Perspectiva	Eixo	Objetivo Estratégico (OE)	Iniciativa Estratégica (IE)
	Arquitetura	O.04 - Aprimorar a arquitetura de sistemas	IE.01 - Avaliar, promover e implantar tecnologias inovadoras
			IE.03 - Aprimorar a infraestrutura de TI das unidades da AGU

Qualidade em Tecnologia da Informação	Infraestrutura	O.05 - Garantir a infraestrutura de TI apropriadas às necessidades da AGU	IE07 - Aprimorar a segurança da infraestrutura de TI
			IE09 - Definir solução de nuvem corporativa
	Soluções	O.06 - Expandir e aperfeiçoar soluções corporativas	IE10 - Prover soluções de TI par atendimento às necessidades da AGU
			IE11 - Aprimorar o portfólio de serviços do DTI

2.34. Além disso, o objeto desta contratação está em conformidade com as diretrizes estabelecidas no Plano Diretor de Logística Sustentável (PDLS) da Advocacia-Geral da União (AGU), conforme disposto na Portaria SGA nº 690 /2025, elaborada em conformidade com a Portaria SEGES/MGI nº 5.376/202. Os requisitos definidos contribuem para o alcance dos objetivos estratégicos da AGU, incorporando critérios que contemplam as dimensões econômica, social, ambiental e cultural, em consonância com os instrumentos de planejamento estratégico da instituição.

2.35. Nesse contexto, a tabela a seguir decorre das diretrizes consideradas e eixos aplicáveis para a contratação pretendida:

ALINHAMENTO AO PLANO DIRETOR DE LOGÍSTICA SUSTENTÁVEL - PDLS 2025-2027 (PORTARIA SGA Nº 690, DE 16 DE JUNHO DE 2025)			
DIRETRIZES ESTRATÉGICAS			
Nº 2 – Promover a transformação digital inclusiva.			
Nº 4 – Ampliar a capacidade de governança e gestão de riscos.			
Nº 6 – Adesão a padrões nacionais e internacionais de sustentabilidade.			
Nº 11 – Contratações alinhadas ao PCA, à modernização e à inovação.			
Nº 12 – Aprimoramento da integração com o mercado fornecedor.			
EIXOS APLICÁVEIS	PROBLEMÁTICA	OBJETIVO	INDICADOR CORRELACIONADO
Nº 1	P01	OB07	-
Racionalização da ocupação de espaços físicos.	Consumo não racional de recursos ambientais e financeiros.	Promover a aquisição de materiais ambientalmente corretos para execução de serviços.	Percentual de redução de aquisição de materiais de consumo.
Nº 4	P05	OB11	-
Fomento à inovação no mercado.	Baixo número de soluções inovadoras implementadas.	Fomentar a implementação de soluções inovadoras.	Quantidade de soluções inovadoras voltadas à sustentabilidade implementadas em processos ou serviços da AGU.
Nº 5	P06	OB12	-
Negócios de impacto nas contratações.	Baixo número de contratações e ações que contemplem negócios de impacto.	Fomentar as contratações e ações que contemplem negócios de impacto.	Quantidade de postos inclusivos criados.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares e no "ANEXO I" deste Termo de Referência.

3.2. A solução HCI consolida computação, armazenamento, virtualização e rede/segurança distribuída em um único domínio operacional, com console unificado e APIs/IaC para automação completa do ciclo de vida. Em termos técnicos, adota arquitetura scaleout em cluster, permitindo expansão linear por nó, alta disponibilidade nativa com tolerância a falhas de discos/nós e atualizações rolling coordenadas (LCM) sem janelas de indisponibilidade. A observabilidade é fullstack, correlacionando métrica de máquinas virtuais, datastore/bucket e rede leste-oeste,

reduzindo tempo médio de reparo/retorno e dando base objetiva para disponibilidade e experiência percebida pelos usuários do EVA.

3.3. Do ponto de vista de desempenho e dados, a HCI moderna explora SSDs NVMe e data locality para latência baixa e throughput alto em cargas como Moodle, bancos, cache e mídia, evitando hairpins pelo core. No mesmo cluster, disponibiliza serviços multiprotocolo (bloco, arquivo e objeto) e funções de dados integradas, thin provisioning, deduplicação, compressão, snapshots e clones eficientes, além de criptografia em repouso e em trânsito com suporte a KMS/BYOK. Isso viabiliza desde o repositório transacional até acervos de mídia com áreas de staging/transcoding e preservação, mantendo o controle local de capacidade e performance, necessário para picos sazonais de matrícula e avaliações.

3.4. Quanto a resiliência e continuidade, a plataforma oferece HA intrasite (capacidade de manter serviços em funcionamento), selfhealing e orquestração de recuperação de desastres nativa com runbooks e testes sem impacto, suportando replicação síncrona/assíncrona e metas de RPO/RTO definidas para workloads críticos (por exemplo, Moodle). A elasticidade híbrida é opcional: é possível integrar com nuvem para backup/arquivamento em objeto, extensão de capacidade ou distribuição de conteúdo, além de interoperar com balanceadores, WAF e CDN. Segurança é tratada de ponta a ponta com microsegmentação/firewall distribuído no hipervisor, RBAC e MFA, trilhas de auditoria, integração com SIEM/SOAR e backups imutáveis (WORM), atendendo LGPD e diretrizes do setor público.

3.5. No âmbito comercial, a HCI simplifica governança e suporte ao reduzir a quantidade de contratos e consoles, sem impedir critérios de transparência e concorrência: é possível definir métricas objetivas (latência, IOPS/GB, eficiência de dados, disponibilidade, tempo de reparo, qualidade de suporte) e compará-las entre fornecedores/hipervisores suportados. O modelo “pay as you grow” por nó traz previsibilidade de custos e alinha investimento ao crescimento real de cursos, vídeos e usuários; a consolidação operacional reduz OpEx (menos integrações frágeis e retrabalho), enquanto documentação e migração assistida encurtam a curva de adoção e mitigam riscos operacionais.

3.6. Por fim, a HCI acelera a oferta educacional ao transformar infraestrutura em um serviço ágil: novos ambientes de curso, turmas e integrações são provisionados via catálogos e pipelines IaC, com políticas padronizadas de segurança e proteção de dados. A combinação de baixa latência, gestão unificada e automação end to end sustenta experiência consistente, mesmo em picos sazonais, enquanto a capacidade local para o acervo e a recuperação de desastre orquestrado asseguram continuidade acadêmica. Em termos práticos, a AGU ganha velocidade de inovação pedagógica com controle fino de custos e conformidade, reduzindo os riscos do projeto ao longo do ciclo de vida.

4. REQUISITOS DA CONTRATAÇÃO

Requisitos de Negócio

4.1. A presente contratação orienta-se pelos seguintes requisitos de negócio:

4.1.1. Disponibilidade contínua do Portal: garantir acesso ininterrupto ao EVA;

4.1.2. Experiência de uso consistente: manter desempenho estável para navegação, aulas, avaliações e mídia, inclusive em picos sazonais;

4.1.3. Escalabilidade alinhada à demanda: crescer de forma modular e previsível conforme aumentam cursos, vídeos, usuários e acessos simultâneos;

4.1.4. Conformidade regulatória: atender plenamente à LGPD e às diretrizes de segurança do setor público, com governança e auditoria;

4.1.5. Transparência e concorrência: adotar critérios objetivos de seleção (desempenho, latência, eficiência, suporte) que preservem a concorrência e reduzam, ao máximo, o lock-in;

4.1.6. Eficiência operacional: reduzir a complexidade do ambiente, diminuindo esforço de gestão e riscos operacionais;

- 4.1.7. Previsibilidade de custos: oferecer visibilidade e controle do custo total ao longo do ciclo de vida, com investimento proporcional ao crescimento real;
- 4.1.8. Resiliência e continuidade acadêmica: assegurar continuidade do ensino com planos de recuperação de desastres, priorizando workloads críticos como o Moodle;
- 4.1.9. Suporte técnico: suporte aderente à criticidade (24x7 para incidentes graves), documentação e migração assistida;
- 4.1.10. Agilidade na oferta educacional: otimizar tempo de disponibilização de novos cursos/funcionalidades, sustentando inovação pedagógica e alcance social;
- 4.1.11. Ampliação na oferta educacional: oferecer novos cursos ao governo federal e a cidadãos de forma ampla.

Requisitos Técnicos:

4.2. A presente contratação orienta-se pelos seguintes requisitos técnicos:

- 4.2.1. Integração: consolidar processamento, armazenamento e virtualização em um único domínio operacional, simplificando gestão e provisão;
- 4.2.2. Alta disponibilidade nativa: cluster com tolerância a falhas de nós/discos e atualizações “rolling”, evitando janelas de indisponibilidade;
- 4.2.3. Desempenho de baixa latência: uso de SSDs NVMe e alta conectividade leste-oeste para acelerar Moodle, bancos de dados, cache e serviços multimídia;
- 4.2.4. Serviços de dados modernos: compressão, deduplicação, thin provisioning, snapshots, clones eficientes e criptografia em repouso;
- 4.2.5. Multiprotocolos de armazenamento: suporte a blocos, arquivos e objetos (iSCSI/NFS/SMB/S3) para adequar-se a bancos, repositórios, mídia e relatórios;
- 4.2.6. Capacidade local para o acervo: espaço para staging, transcoding, cópias de preservação e migrações, considerando volume atual e perspectiva de crescimento;
- 4.2.7. Rede redundante e segmentada: conectividade de alta capacidade com redundância, LACP/MLAG, VLANs/VRFs e microsegmentação;
- 4.2.8. Segurança de ponta a ponta: RBAC, MFA, trilhas de auditoria, criptografia em trânsito/repouso, integração com SIEM/SOAR e backups imutáveis (WORM);
- 4.2.9. Recuperação de desastres e elasticidade híbrida: replicação síncrona/assíncrona entre sites, orquestração de failover com RPO/RTO definidos e possibilidade de extensão para nuvem; integração com balanceadores, WAF e, quando aplicável, CDN;
- 4.2.10. Gestão unificada e automação: console único com observabilidade, LCM para atualizações coordenadas, APIs/IaC para automação; interoperabilidade com hipervisores amplamente usados e caminho opcional para contêineres/Kubernetes.

Requisitos de Capacitação

4.3. Não faz parte do escopo da contratação a realização de capacitação técnica na utilização dos recursos relacionados ao objeto da presente contratação.

Requisitos Legais

4.4. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133, de 2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), Instrução Normativa SEGES/MP nº 5, de 26 de

maio de 2017 ratificada pela Instrução Normativa SEGES/ME nº 98, de 26 de dezembro de 2022, Instrução Normativa SEGES/ME nº 77, de 4 de novembro de 2022, Instrução Normativa SEGES/ME nº 73, de 30 de setembro de 2022, Instrução Normativa GSI nº 1, de 27 de maio de 2020, Decreto nº 11.462, de 31 de março de 2023, Portaria AGU n. 166, de 12 de março de 2025 e a outras legislações aplicáveis.

Requisitos de Manutenção

4.5. Devido às características da solução, a Contratada deverá realizar manutenções corretivas, preventivas, adaptativas e evolutivas. O objetivo é assegurar a disponibilidade integral da solução durante o período de garantia de 12 (doze) meses, contados a partir da emissão do Termo de Recebimento Definitivo.

Requisitos Temporais

4.6. A Entrega dos equipamentos deverá ser efetivada no prazo máximo de até 60 (sessenta) dias corridos, a contar do recebimento da Ordem de Fornecimento de Bens (OFB), emitida pela Contratante, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante;

4.6.1. Cronograma de Entregas: na execução das atividades deverão ser observados os seguintes prazos:

Evento	Atividade / Entrega	Prazo
1	Reunião Inicial	Em até 10 (dez) dias úteis após a assinatura do contrato.
2	Entrega dos Equipamentos	Em até 60 (sessenta) dias corridos contados da assinatura da OFB.
3	Serviços de Instalação e implantação	Até 15 (quinze) dias após a emissão de Ordem de Serviço - OS (a qual será emitida após a entrega dos equipamentos) pela AGU.
4	Manuais Técnicos, Documentação do Fabricante	No ato da entrega dos equipamentos.
5	Termos de Sigilo, Termo de Ciência e Plano de Implantação	Durante a Reunião Inicial.

4.7. Na contagem dos prazos estabelecidos neste Termo de Referência, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento.

4.8. Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias corridos. Ressaltando que serão contados os dias a partir da hora em que ocorrer o incidente até a mesma hora do último dia, conforme os prazos.

Requisitos de Segurança e Privacidade

4.9. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação da AGU, e deverá respeitar as normas nacionais de proteção de dados e informações vigentes, sobretudo considerando a possibilidade de custódia de conhecimentos, informações e dados pelo prestador de serviços, observadas as seguintes diretrizes:

- a) Garantia de aplicabilidade da legislação brasileira sobre os princípios, diretrizes e responsabilidades relacionados à segurança da informação e à proteção de dados.
- b) Garantia que, em qualquer hipótese, a Administração tem a tutela absoluta sobre os conhecimentos, informações e dados produzidos pelos serviços.
- c) Vedado o uso corporativo dos conhecimentos, informações e dados pelo prestador de serviço.
- d) Possuir Plano de Continuidade, Recuperação de Desastres e Contingência de Negócio, que possa ser testado regularmente, objetivando a disponibilidade dos dados e serviços em caso de interrupção.
- e) Desenvolver e colocar em prática procedimentos de respostas a incidentes relacionados com os serviços.

4.10. A CONTRATADA deverá seguir as normas internas de segurança da informação da AGU, bem como suas atualizações.

4.11. A CONTRATADA será expressamente responsabilizada quanto à manutenção de sigilo absoluto sobre quaisquer dados, informações, códigos-fonte e artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venham a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob pena de aplicação de sanção e outras penalidades previstas na legislação vigente, independente da classificação de sigilo conferida pela AGU a tais documentos.

4.12. A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, da AGU sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos.

4.13. Cada profissional da CONTRATADA deverá assinar termo declarando estar ciente de que a estrutura computacional disponibilizada pela AGU não poderá ser utilizada para fins particulares, e que a navegação em sítios da Internet e as correspondências em meio eletrônico utilizando o endereço da AGU ou acessadas a partir dos seus equipamentos poderão ser auditadas.

4.14. A CONTRATADA deverá assinar termo de compromisso declarando total obediência às normas de segurança vigentes ou que venham a ser implantadas, a qualquer tempo, na AGU.

Requisitos Sociais, Ambientais e Culturais

4.15. A solução deve estar aderente às seguintes diretrizes sociais, ambientais, culturais e acessibilidade, observando-se, no que couber, o Guia Nacional de Contratações Sustentáveis e suas atualizações, elaborado pela Câmara Nacional de Sustentabilidade da Controladoria Geral da União/Advocacia Geral da União e o Plano Diretor de Logística Sustentável (PDLS) da Advocacia-Geral da União (AGU):

4.15.1. A solução deve atender a critérios de baixo impacto ambiental e eficiência energética:

4.15.1.1. Eficiência Energética: os equipamentos fornecidos devem possuir fontes de alimentação de alta eficiência, com certificação 80 PLUS Platinum ou superior (ou equivalente), além de conformidade com padrões internacionais de consumo inteligente, como a certificação ENERGY STAR (ou selo Procel /ENCE aplicável a servidores).

4.15.1.2. Restrição de Substâncias Tóxicas: os componentes de hardware devem atestar conformidade com a diretiva RoHS (*Restriction of Certain Hazardous Substances*), garantindo a ausência ou limitação de metais pesados (como chumbo, mercúrio e cádmio) em sua fabricação.

4.15.1.3. Logística Reversa e Resíduos Sólidos: a Contratada deverá ser responsável pelo recolhimento e pela destinação ambientalmente adequada de todas as embalagens geradas durante a instalação (preferencialmente utilizando materiais recicláveis ou papelão pardo, evitando EPS/Isopor). Caso a contratação preveja substituição de parque (desfazimento), a Contratada deve executar a logística reversa dos equipamentos antigos, em observância à Política Nacional de Resíduos Sólidos (Lei nº 12.305/2010).

4.16. A contratação deve observar as diretrizes de responsabilidade corporativa e fomento às políticas públicas de inclusão social.

4.16.1. Os equipamentos devem vir acompanhados de manuais em língua portuguesa, salvo comprovada indisponibilidade pelo fabricante, e que atendam às normas técnicas de acessibilidade vigentes.

Requisitos da Arquitetura Tecnológica

4.18. Os equipamentos deverão observar integralmente os requisitos de arquitetura tecnológica descritos no "ANEXO I" deste Termo de Referência.

4.19. A adoção de tecnologia ou arquitetura diversa deverá ser autorizada previamente pela CONTRATANTE. Caso não seja autorizada, é vedado à CONTRATADA adotar arquitetura, componentes ou tecnologias diferentes daquelas definidas pela CONTRATANTE.

4.20. Deve ser escalável, flexível e compatível com integrações nativas e de terceiros, assegurando alta disponibilidade, mecanismos de backup e recuperação de desastres. Além disso, deve permitir gerenciamento e monitoramento centralizados em tempo real, apoiar tecnologias modernas como containers, microserviços e automação, e manter alinhamento com as melhores práticas e padrões tecnológicos do mercado.

Requisitos de Projeto e de Implementação

4.21. Os equipamentos deverão observar integralmente os requisitos de projeto e de implementação descritos a seguir:

- a) A CONTRATADA deverá elaborar e apresentar um Plano de Projeto de Implantação, adotando como base o modelo constante no Anexo IV, detalhando as ações necessárias para a implantação da solução.
- b) O Plano de Projeto deverá ser enviado para validação e aprovação pela equipe técnica da AGU conforme disposto no Anexo IV.
- c) O Plano de Projeto de Implantação deverá conter os responsáveis envolvidos, o cronograma e a análise do risco associada às atividades de fornecimento e implantação.

4.22. O fornecedor deverá entregar toda a documentação técnica da solução, incluindo manuais oficiais do fabricante (em português, se disponíveis, ou em inglês), licenças, mídia de instalação, diagramas de arquitetura implementada e documentação de configuração.

4.23. Todo procedimento de instalação, configuração, testes e documentação é de responsabilidade da Contratada e deverá ser realizado pelo fabricante ou por profissional com as certificações necessárias fornecidas pelo fabricante.

Requisitos de Implantação

4.24. Os equipamentos deverão observar integralmente os requisitos de implantação, instalação e fornecimento descritos no Estudo Técnico Preliminar e no "ANEXO I". Adicionalmente:

- 4.24.1. A contratada deverá realizar a instalação física dos equipamentos no datacenter da AGU e a configuração de todo o sistema de armazenamento, assegurando o pleno funcionamento da solução com todas as funcionalidades previstas. Isso inclui a integração com os sistemas e servidores existentes no órgão, aplicação de customizações necessárias e realização de ajustes para compatibilidade com o ambiente tecnológico. Também deve realizar testes e relatório de pós-implantação, entregando a solução plenamente funcional.

Requisitos de Garantia, Manutenção e Assistência Técnica

4.25. O prazo de garantia contratual dos bens, complementar à garantia legal, será de, no mínimo, 12 (doze) meses, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto. A garantia integral de fábrica, cobrindo hardware e software integrado, será contada a partir do recebimento definitivo do objeto e abrange a realização de manutenção corretiva, preventiva e proativa, com fornecimento e substituição de peças novas e originais, sem ônus para a AGU.

4.26. Caso o prazo da garantia oferecida pelo fabricante seja inferior ao estabelecido nesta cláusula, o fornecedor deverá complementar a garantia do bem ofertado pelo período restante.

4.27. A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o Contratante.

4.28. A garantia abrange a realização da manutenção corretiva dos bens pelo próprio Contratado, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

4.29. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.

4.30. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.

4.31. Uma vez notificado, o Contratado realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até 10 (dez) dias úteis, contado a partir da data de retirada do equipamento das dependências da Administração pelo Contratado ou pela assistência técnica autorizada.

4.31.1. O prazo indicado para reparação ou substituição dos bens, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada do Contratado, aceita pelo Contratante.

4.32. Na hipótese do subitem acima, o Contratado deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pelo Contratante, de modo a garantir a continuidade dos trabalhos administrativos durante a execução dos reparos.

4.33. Decorrido o prazo para reparos e substituições sem o atendimento da solicitação do Contratante ou a apresentação de justificativas pelo Contratado, fica o Contratante autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir do Contratado o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos.

4.34. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade do Contratado.

4.35. A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

4.36. Atualizações e Manutenção Preventiva: Durante a vigência da garantia, a contratada (em conjunto com o fabricante) deve fornecer todas as atualizações de software, firmware e patches relevantes para o equipamento, bem como realizar manutenções preventivas periódicas conforme recomendação do fabricante.

4.37. Suporte Técnico: é necessário suporte ágil e ininterrupto para garantir alta disponibilidade. A contratada deve disponibilizar central de atendimento telefônico da CONTRATADA, disponível durante vinte e quatro horas por dia e sete dias na semana (24x7), com atendimento em português, possibilitando a abertura de chamados técnicos, sem limite de quantidade de chamados.

4.38. A garantia e o suporte técnico deverá ser prestado diretamente pelo fabricante da solução ou por técnicos certificados da Contratada.

Requisitos de Experiência Profissional

4.39. Os serviços de assistência técnica, suporte, garantia deverão ser prestados por profissionais devidamente capacitados e habilitados para o objeto especificado neste Termo de Referência, bem como com todos os recursos ferramentais necessários para a prestação dos serviços.

Requisitos de Formação da Equipe

4.40. Os serviços deverão ser prestados por profissionais devidamente capacitados e habilitados para o objeto especificado neste Termo de Referência.

Requisitos de Metodologia de Trabalho

4.41. O fornecimento dos equipamentos e serviços estão condicionados ao recebimento pelo Contratado de Ordem de fornecimento de Bens/ Serviços (OFB/OS) emitida pela Contratante.

4.42. A OFB indicará o tipo de equipamento, a quantidade e a localidade na qual os equipamentos deverão ser entregues.

4.43. O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana de maneira eletrônica e/ou por via telefônica.

4.44. O andamento do fornecimento dos equipamentos deve ser acompanhado pelo Contratado, que dará ciência de eventuais acontecimentos à Contratante.

Requisitos de Segurança da Informação e Privacidade

4.45. O Contratado deverá observar integralmente os requisitos de Segurança da Informação e Privacidade descritos a seguir:

4.45.1. As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

4.45.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.

4.45.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

4.45.4. Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever da CONTRATADA eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

4.45.5. É dever da CONTRATADA orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

4.45.6. A CONTRATADA deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

4.45.7. O CONTRATANTE poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo a CONTRATADA atender prontamente eventuais pedidos de comprovação formulados.

4.45.8. A CONTRATADA deverá prestar, no prazo fixado pelo CONTRATANTE, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

4.45.9. Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

4.45.10. Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.

4.45.11. O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

4.45.12. Os contratos e convênios de que trata o § 1º do art. 26 da LGPD deverão ser comunicados à autoridade nacional.

Outros Requisitos Aplicáveis

4.46. Comprovação de parceria: a empresa licitante deverá apresentar declaração emitida pela(s) fabricante (s) de sua oferta informando que é uma revenda autorizada daquele(s) fabricante(s), demonstrando desta forma que é habilitada a comercializar produtos e serviços dela no Brasil;

4.47. A exigência da declaração torna-se necessária pela complexidade e relevância da solução para a CONTRATANTE, uma vez que as empresas elegíveis para manutenção e suporte da solução devem ser parceiras credenciadas;

Sustentabilidade

4.48. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

4.48.1. Os bens deverão ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento;

4.48.2. Os equipamentos entregues deverão ter longa vida útil e suporte a atualizações, minimizando substituições prematuras e reduzindo impactos ambientais relacionados ao ciclo de vida; 4.48.3. Toda a documentação entregue (relatórios, manuais, registros de implantação) deve ser preferencialmente em formato digital, evitando impressão desnecessária;

4.48.4. A contratada deverá implementar ações de logística reversa para baterias, componentes eletrônicos e demais resíduos gerados, assegurando sua coleta, transporte e destinação final ambientalmente adequada;

4.48.5. A Contratada deverá adotar práticas de sustentabilidade ambiental na execução do objeto, quando couber, conforme disposto na Instrução Normativa SLTI/MP nº 01/2010, de 19 de janeiro de 2010, no Guia Nacional de Contratações Sustentáveis, de setembro de 2023 e na Lei 14.133/21

Indicação de marcas ou modelos:

4.49. Não se aplica.

Da vedação de utilização de marca/produto na execução do serviço

4.50. Não se aplica.

Da exigência de carta de solidariedade

4.51. Não se aplica.

Subcontratação

4.52. Não será admitida a subcontratação do objeto contratual.

Da participação de consórcios e cooperativas

4.53. Fica vedada a participação de empresas reunidas em consórcio. A vedação à participação em consórcio justifica-se pela arquitetura indissociável da solução de hiperconvergência (HCI), que unifica nativamente computação, armazenamento e rede. Admitir consórcios fragmentaria a execução contratual e o suporte técnico, gerando riscos de transferência de responsabilidades entre as empresas em caso de incidentes. Para assegurar a mitigação de riscos operacionais e garantir um ponto único de contato, exige-se a centralização em uma única contratada. Ressalta-se que essa restrição não fere a competitividade do certame, visto que existe no mercado diversos integradores de TI capazes de fornecer a solução de forma unificada.

4.53.1. Fica vedada também, a participação de cooperativas de trabalho, em razão da incompatibilidade entre o modelo cooperativista e as exigências técnicas e operacionais do objeto. A solução a ser contratada contempla o fornecimento de soluções de alta complexidade técnica e que demandam a necessidade de responsabilidade única na execução do objeto. As cooperativas de trabalho, regidas pelas Leis nº 5.764/1971 e nº 12.690/2012, baseiam-se na autogestão e na ausência de subordinação hierárquica, características que as tornam inadequadas para contratações que demandam relação de subordinação e pessoalidade, além de responsabilidade direta da contratada pela execução e pelos resultados decorrentes dessas atividades.

Da exigência de amostra

4.54. Não será exigida a apresentação de amostra do objeto.

Garantia da contratação

- 4.55. Será exigida garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, com validade durante toda a execução do contrato e por 90 (noventa) dias após o término de sua vigência, podendo o contratado optar pela caução em dinheiro ou em títulos da dívida pública, seguro-garantia, fiança bancária ou título de capitalização, em valor correspondente a 5% (cinco por cento) do valor total da contratação.
- 4.56. Em caso de opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.
- 4.56.1. A apólice de seguro-garantia permanecerá em vigor mesmo que o Contratado não pague o prêmio nas datas convencionadas.
- 4.56.2. Caso o adjudicatário não apresente a apólice de seguro de garantia antes da assinatura do contrato, ocorrerá a preclusão do direito de escolha dessa modalidade de garantia.
- 4.56.3. A apólice de seguro-garantia deverá acompanhar as modificações referentes à vigência do contrato principal mediante a emissão do respectivo endosso pela seguradora.
- 4.56.4. Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvados os períodos de suspensão contratual.
- 4.56.5. Caso o adjudicatário não opte pelo seguro-garantia ou não apresente a apólice de seguro de garantia antes da assinatura do contrato, deverá apresentar, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do Contratante, contado da assinatura do contrato, comprovante de prestação de garantia nas modalidades de caução em dinheiro ou títulos da dívida pública, fiança bancária ou títulos de capitalização.
- 4.57. Caso seja a garantia em dinheiro a modalidade de garantia escolhida pelo Contratado, deverá ser efetuada em favor do Contratante, em conta específica na Caixa Econômica Federal, com correção monetária.
- 4.58. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério competente.
- 4.59. No caso de garantia na modalidade de fiança bancária, deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.
- 4.60. Na hipótese de opção pelo título de capitalização, a garantia deverá ser custeada por pagamento único, com resgate pelo valor total, sob a modalidade de instrumento de garantia, emitido por sociedades de capitalização regulamente constituídas e autorizadas pelo Governo Federal.
- 4.60.1. O título de capitalização deverá ser apresentado ao Contratante juntamente com as condições gerais e o número do processo administrativo sob o qual o plano de capitalização foi aprovado pela Susep (art. 8º, III, da Circular SUSEP nº 656, de 11 de março de 2022).
- 4.61. A garantia assegurará, qualquer que seja a modalidade escolhida, sob pena de não aceitação, o pagamento de:
- 4.61.1. prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas; e
- 4.61.2. multas moratórias e punitivas aplicadas pela Administração ao Contratado.
- 4.62. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, contado da data de assinatura do termo aditivo ou da emissão do apostilamento, seguindo os mesmos parâmetros utilizados quando da contratação.
- 4.63. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o Contratado ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

4.64. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, o Contratado obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do Contratante, contados da data em que for notificada[A31] .

4.65. O Contratante executará a garantia na forma prevista na legislação que rege a matéria.

4.65.1. O emitente da garantia ofertada pelo Contratado deverá ser notificado pelo Contratante quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

4.65.2. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep nº 662, de 11 de abril de 2022.

4.66. Extinguir-se-á a garantia com a restituição da carta fiança, autorização para a liberação de importâncias depositadas em dinheiro a título de garantia ou anuência ao resgate do título de capitalização, acompanhada de declaração do Contratante, mediante termo circunstanciado, de que o Contratado cumpriu todas as cláusulas do contrato.

4.66.1. A extinção da garantia na modalidade seguro-garantia observará a regulamentação da Susep.

4.66.2. A Administração deverá apurar se há alguma pendência contratual antes do término da vigência da apólice.

4.67. A garantia somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.

4.68. O Contratado autoriza o Contratante a reter, a qualquer tempo, a garantia, na forma prevista neste Termo de Referência.

4.69. O garantidor não é parte para figurar em processo administrativo instaurado pelo Contratante com o objetivo de apurar prejuízos e/ou aplicar sanções ao Contratado.

4.70. A garantia de execução é independente de eventual garantia do produto ou serviço prevista neste Termo de Referência.

Vistoria

4.71. Fica facultada ao interessado o direito de realização de vistoria prévia, para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 9 horas às 17 horas, devendo o agendamento ser realizado previamente pelo endereço eletrônico dlog.licitacao@agu.gov.br, na Advocacia Geral da União - Departamento de Tecnologia da Informação - Setor de Indústrias Gráficas SIG, Quadra 06, Lote 800 – Brasília - DF, CEP: 70610-460.

4.72. Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

4.73. Para a vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

4.74. A Declaração de Vistoria integrante do Termo de Referência, nos termos do ANEXO VI, deverá ser assinada pelos representantes da AGU e da Licitante, ou o seu representante legal, comprovando que a empresa realizou a vistoria técnica para conhecimento dos serviços necessários, do ambiente tecnológico e das condições técnicas para sua realização.

4.75. Caso o interessado opte por não realizar a vistoria, deverá prestar declaração formal assinada pelo seu responsável técnico acerca do conhecimento pleno das condições e peculiaridades da contratação.

4.76. A Licitante poderá optar pela não realização da vistoria, para tanto deverá apresentar, junto com sua proposta de preços, caso seja a vencedora da etapa de lances, a Declaração de Recusa de Vistoria, conforme modelo fornecido, nos termos do ANEXO VII, devidamente assinada por seus representantes legais.

4.77. A não realização da vistoria, quando facultativa, não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o Contratado assumir os ônus dos serviços decorrentes.

Informações relevantes para o [dimensionamento E/OU apresentação] da proposta

4.78. A demanda do órgão tem como base as características detalhadas neste Termo de Referência e nas especificações técnicas do ANEXO I.

Reserva de cotas para microempresas e empresas de pequeno porte:

4.79. Na presente licitação, não será aplicada a reserva de cota de até 25% (vinte e cinco por cento) do objeto para contratação de microempresas e empresas de pequeno porte, uma vez que o objeto não contempla itens com valores inferiores a R\$ 80.000,00 (oitenta mil reais) e o parcelamento do objeto mostrou-se inviável, conforme justificativas apresentadas no subitem 2.27 deste Termo de Referência.

Margem de Preferência

4.80. Não se aplica a margem de preferência tendo em vista que a solução de hiperconvergência não possui comprovação de atendimento aos critérios de nacionalização exigidos. Especificamente, não há evidências de que os produtos atendam ao Processo Produtivo Básico (PPB) ou estejam vinculados ao Desenvolvimento de Tecnologia Nacional (DTN), conforme exigido para a concessão da margem de preferência.

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da CONTRATANTE:

5.1.1. nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

5.1.2. encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

5.1.3. receber o objeto fornecido pelo Contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

5.1.4. aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

5.1.5. liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

5.1.6. comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

5.1.7. prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer.

5.2. São obrigações do CONTRATADO:

5.2.1. indicar formalmente preposto apto a representá-la junto à Contratante, que deverá responder pela fiel execução do contrato;

5.2.2. atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

5.2.3. reparar quaisquer danos diretamente causados à Contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução do contrato pela Contratante;

5.2.4. propiciar todos os meios necessários à fiscalização do contrato pela Contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

5.2.5. manter, durante toda a execução do contrato, as mesmas condições da habilitação;

5.2.6. quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

5.2.7. ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração; e

5.2.8. fazer a transição contratual, com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações.

5.3. São obrigações do órgão gerenciador do registro de preços:

5.3.1. efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;

5.3.2. conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;

5.3.3. definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:

5.3.4. as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e

5.3.5. definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável;

5.3.6. definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:

5.3.7. a definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;

5.3.8. as regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pelo contratado; e

5.3.9. as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a verificação de Amostra do Objeto, observado o disposto no inciso III, alínea "c", item 2 do art. 17 da Instrução Normativa SGS/ME nº 94, de 2022, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

5.3.10. Caberá à AGU, como órgão gerenciador da Ata de Registro de Preços, as responsabilidades elencadas no Decreto nº 11.462, de 31 de março de 2023, que regulamenta o Sistema de Registro de Preços.

5.3.11. Dentre as competências da AGU, destaca-se o procedimento de Intenção de Registro de Preços, publicado no Portal de Compras do Governo Federal (<https://www.gov.br/compras/pt-br/>), visando a divulgação dos itens a serem licitados e facultar aos órgãos e entidades integrantes do Sistema de Serviços Gerais (SISG), antes de iniciar o procedimento licitatório, consultar a IRP em andamento e deliberar a respeito da conveniência de sua participação. Contudo, considerando a especificidade da solução para o ambiente da AGU, a capacidade de gerenciamento da AGU, verifica-se a possibilidade de dispensa da divulgação da intenção de registro de preços.

5.3.12. A dispensa da divulgação da intenção de registro de preços encontra amparo no Decreto nº 11.462, de 31 de março de 2023, no seu art. 9º, parágrafo 2º, conforme transcrito a seguir, in verbis:

Da intenção de registro de preços (...)

§ 2º O procedimento previsto no caput poderá ser dispensado quando o órgão ou a entidade gerenciadora for o único contratante.

5.3.13. Além disso, não será admitida a adesão à ata de registro de preços decorrente da licitação, na forma justificada neste Termo de Referência.

6. MODELO DE EXECUÇÃO DO CONTRATO

Rotinas de Execução

Do Encaminhamento Formal de Demandas

6.1. O gestor do contrato emitirá a Ordem de fornecimento de bens (OFB) para a entrega dos bens desejados ou emitirá a Ordem de Serviço (OS) para a prestação dos serviços.

6.2. O Contratado deverá fornecer equipamentos com as mesmas configurações e quantidades definidas na OFB.

6.3. O recebimento provisório e definitivo dos bens é disciplinado em tópico próprio deste Termo de Referência.

Forma de execução e acompanhamento do contrato

Condições de Entrega

6.4. O prazo de entrega dos bens é de até 60 (sessenta) dias, contados do(a) data de assinatura da OFB.

6.5. Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 10 (dez) dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

6.6. Os bens deverão ser entregues no seguinte endereço:

a) Advocacia-Geral da União localizado no SIG - Quadra 6 Lote 800, em Brasília, DF - Sede III;

b) Advocacia-Geral da União localizado no Setor de Autarquias Sul - Quadra 3 - Lote 5/6, Ed. MultiBrasil Corporate, em Brasília, DF - Sede I.

6.7. Os equipamentos deverão estar acondicionados adequadamente em caixas lacradas de forma a propiciar a completa segurança durante o transporte.

6.8. Todos os equipamentos deverão ser novos, não recondicionados, de primeiro uso e não deverão conter amassados, arranhões ou outros problemas e, ainda, serem entregues em pleno estado de funcionamento.

Formas de transferência de conhecimento

6.9. Transferência de conhecimento por meio de atividades teóricas e práticas voltadas à operação, monitoramento e manutenção básica da solução de Infraestrutura Hiperconvergente (HCI), abrangendo o gerenciamento do cluster, a expansão de nós, os procedimentos de backup e restore e ações de troubleshooting para suporte à operação contínua da solução.

Procedimentos de transição e finalização do contrato

6.10. Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

Quantidade mínima de bens ou serviços para comparação e controle

6.11. Cada OFB conterá a quantidade a ser fornecida, incluindo a sua localização e o prazo, conforme definições deste Termo de Referência.

Mecanismos formais de comunicação

6.12. São definidos como mecanismos formais de Comunicação, entre a Contratante e o Contratado, os seguintes:

6.12.1. Ordem de Fornecimento de Bens;

6.12.2. Relatórios e Ata de Reunião;

6.12.3. Ofício;

6.12.4. Sistema de abertura de chamados;

6.12.5. E-mails institucional/corporativo e Cartas;

6.12.6. Ferramenta Microsoft Teams ou Google Meet ou similar em uso pela AGU;

6.12.7. SUPER SAPIENS - (<https://supersapiens.agu.gov.br/auth/login>);

6.12.8. Demais Termos previstos no instrumento convocatório.

Formas de Pagamento

6.13. Os critérios de medição e pagamento serão tratados em tópico próprio do Modelo de Gestão do Contrato.

Manutenção de Sigilo e Normas de Segurança

6.14. O Contratado deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução do contrato, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

6.15. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação, encontram-se nos ANEXOS V e XI.

7. MODELO DE GESTÃO DO CONTRATO

7.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

7.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

7.3. As comunicações entre o órgão ou entidade e o Contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

7.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

Reunião Inicial

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

7.6. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até 10 (dez) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

7.7. A pauta desta reunião observará, pelo menos:

7.7.1. Presença do representante legal da contratada, que apresentará o seu preposto;

7.7.2. Entrega, por parte da Contratada, do Termo de Compromisso, dos Termos de Ciência e Plano de Implantação;

7.7.3. esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

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

7.7.5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste Termo de Referência.

Fiscalização

7.8. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos, nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

Fiscalização Técnica

7.9. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

7.10. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.

7.11. Identificada qualquer inexecução ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

7.12. O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

7.13. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprezadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato.

7.14. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.

Fiscalização Administrativa

7.15. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

7.16. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência.

7.17. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade do Contratado, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da Contratante ou de seus agentes, gestores e fiscais, de conformidade.

Gestor do Contrato

7.18. Cabe ao gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022:

7.18.1. coordenar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

7.18.2. acompanhar os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

7.18.3. acompanhar a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotar os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

7.18.4. emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

7.18.5. tomar providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso.

7.18.6. elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.

7.18.7. enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

7.19. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual.

Critérios de Aceitação

7.20. A avaliação da qualidade dos produtos entregues, para fins de aceitação, consiste na verificação dos critérios relacionados a seguir:

7.21. Todos os equipamentos fornecidos deverão ser novos (incluindo todas as peças e componentes presentes nos produtos), de primeiro uso (sem sinais de utilização anterior), não recondicionados e em fase de comercialização normal através dos canais de venda do fabricante no Brasil (não serão aceitos produtos end-of-life).

7.22. Todos os componentes do(s) equipamento(s) e respectivas funcionalidades deverão ser compatíveis entre si, sem a utilização de adaptadores, frisagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos não previstos nas especificações técnicas ou, ainda, com emprego de materiais inadequados ou que visem adaptar forçadamente o produto ou suas partes que sejam fisicamente ou logicamente incompatíveis.

7.23. Todos os componentes internos do(s) equipamento(s) deverá(ão) estar instalado(s) de forma organizada e livres de pressões ocasionados por outros componentes ou cabos, que possam causar desconexões, instabilidade, ou funcionamento inadequado.

7.24. O número de série de cada equipamento deve ser obrigatório e único, afixado em local visível, na parte externa do gabinete e na embalagem que o contém. Esse número deverá ser identificado pelo fabricante, como válido para o produto entregue e para as condições do mercado brasileiro no que se refere à garantia e assistência técnica no Brasil.

7.25. Serão recusados os produtos que possuam componentes ou acessórios com sinais claros de oxidação, danos físicos, sujeira, riscos ou outro sinal de desgaste, mesmo sendo o componente ou acessório considerado como novos pelo fornecedor dos produtos.

7.26. Os produtos, considerando a marca e modelo apresentados na licitação, não poderão estar fora de linha comercial, considerando a data de LICITAÇÃO (abertura das propostas). Os produtos devem ser fornecidos completos e prontos para a utilização, com todos os acessórios, componentes, cabos etc.

7.27. Todas as licenças, referentes aos softwares e drivers solicitados, devem estar registrados para utilização do Contratante, em modo definitivo (licenças perpétuas), legalizado, não sendo admitidas versões “shareware” ou “trial”. O modelo do produto ofertado pelo licitante deverá estar em fase de produção pelo fabricante (no Brasil ou no exterior), sem previsão de encerramento de produção, até a data de entrega da proposta.

7.28. A Contratante poderá optar por avaliar a qualidade de todos os equipamentos fornecidos ou uma amostra dos equipamentos, atentando para a inclusão nos autos do processo administrativo de todos os documentos que evidenciem a realização dos testes de aceitação em cada equipamento selecionado, para posterior rastreabilidade.

7.29. Só haverá o recebimento definitivo, após a análise da qualidade dos bens e/ou serviços, em face da aplicação dos critérios de aceitação, resguardando-se ao Contratante o direito de não receber o OBJETO cuja qualidade seja comprovadamente baixa ou em desacordo com as especificações definidas neste Termo de Referência – situação em que poderão ser aplicadas à CONTRATADA as penalidades previstas em lei, neste Termo de Referência e no CONTRATO. Quando for o caso, a empresa será convocada a refazer todos os serviços rejeitados, sem custo adicional.

Procedimentos de Teste e Inspeção

7.30. Os serviços serão recebidos após a avaliação e realização dos testes necessários e a verificação do seu funcionamento, conforme exigências deste documento.

Níveis Mínimos de Serviço Exigidos

7.31. Os níveis mínimos de serviço são indicadores mensuráveis estabelecidos pelo Contratante para aferir objetivamente os resultados pretendidos com a contratação. São considerados para a presente contratação os seguintes indicadores:

IAE – INDICADOR DE ATRASO NO FORNECIMENTO DO EQUIPAMENTO	
Tópico	Descrição
Finalidade	Medir o tempo de atraso na entrega dos produtos e serviços constantes na Ordem de Fornecimento de Bens.
Meta a cumprir	IAE <= 0
Instrumento de medição	OFB, Termo de Recebimento Provisório (TRP)
	A avaliação será feita conforme linha de base do cronograma registrada na OFB.

Forma de acompanhamento	Será subtraída a data de entrega dos produtos da OFB (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data de início da execução da OFB.
Periodicidade	Para cada Ordem de Fornecimento de Bens encerrada e com Termo de Recebimento Definitivo.
Mecanismo de Cálculo (métrica)	<p>IAE = <u>TEX – TEST</u></p> <p>Onde:</p> <p>IAE – Indicador de Atraso de Entrega da OFB;</p> <p>TEX – Tempo de Execução – corresponde ao período de execução da OFB, da sua data de início até a data de entrega dos produtos da OFB.</p> <p>A data de início será aquela constante na OFB; caso não esteja explícita, será o primeiro dia útil após a emissão da OFB.</p> <p>A data de entrega da OFB deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes neste Termo de Referência. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução da OFB continua a correr, findando-se apenas quanto o Contratado entrega os produtos da OFB e haja aceitação por parte do fiscal técnico.</p> <p>TEST – Tempo Estimado para a execução da OFB – constante na OFB, conforme estipulado no Termo de Referência.</p>
Observações	<p>Obs1: Serão utilizados dias corridos na medição.</p> <p>Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador.</p>
Início de Vigência	A partir da emissão da OFB.
Faixas de ajuste no pagamento e Sanções	<p>Para valores do indicador IAE:</p> <p>Menor ou igual a 0 – Pagamento integral da OFB;</p> <p>De 1 a 60 - aplicar-se-á glosa de 0,1% por dia de atraso sobre o valor da OFB ou fração em atraso.</p> <p>Acima de 60 - aplicar-se-á glosa de 10%</p> <p>multa de 3% sobre o valor do Contrato, para valores do indicador IAE maiores que 75 dias.</p>

ITI - INDICADOR DE TEMPO DE INSTALAÇÃO DOS EQUIPAMENTOS	
Tópico	Descrição
Finalidade	Medir o tempo de atraso para instalação dos equipamentos após o aceite provisório.
Meta a cumprir	ITI <= 15 dias corridos (A meta definida visa garantir a instalação dos produtos constantes na Ordem de Serviço - OS dentro do prazo previsto).

Instrumento de medição	Cálculo do prazo de cada solicitação de instalação de equipamento em relação ao Nível de Serviço
Forma de acompanhamento	Cálculo do prazo de cada solicitação de instalação de equipamento em relação ao Nível de Serviço
Periodicidade	Para cada solicitação de instalação de equipamento.
Mecanismo de Cálculo (métrica)	ITI = TEE Onde: ITI - Indicador de Tempo de Instalação dos equipamentos após o aceite provisório; TEE - Tempo em dias úteis para execução da instalação do equipamento após o aceite provisório.
Observações	Obs1: Serão utilizados dias corridos na medição. Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador
Início de Vigência	A partir do aceite da entrega provisória.
Faixas de ajuste no pagamento e Sanções	ITI <= 15 dias: Pagamento integral da Ordem de Fornecimento de Bens ou fração em atraso; ITI >= 16 e <= 30 dias: Glosa de 1% sobre o valor da Ordem de Fornecimento de Bens ou fração em atraso; ITI >= 31 e < 45 dias: Glosa de 2% sobre o valor da Ordem de Fornecimento de Bens ou fração em atraso; ITI >= 45 dias: Glosa de 4% sobre o valor da Ordem de Fornecimento de Bens ou fração em atraso. Multa de 1% sobre o valor do Contrato, para valores do indicador ITI maiores que 60 dias corridos.

7.32.1. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a CONTRATADA:

7.32.1.1. não produziu os resultados acordados;

7.32.1.2. deixou de executar, ou não executou com a qualidade mínima exigida as atividades contratadas; ou

7.32.1.3. deixou de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.

7.33. A utilização do indicador não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

8. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NOS PAGAMENTOS

8.1. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela Contratante, conforme a tabela abaixo:

ID	Ocorrência	Glosa/Sanção
----	------------	--------------

1	Indisponibilidade superior a 40 minutos.	Advertência e notificação formal para correção; Em caso de reincidência: multa compensatória de 0,5% sobre o valor do contrato.
2	Indisponibilidade superior a 36 horas considerando o período de 30 dias.	Multa compensatória de 1% sobre o valor do contrato. Em caso de reincidência: multa compensatória de 3%
3	Reestabelecimento acima de 4h (Incidente com indisponibilidade total)	Multa moratória de 1% sobre o valor do contrato; Cada hora excedente agrava a dosimetria em 0,1% sobre o valor do contrato, limitado a 1%.
4	Reestabelecimento acima de 8h (Incidente com degradação severa ou perda de redundância)	Multa moratória de 0,5% sobre o valor do contrato; Cada hora excedente agrava a dosimetria em 0,1% sobre o valor do contrato, limitado a 1%.
5	Reestabelecimento acima de 24h (Falha de componente não crítico)	Advertência por evento. Reincidência de 3 ou mais ocorrências em 30 dias: multa compensatória de 1% sobre o valor do contrato.
6	Atraso na resposta aos chamados superior a 15 minutos (Indisponibilidade total ou Incidente com degradação severa)	Multa moratória proporcional à quantidade de chamados em atraso (razão da quantidade de chamados em atraso pela quantidade de chamados abertos), limitado a 5% do valor do contrato.
7	Atraso na resposta aos chamados superior a 4 horas (Falha em Configurações/atualizações)	Multa moratória proporcional à quantidade de chamados em atraso (razão da quantidade de chamados em atraso pela quantidade de chamados abertos), limitado a 3% do valor do contrato.
8	Atraso na resposta aos chamados superior a 2 horas (Falha em componente não crítico)	Advertência; Em caso de ausência de resposta por prazo superior a 10 dias úteis ou recebimento de 3 advertências: multa moratória proporcional à quantidade de chamados em atraso (razão da quantidade de chamados em atraso pela quantidade de chamados abertos), limitado a 2% do valor do contrato.
9	Não prestar os esclarecimentos imediatamente, referente à execução do contrato, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 24 (vinte e quatro) horas úteis.	Multa de 0,05% sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela Contratante, até o limite de 5 (cinco) dias úteis. Após o limite de 5 (cinco) dias úteis: aplicar-se-á multa compensatória de 1% do valor total do Contrato.
10	Não atender aos indicadores IAE e ITI.	Conforme sanções/Glosas previstas nas Faixas de Ajuste dos respectivos indicadores, detalhados no subitem 7.32.

11	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação: aplica-se multa compensatória de 0,25% do valor total do Contrato.
----	--	---

8.2. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que o Contratado:

8.2.1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

8.2.2. deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

8.3. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:

a) der causa à inexecução parcial do contrato;

b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

c) der causa à inexecução total do contrato;

d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

f) praticar ato fraudulento na execução do contrato;

g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

8.4. Serão aplicadas ao Contratado que incorrer nas infrações acima descritas as seguintes sanções:

8.4.1 Advertência, quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;

8.4.2. Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima, sempre que não se justificar a imposição de penalidade mais grave;

8.4.3. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave.

8.4.4. Multa:

8.4.4.1 Moratória, para as infrações descritas no item “d”, de 0,1% (um décimo por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias.

8.4.4.2. Moratória de 0,07% (sete centésimos por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 2% (dois por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia;

8.4.4.2.1. O atraso superior a 25 (vinte e cinco) dias para apresentação, suplementação ou reposição da garantia autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

8.4.4.3. Compensatória, para as infrações descritas acima alíneas “e” a “h” de 20% (vinte por cento) a 30% (trinta por cento) do valor da contratação.

8.4.4.4. Compensatória, para a inexecução total do contrato prevista acima na alínea “c”, de 20% (vinte por cento) a 30% (trinta por cento) do valor da contratação.

8.4.4.5. Compensatória, para a infração descrita acima na alínea “b”, de 15% (quinze por cento) a 20% (vinte por cento) do valor da contratação.

8.4.4.6. Compensatória, em substituição à multa moratória para a infração descrita acima na alínea “d”, de 1% (um por cento) a 5% (cinco por cento) do valor da contratação.

8.4.4.7. Compensatória, para a infração descrita acima na alínea “a”, de 6% (seis por cento) a 15% (quinze por cento) do valor da contratação.

8.4.5. As multas constantes no quadro do item 8.1 não poderão ser aplicadas de forma cumulativa com as constantes nos itens 8.4.4., considerando que já constam com sanções específicas.

8.5. A aplicação das sanções previstas neste Termo de Referência não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante.

8.6. Todas as sanções previstas neste Termo de Referência poderão ser aplicadas cumulativamente com a multa.

8.7. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

8.8. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

8.9. A multa poderá ser recolhida administrativamente no prazo máximo de 10 (dez) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

8.10. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

8.10.1. Para a garantia da ampla defesa e contraditório, as notificações serão enviadas eletronicamente para os endereços de e-mail informados na proposta comercial, bem como os cadastrados pela empresa no SICAF.

8.10.2. Os endereços de e-mail informados na proposta comercial e/ou cadastrados no SICAF serão considerados de uso contínuo da empresa, não cabendo alegação de desconhecimento das comunicações a eles comprovadamente enviadas.

8.11. Na aplicação das sanções serão considerados:

8.11.1. a natureza e a gravidade da infração cometida;

8.11.2. as peculiaridades do caso concreto;

8.11.3. as circunstâncias agravantes ou atenuantes;

8.11.4. os danos que dela provierem para o Contratante; e

8.11.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

8.12. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei.

8.13. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Termo de Referência ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

8.14. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal.

8.14.1. As penalidades serão obrigatoriamente registradas no SICAF.

8.15. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133, de 2021.

8.16. Os débitos do Contratado para com a Administração Contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o Contratado possua com o mesmo órgão ora Contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

9. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

Recebimento do Objeto

9.1. Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

9.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 10 (dez) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

9.3. O recebimento definitivo ocorrerá no prazo de 10 (dez) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado, bem como para os respectivos serviços associados de instalação e treinamento conforme as OS emitidas.

9.4. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

9.5. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal quanto à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

9.6. O prazo para a solução, pelo Contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

9.7. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança dos bens nem a responsabilidade ético-profissional pela perfeita execução do contrato.

9.8. As atividades de montagem, instalação e quaisquer outras necessárias para o funcionamento ou uso do bem correrão por conta do Contratado e são condição para o recebimento do objeto.

Liquidação

9.9. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §3º da Instrução Normativa SEGES/ME nº 77/2022.

9.10. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

9.10.1. o prazo de validade;

9.10.2. a data da emissão;

9.10.3. os dados do contrato e do órgão contratante;

9.10.4. o período respectivo de execução do contrato;

9.10.5. o valor a pagar; e

9.10.6. eventual destaque do valor de retenções tributárias cabíveis.

9.11. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o Contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao Contratante;

9.12. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

9.13. A Administração deverá realizar consulta ao SICAF para:

9.13.1. verificar a manutenção das condições de habilitação exigidas;

9.13.2. identificar possível razão que impeça a participação em licitação/contratação no âmbito do órgão ou entidade, tais como a proibição de contratar com a Administração ou com o Poder Público, bem como ocorrências impeditivas indiretas.

9.14. Constatando-se, junto ao SICAF, a situação de irregularidade do Contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do Contratante.

9.15. Não havendo regularização ou sendo a defesa considerada improcedente, o Contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do Contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

9.16. Persistindo a irregularidade, o Contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao Contratado a ampla defesa, segundo o devido processo legal.

9.17. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o Contratado não regularize sua situação junto ao SICAF.

Prazo de pagamento

9.18. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

9.19. No caso de atraso pelo Contratante, os valores devidos ao Contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do Índice Nacional de Preços ao Consumidor Amplo (IPCA) de correção monetária.

Forma de pagamento

9.20. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo Contratado.

9.21. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

9.22. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

9.23. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

9.24. O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

Antecipação de pagamento

9.25. Não será admitida antecipação de pagamento.

Cessão de Crédito

9.26. As cessões de crédito dependerão de prévia aprovação do Contratante.

9.26.1. A eficácia da cessão de crédito, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

9.26.2. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do Contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 8.429, de 1992, nos termos do Parecer JL-01, de 18 de maio de 2020.

9.26.3. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (Contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração.

9.26.4. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do Contratado.[]

9.27. O disposto nesta seção não afeta as operações de crédito de que trata a Instrução Normativa SEGES/MGI nº 82, de 21 de fevereiro de 2025, as quais ficam por esta regidas.

Reajuste

9.28. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em 28/10/2025.

9.29. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

9.30. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

9.31. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o Contratante pagará ao Contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

9.32. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

9.33. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

9.34. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

9.35. O reajuste será realizado por apostilamento.

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E FORMA DE FORNECIMENTO

Forma de seleção e critério de julgamento da proposta

10.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA por Sistema de Registro de Preços, com adoção do critério de julgamento pelo MENOR PREÇO.

Forma de fornecimento

10.2. O fornecimento do objeto será integral, de acordo com a demanda solicitada pelo Contratante.

Critérios de aceitabilidade de preços

10.3. Por se tratar de contratação para registro de preços, com o critério de julgamento de menor preço, o critério de aceitabilidade de preços unitários máximos será:

10.3.1. Valor total por grupo de itens: conforme tabela constante no item 1.1 deste Termo de Referência.

Exigências de habilitação

10.4. Para fins de habilitação, deverá o interessado comprovar os seguintes requisitos:

Habilitação jurídica

10.5. pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

10.6. empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

10.7. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;

10.8. sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

10.9. sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020;

10.10. sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

10.11. filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

10.12. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

10.13. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

10.14. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional;

10.15. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

10.16. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

10.17. Prova de inscrição no cadastro de contribuintes Estadual ou Distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

10.18. Prova de regularidade com a Fazenda Estadual ou Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

10.19. Caso o fornecedor seja considerado isento dos tributos relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

10.20. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

10.21. certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do interessado, caso se trate de pessoa física, desde que admitida a sua participação na licitação/contratação, ou de sociedade simples;

10.22. certidão negativa de falência expedida pelo distribuidor da sede do fornecedor;

10.23. balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos dois últimos exercícios sociais, já exigíveis e apresentados na forma da lei, comprovando, índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um), obtidos por meio da aplicação das seguintes fórmulas:

LG =	Ativo Circulante + Realizável a Longo Prazo
	Passivo Circulante + Passivo Não Circulante

SG =	Ativo Total
	Passivo Circulante + Passivo Não Circulante

LC =	Ativo Circulante
	Passivo Circulante

10.24. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação capital mínimo de 10% do valor total estimado da contratação.

10.25. Os indicadores fixados acima deverão ser atingidos em cada um dos dois últimos exercícios sociais, sob pena de inabilitação.

10.26. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos;

10.27. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

10.28. As empresas criadas no exercício financeiro da licitação/contratação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.

10.29. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

Qualificação Técnica

10.30. Embora os itens de maior relevância e valor consistam no fornecimento de equipamentos cuja garantia será contratada diretamente pelo fornecedor junto ao fabricante, a equipe técnica considera necessária a comprovação de um quantitativo mínimo de capacidade técnica para a adequada execução do objeto. Tal exigência justifica-se por se tratar de uma solução de hiperconvergência de alta complexidade, dimensionada para as necessidades específicas da AGU, envolvendo elevada capacidade de hardware e funcionalidades avançadas de HCI.

10.30.1. Serão admitidos, para fins de comprovação de quantitativo mínimo exigido, a apresentação e o somatório de diferentes atestados relativos a contratos executados de forma concomitante.

10.31. Dessa forma, para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

10.31.1. Apresentar atestado de capacidade técnica, expedido por pessoa jurídica de direito público ou privado, declarando que a empresa LICITANTE executou ou executa, a contento, o fornecimento de solução de infraestrutura convergente ou similar em complexidade tecnológica, envolvendo processamento, armazenamento e recursos de virtualização integrados. O atestado deverá demonstrar experiência na execução de objeto de capacidade compatível com o desta contratação, admitindo-se, para fins quantitativos, a execução mínima de:

a) 1 (um) cluster de 3 (três) nós, desde que aceito pela área técnica, incluindo, obrigatoriamente, o fornecimento prévio de solução com, no mínimo, 38 (trinta e oito) núcleos físicos, equivalentes a aproximadamente 20% do total de 192 núcleos físicos previstos para um Appliance do item 01 (Appliance para Solução de Hiperconvergência).

b) 1 (um) cluster de 3 (três) nós ou solução de armazenamento de alta disponibilidade, desde que aceito pela área técnica, incluindo, obrigatoriamente, o fornecimento prévio de solução com, no mínimo, 63 TB, de capacidade de armazenamento bruta, equivalentes a 20% de 315 TB, previstos no item 02 (Armazenamento Unificado de Arquivos e Objetos).

10.32. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

10.33. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual do Contratante e local em que foram prestados os serviços, entre outros documentos.

10.34. Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

10.35. Serão aceitos atestados ou outros documentos hábeis emitidos por entidades estrangeiras quando acompanhados de tradução para o português, salvo se comprovada a inidoneidade da entidade emissora.

10.36. A apresentação, pelo fornecedor, de certidões ou atestados de desempenho anterior emitido em favor de consórcio do qual tenha feito parte será admitida, desde que atendidos os requisitos do art. 67, §§ 10 e 11, da Lei nº 14.133/2021 e regulamentos sobre o tema.

Disposições gerais sobre habilitação

10.37. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

10.38. Na hipótese de o fornecedor ser empresa estrangeira que não funcione no País, para assinatura do contrato ou da ata de registro de preços ou do aceite do instrumento equivalente, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

10.39. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

10.40. Se o fornecedor for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

10.41. Serão aceitos registros de CNPJ de fornecedor matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O custo estimado total da contratação, que corresponde ao valor máximo aceitável, é de **R\$ 18.727.137,24** (dezoito milhões, setecentos e vinte e sete mil, cento e trinta e sete reais e vinte e quatro centavos), conforme custos unitários apostos na tabela contida no item 1.1 desde Termo de Referência.

11.2. O custo estimado da contratação não possui caráter sigiloso.

11.3. A estimativa de custo levou em consideração o risco envolvido na contratação e sua alocação entre Contratante e Contratado, conforme especificado na matriz de risco constante do Contrato.

11.4. Em caso de Registro de Preços, os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:

- 11.4.1. em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos do disposto na alínea “d” do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;
- 11.4.2. em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;
- 11.4.3. serão reajustados os preços registrados, respeitada a contagem da anualidade e o índice previsto para a contratação.

12. ADEQUAÇÃO ORÇAMENTÁRIA

12.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

12.2. A contratação será atendida pela seguinte dotação:

- I) Gestão/unidade: 00001/110792;
- II) Fonte de recursos: 0100000000 - Tesouro Nacional;
- III) Programa de trabalho: 02.061.2031.21B5.0001 - Modernização da Infraestrutura de TI;
- IV) Elemento de despesa:
 - 44.90.52 - Equipamentos e Material Permanente;
 - 33.90.40 - Instalação.
- V) Plano interno: AGU0015;

12.3. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

Cronograma Físico Financeiro

12.4. O pagamento será efetuado em moeda corrente nacional, condicionado a um cronograma físico-financeiro atrelado à execução das atividades e entregas, da seguinte forma:

12.5. Será realizado o pagamento do valor correspondente ao Item solicitado em OFB/OS, após a emissão do respectivo Termo de Recebimento Definitivo pela Fiscalização, conforme critérios de aceitação estabelecidos neste Termo de Referência.

--	--	--	--

Descrição	Periodicidade	Natureza	Condições de Pagamento
Itens 1 e 2	Parcela única	Investimento	Pagamento mediante OS/OFB e emissão de Termo de Recebimento Definitivo.
Itens 3 e 4	Parcela única	Custeio	Pagamento mediante OS/OFB e emissão de Termo de Recebimento Definitivo.

13. DISPOSIÇÕES FINAIS

13.1. As informações contidas neste Termo de Referência não são classificadas como sigilosas.

UENDEL DA SILVA TAVARES	THIAGO DE SOUSA MARTINS	MARLON FRITZ MARTINS LEITE
Integrante Requisitante	Integrante Técnico	Integrante Administrativo

Autoridade Máxima da Área de TIC
ÁLVARO DA COSTA RONDON NETO Diretor de Tecnologia da Informação

Aprovo,

Autoridade Competente
ELISA MONTEIRO MALAFAIA

14. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

UENDEL DA SILVA TAVARES

Integrante Requisitante



Assinou eletronicamente em 17/04/2026 às 16:06:37.

THIAGO DE SOUSA MARTINS

Integrante Técnico



Assinou eletronicamente em 17/04/2026 às 15:58:54.

MARLON FRITZ MARTINS LEITE

Integrante Administrativo

ALVARO DA COSTA RONDON NETO

Autoridade Máxima da Área de TIC



Assinou eletronicamente em 17/04/2026 às 15:52:29.

Despacho: Aprovo.

ELISA MONTEIRO MALAFAIA

Autoridade Competente

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - ANEXO I - Requisitos Tecnicos da Solucao_VFinal.pdf (214.12 KB)
- Anexo II - Anexo II - Modelo Proposta de Precos (1).pdf (140.29 KB)
- Anexo III - ANEXO III - Planilha Ponto-a-Ponto_HCI.pdf (194.8 KB)
- Anexo IV - ANEXO IV - Plano_Implantacao_HCI_Area Tecnica - VFinal.pdf (332.4 KB)
- Anexo V - ANEXO V - Termo de Compromisso de Manutencao do Sigilo.pdf (140.66 KB)
- Anexo VI - ANEXO VI - Declaracao de Vistoria.pdf (83.96 KB)
- Anexo VII - ANEXO VII - Declaracao de Recusa de Vistoria.pdf (83.32 KB)
- Anexo VIII - Anexo VIII- Modelo de Ordem de Servico.pdf (123.08 KB)
- Anexo IX - Anexo IX - Termo de Recebimento Provisorio - Servicos TIC.pdf (106.02 KB)
- Anexo X - Anexo X - Termo de Recebimento Definitivo.pdf (127.62 KB)
- Anexo XI - Anexo XI - Termo de Ciencia.pdf (77.86 KB)
- Anexo XII - Anexo XII - Termo de Encerramento do Contrato.pdf (106.22 KB)

ANEXO I

REQUISITOS TÉCNICOS DA SOLUÇÃO

1. Appliance para Nuvem Privada

1.1. Deve ser fornecido 6 (seis) equipamentos do tipo servidor físico (appliance/nó para nuvem privada), com possibilidade de expansão e, no mínimo, a seguinte configuração bruta cada:

1.1.1. Deve ser fornecido com 2 (dois) processadores físicos padrão x86. Cada processador deve possuir, no mínimo, 32 (trinta e dois) núcleos físicos. Referência: Intel Xeon Gold 6548Y+ ou superior. Para fins de referência, considerar-se-á superior o processador que contenha ao menos o número especificado de núcleos e “Single Thread Rating” superior ao do processador de referência no site www.cpubenchmark.net.

1.1.2. Deve ser fornecido com 1.536GB (um mil quinhentos e trinta e seis gigabytes) de memória RAM.

1.1.3. Deve ser fornecido com dispositivo (ou um conjunto de dispositivos) de armazenamento de alto desempenho, com no mínimo 92,16TB (noventa e dois virgula dezesseis terabytes) brutos, compostos por pelo menos 6 SSDs do tipo NVMe. Se houver necessidade de licenciamento para utilizar a capacidade total do armazenamento, este deverá ser incluído e fornecido junto com o equipamento.

1.1.4. Deve possuir 2 (duas) placas adaptadoras de rede, cada uma com 2 (duas) portas 25GbE do tipo SFP28.

1.1.5. Deve acompanhar 2 (dois) transceivers compatíveis com os servidores fornecidos e também outros 2 (dois) transceivers compatíveis com Switches Fortinet (FN-TRAN-SFP28-SR), todos no padrão 25GBASE-SR para 25Gbps full-duplex;

1.1.6. Deve acompanhar 2 (dois) cordões ópticos de 15 metros do tipo multimodo OM4 50/125 duplex com conectores LC/LC;

1.1.7. Deve acompanhar 1 (um) Patch Cord UTP Cat6A de no mínimo 2,5m (dois metros e meio) e 1 (uma) interface 1000BASE-T compatível com os serviços de conectividade ofertados.

1.1.8. A depender dos acréscimos especificados nos itens subsequentes, a configuração do servidor será alterada. Nesse caso, será aceita a utilização de equipamentos com maior capacidade, desde que do mesmo fabricante e linha de produtos ofertada e que esses equipamentos permitam formar um cluster entre si.

1.1.9. No caso de projetos de múltiplos nós, se a configuração for compatível com plataformas de hardware que suportam múltiplos nós por chassi, o serviço deverá ser fornecido com tantos nós quando possível no mesmo chassi, a fim de oportunizar espaço.

1.2. Cada appliance deve ser fornecido com no mínimo a seguinte configuração de software:

1.2.1. As especificações a seguir visam apresentar os requisitos necessários e funcionalidades para o software para nuvem privada e demais funções necessárias para atendimento do projeto. Visando mitigar os esforços dispendidos no desenvolvimento de integrações, é preferível que as licitantes proponentes optem por fornecer uma solução única, entretanto, considerando a especificidades de algumas características e visando a liberdade de oferta ao certame, será admitido, para as funcionalidades expressamente indicadas, a junção de múltiplas soluções para integração entre si, com objetivo de atendimento igualitário ao de uma solução única. Caso seja realizado por integração com soluções de parceiros tecnológicos, esta solução deve estar homologada com o fabricante do software para nuvem privada para garantir total integração entre as soluções e fabricantes, sendo que essas informações de compatibilidade entre as soluções devem estar publicadas no site oficial de ambos os fabricantes ou caberão aos fabricantes selecionados pela licitante emitirem carta de conformidade em nome da comissão de licitação deste processo concorrencial, citando o número do processo e data, devidamente assinada pelo responsável técnico a nível nacional, citando o nome da licitante proponente, descrevendo o nome do produto ofertado, e expressando quais ações de integração serão realizadas com outras soluções, assumindo o compromisso de compatibilidade, visando o correto funcionamento e garantindo que a proponente apta para atender estes requisitos por meio de compatibilidade total e completa entre todos os produtos. Não serão aceitas soluções ou funcionalidades implementadas via software ainda em fase de desenvolvimento, ou seja, aquelas que ainda não foram homologadas pelo fabricante para ambiente de produção.

1.2.2. O serviço deve suportar uma infraestrutura computacional para nuvem privada de alta disponibilidade em configuração de cluster para ambiente de virtualização partindo de pelo menos 03 (três) nós (appliance/hardware físico), cada qual com sua respectiva capacidade de processamento, armazenamento, comunicação de rede.

1.2.3. Conforme disposto no inciso V do artigo 40 da lei 14.133, de 01 de abril de 2021, tanto os hardwares quanto os softwares desta solução deverão ser fornecidos por um único fabricante, o qual será responsável também, pelo suporte e garantia da plataforma como um todo ou fornecido hardware (servidores) que sejam homologados em formato OEM pelo fabricante da solução, desde que, o suporte seja unificado e prestado pelo fabricante, não sendo aceito por empresas parceiras e/ou licitantes.

1.2.4. O software hiperconvergente deve incorporar segurança em conformidade com padrões governamentais e internacionais de segurança e privacidade: NIST SP800-53, FIPS 140-2, Common Criteria EAL2+, constar na lista de produtos aprovados pela rede de informação do Departamento de Defesa norte americano (DoDIN APL), além de permitir o emprego de configurações baseadas no Guia de Implementação Técnica de Segurança (STIG) da Agência de Sistemas de Informação do Departamento de Defesa dos EUA (DISA).

1.2.5. Tanto para cluster com dados, como para cluster vazio, a solução deverá permitir configurar criptografia de dados durante a ingestão (inline) ou após a gravação na camada de armazenamento (data-at-rest encryption) com gerenciador de chaves (KMS), local ou externo (sem ponto único de falha em ambos os cenários), que suporte a troca da chave mestre de criptografia em períodos arbitrários para aumento de segurança, para que os dados sejam inacessíveis em caso de roubo de um disco ou equipamento. Caso a solução dependa exclusivamente de um serviço externo para gerenciamento de chaves criptográficas, este deverá ser fornecido sem ponto único de falha juntamente com a solução. Caso esta funcionalidade requeira licenciamento de software ou componentes de hardware adicionais, estes deverão ser fornecidos com a solução garantindo a redundância entre os sites do CONTRATANTE.

1.2.6. Permitir a realização de snapshots através do SDS com consistência para os dados da aplicação (application-consistent), tanto para VMs com sistema operacional Linux como para VMs com sistema operacional Windows, através de tecnologia VSS e semelhantes.

1.2.7. Permitir que o próprio administrador da máquina virtual realize a recuperação granular de arquivos sem a necessidade de envolvimento da equipe responsável pela gestão das cópias de segurança (backup).

1.2.8. Deve suportar escalabilidade horizontal de 32 (trinta e dois) nós por cluster, isso é, a adição de novos nós ao cluster com gerenciamento através de uma console gráfica, sem a parada do ambiente de produção, aumentando como um todo a capacidade de armazenamento, processamento e memória disponibilizados ao Hypervisor. Deve ser permitida a inclusão futura de novos equipamentos, mesmo que de gerações e configurações diferentes ao cluster implantado.

1.2.9. Deve possuir capacidade para realizar snapshots granulares em nível de máquina virtual (VM) para permitir a proteção de dados abrangendo todos os discos virtuais. Além disso, deve haver a capacidade de criar clones de snapshots de VM para testes de software, bem como suporte para recuperação granular de nível de arquivo diretamente da VM, com o mínimo de intervenção nas operações de infraestrutura.

1.2.10. Deve possuir capacidade de manter múltiplas cópias dos dados em diferentes locais. No caso de um cluster formado pelo menos por 3 (três) nós, a solução deve possibilitar 2 (duas cópias) de dados em nós distintos do cluster para garantir tolerância de falha em até 1 (um) nó. E no caso de um cluster

formado pelo menos por 5 (cinco) nós, a solução deve possibilitar até 3 (três cópias) de dados em nós distintos do cluster para garantir tolerância de falha em até 2(dois) nós.

1.2.11. No caso de aquisições de múltiplos nós, se a configuração for compatível com plataformas de hardware que suportam múltiplos nós por chassi, o serviço deverá ser fornecido com tantos nós quando possível no mesmo chassi, a fim de oportunizar espaço.

1.2.12. Deve possuir capacidade para criar cópias redundantes de dados e distribuí-las em nós que não compartilham o mesmo bloco. Além disso, deve ser capaz de manter as máquinas virtuais operando mesmo após uma falha em um bloco, devido à existência de cópias redundantes de dados e metadados em outros blocos.

1.2.13. Deve possuir capacidade para criar cópias redundantes de dados e distribuí-las em nós que não compartilham o mesmo rack. A redundância de dados deve ser assegurada em situações de falhas, como a falha de todas as fontes de alimentação em um rack, a falha de um switch top-of-rack (TOR), ou a ocorrência de uma partição de rede que torne um rack inacessível a partir de outros racks. Além disso, deve ser capaz de manter a operação contínua de máquinas virtuais, mesmo na falha de um rack ou na falha de dois racks, garantindo que as cópias redundantes dos dados e metadados das máquinas virtuais estejam disponíveis em outros racks quando ocorrer a falha de um rack.

1.2.14. Deve possuir funcionalidade de compressão de dados após a escrita (com a flexibilidade de ajustar o tempo de atraso) e compressão inline aos appliances ofertados.

1.2.15. Deve possuir deduplicação de cache para otimização de desempenho aos appliances ofertados, bem como a possibilidade de ativar a deduplicação de capacidade para dados persistentes, visando a redução do uso de armazenamento em disco rígido.

1.2.16. Deve permitir a configuração de diferentes combinações de compressão e deduplicação para diferentes cargas de trabalho (storage profiles, storage containers, entre outros).

1.2.17. Para permitir um melhor aproveitamento dos recursos de armazenamento do cluster, deve suportar método de proteção de dados Erasure Coding, no qual os dados são divididos em fragmentos, estendidos e codificados com pedaços de dados redundantes e armazenados em diferentes nós.

1.2.18. Caso a solução ofertada não possua funcionalidades para otimização de armazenamento, como compressão, deduplicação e erasure coding, o licitante deverá fornecer 60% a mais de dispositivos de armazenamento em sua proposta comercial, garantindo assim a capacidade necessária para atender às demandas de armazenamento.

1.2.19. Deve permitir adição de nós que incrementem apenas o armazenamento do cluster de forma independente do processamento e memória.

1.2.20. No caso de movimentação de VMs (máquinas virtuais) entre os nós do cluster, a solução deve manter os dados das máquinas virtuais no armazenamento local do próprio nó, além disso os dados devem ser movidos, caso necessário, em segundo plano, para esse novo servidor, buscando o melhor desempenho possível através do acesso local ao dado.

1.2.21. Deve possuir funcionalidade para expor recursos de armazenamento diretamente para sistemas operacionais virtualizados e hosts físicos utilizando o protocolo iSCSI.

1.2.22. Deve ser fornecido serviço de armazenamento de objetos com no mínimo as seguintes características:

1.2.22.1. Deve ser compatível com a API REST do Amazon Web Services Simple Storage Service (AWS S3).

1.2.22.2. Deve possuir a capacidade de criar ""buckets"" com políticas WORM, que impeçam a modificação ou exclusão de dados enquanto a política estiver ativa.

1.2.22.3. Os dados armazenados na solução, especialmente aqueles sob políticas WORM, devem ser imutáveis e não podem ser alterados ou excluídos.

1.2.22.4. Deve oferecer suporte ao versionamento de objetos, permitindo que múltiplas versões de um mesmo objeto sejam mantidas. As versões mais antigas não devem ser sobrescritas.

1.2.22.5. Deve permitir a definição de políticas de retenção baseadas na idade dos dados para cumprir regulamentações específicas, além disso deve ser possível definir quando os dados serão excluídos automaticamente.

1.2.22.6. Deve permitir a divisão de grandes conjuntos de dados em partes menores para aumentar a eficiência no processo de upload e facilitar a retomada de uploads interrompidos.

1.2.22.7. Deve oferecer recursos de gerenciamento de identidade e acesso, permitindo o controle granular sobre quem pode acessar os "buckets" e objetos. Deve ser possível revogar e regenerar chaves de acesso conforme necessário.

1.2.22.8. Deve oferecer suporte para a criação de "buckets" usando protocolos S3 e NFS. O suporte ao protocolo NFS deve ser nativamente implementado e interoperável com o protocolo S3.

1.2.22.9. Deve ser ofertado o licenciamento para prover pelo menos 1TB de armazenamento de objetos para cada appliance adquirido. Caso a solução exija um appliance externo para oferecer essa funcionalidade, o licitante deve fornecer este appliance de forma redundante na proposta comercial, garantindo alta disponibilidade e resiliência.

1.2.23. Deve ser fornecido serviços de armazenamento de arquivos com características específicas para atender às necessidades de armazenamento de dados não estruturados, incluindo home directories, perfis de usuário, compartilhamento de departamentos, dados de aplicativos, logs de aplicativos, backups e arquivos de arquivo com no mínimo as seguintes características:

1.2.23.1. Deve ser uma solução de armazenamento definida por software, escalável e integrada infraestrutura computacional ofertada. Deve ser capaz de fornecer alta disponibilidade, resiliência de dados e recuperação de desastres.

1.2.23.2. Deve oferecer suporte aos protocolos SMB e NFS para clientes e servidores.

1.2.23.3. Deve ser integrada com o Active Directory para fornecer autenticação, enumeração baseada em acesso, quotas e a capacidade de auto-recuperação de versões anteriores de arquivos (Windows Previous Versions).

1.2.23.4. Deve ser compatível com ambientes de virtualização ofertado.

1.2.23.5. Deve suportar técnicas de eficiência de dados, incluindo Erasure Coding e compressão.

1.2.23.6. Deve ser capaz de fornecer relatórios detalhados sobre o uso de armazenamento, capacidade, idade de dados e atividades de arquivo.

1.2.23.7. Deve oferecer recursos avançados de análise de arquivos e auditoria para melhorar a visibilidade e a segurança dos dados armazenados.

1.2.23.8. Deve incluir uma ferramenta de análise de arquivos que forneça os seguintes recursos:

1.2.23.8.1. Tendência de capacidade de armazenamento.

1.2.23.8.2. Relatório dos principais usuários ativos.

1.2.23.8.3. Relatório dos principais arquivos acessados.

1.2.23.8.4. Análise de idade de dados.

1.2.23.8.5. Distribuição de arquivos por tamanho.

1.2.23.8.6. Distribuição de arquivos por tipo.

1.2.23.8.7. Detecção de anomalias, incluindo eventos que excedem limites definidos.

1.2.23.8.8. Registro de permissões negadas.

1.2.23.9. Deve incluir uma funcionalidade de análise de idade de dados que permita aos administradores visualizarem com que frequência os usuários acessam os dados ao longo do tempo. Os intervalos de idade dos dados devem ser personalizáveis, e a solução deve mostrar o crescimento percentual em cada categoria.

1.2.23.10. Deve oferecer capacidades avançadas de auditoria de trilhas que permitam aos administradores pesquisarem atividades de arquivos específicos por usuário, tipo de operação e horário. Deve ser possível filtrar e exportar essas informações para fins de relatório.

1.2.23.11. Deve permitir a definição de alertas de anomalias para operações específicas executadas por usuários ou no servidor de arquivos como um todo. Os eventos de anomalias devem ser configuráveis em termos de tipos de eventos, porcentagem de operações e contagem de operações. Também deve ser possível especificar os destinatários de notificações por e-mail para eventos de anomalias.

1.2.23.12. Deve ser capaz de bloquear a criação e a renomeação de arquivos com extensões específicas. Deve ser possível definir políticas de bloqueio de arquivos com base em extensões de arquivo e nomes de arquivo usando curingas. A solução deve incluir uma lista de extensões de arquivo conhecidas de ransomware e bloquear automaticamente qualquer tentativa de criação ou renomeação de arquivos com essas extensões.

1.2.23.13. Deve ser ofertado o licenciamento para prover pelo menos 1TB para armazenamento de arquivos para cada appliance adquirido. Caso a solução exija um appliance ex-terno para oferecer essa funcionalidade, o licitante deve fornecer este appliance de forma redundante na proposta comercial, garantindo alta disponibilidade e resiliência.

1.2.24. Deve possuir opções de agendamento de replicação de dados para Disaster Recovery (DR), com base em categorias de RPO (Recovery Point Objective) com no mínimo as seguintes características:

1.2.24.1. Agendamento síncrono, com RPO zero, deve realizar replicação de dados em tempo real entre dois locais em uma configuração de disponibilidade metropolitana (Stretched Cluster/ Metro).

1.2.24.2. Agendamento próximo de síncrono com RPO entre 1 (um) e 15 (quinze) minutos.

1.2.24.3. Agendamento assíncrono, com RPO de 60 minutos ou superior, que podem utilizar snapshots completos e permitem configurações em termos de horas, dias, semanas e meses.

1.2.25. Deve possuir a funcionalidade, sem nenhuma limitação de licenciamento em o número VMs protegidas, para plano de recuperação que possa orquestrar a restauração de grupos de proteção (entidades protegidas) em um site de recuperação (zona de recuperação) com no mínimo as seguintes características:

1.2.25.1. Deve consistir em procedimentos pré-definidos que garantam a recuperação eficiente das entidades no cluster de recuperação, com a capacidade de especificar estágios de reinício para máquinas virtuais e atrasos entre esses estágios.

1.2.25.2. Deve permitir a sincronização bidirecional entre zonas de recuperação e a possibilidade de retornar à zona primária usando o mesmo plano.

1.2.25.3. Deve permitir a criação de planos de recuperação que possam ser validados e testados para garantir que o sistema possa se recuperar em caso de failover.

1.2.25.4. Caso o licenciamento para esta funcionalidade seja determinado pelo número de máquinas virtuais, deverá ser considerado o mínimo de 100 (cem) máquinas virtuais por equipamento ou host pertencente ao cluster.

1.2.26. Deve implementar a autenticação de clientes possibilitando o acesso seguro através da troca de um certificado digital. Além disso deve validar que o certificado seja assinado por uma Autoridade Certificadora (CA) confiável.

1.2.27. Deve oferecer um recurso que permita reforçar a segurança e restringir o acesso não autorizado à solução de infraestrutura computacional, no qual deve desativar a autenticação por senha para SSH e deve ser restrito a usuários autenticados com base em chaves públicas, onde apenas usuários com credenciais de chave pública autorizadas devem ter permissão para acessar recursos do sistema.

1.2.28. Deve ser fornecido hypervisor, plenamente licenciado, para permitir a abstração de aplicativos do hardware subjacente, viabilizando o provisionamento, atualização e gerenciamento escalável de Máquinas Virtuais (VMs). Além disso, deve possibilitar um modelo operacional consistente em ambientes híbridos, abrangendo nuvem privada (data centers) e suporte nuvens públicas.

1.2.29. Com o objetivo de aprimorar a eficiência operacional oferecer maior escalabilidade de desempenho, a solução deve implementar uma abordagem de múltiplas filas (multi-queue) para otimizar a transferência de dados entre máquinas virtuais e o armazenamento, resultando em um aumento substancial na capacidade de E/S e uma redução significativa na utilização da CPU. Além disso, as filas de armazenamento devem ser ajustadas automaticamente de acordo com o número de vCPUs configuradas para cada máquina virtual, garantindo um desempenho superior à medida que a carga de trabalho se expande.

1.2.30. Deve implementar recurso de segurança Windows Defender Credential Guard em máquinas virtuais Windows, isolando de forma segura as credenciais de usuário do restante do sistema operacional.

1.2.31. O cluster deve suportar appliances com Unidades de Processamento Gráfico (GPU), permitindo a instalação de placas de GPU físicas em appliances de nuvem privada e a atribuição a máquinas virtuais (VMs) em modo de passagem direta (GPU Passthrough) e por meio de alocação virtual de GPU (vGPU).

1.2.32. Deve possuir funcionalidade para alta disponibilidade para máquinas virtuais para garantir a reinicialização das VMs em um nó (host) alternativo no cluster, em caso de falha no nó (host) original devido a falha completa, isolamento de rede ou falha nos processos de gerenciamento. Além disso, deve possibilitar a reserva espaço em todos os hosts do cluster para garantir que todas as VMs possam reiniciar em outros hosts em caso de falha, com a opção de ativar a reserva de alta disponibilidade.

1.2.33. Deve ser fornecido serviço para gerenciamento de Kubernetes básico com no mínimo as seguintes características:

1.2.33.1. Deve permitir o provisionamento, operações e gerenciamento de ciclo de vida de clusters Kubernetes.

1.2.33.2. Deve suportar o gerenciamento do ciclo de vida de workload clusters.

1.2.33.3. Deve possuir múltiplas formas de criação de clusters de workload, incluindo uma interface gráfica amigável (UI), comandos de linha (CLI) e definições YAML.

1.2.33.4. Deve integrar o login unificado (Single Sign On) para autenticação de usuários, permitindo uma experiência segura e simplificada para acesso aos clusters Kubernetes.

1.2.33.5. Deve possuir controle baseado em funções (RBAC - Role-Based Access Control) deve permitir a criação e gestão de permissões específicas para administradores, restringindo o acesso a apenas os recursos e funcionalidades necessárias.

1.2.33.6. Deve suportar ambientes isolados (air-gapped), permitindo a instalação, configuração e operação de clusters Kubernetes sem a necessidade de conexão à internet.

1.2.33.7. Deve permitir a implementação de mecanismos de balanceamento de carga para distribuir automaticamente o tráfego de rede entre os nós do cluster.

1.2.33.8. Deve fornecer suporte completo ao Container Storage Interface (CSI), permitindo que os orquestradores de contêineres como o Kubernetes interajam de maneira eficiente com os subsistemas de armazenamento, abstraindo a complexidade do provisionamento e gestão de volumes de armazenamento.

1.2.34. Deve possuir funcionalidade para configurar políticas de afinidade e anti-afinidade para gerenciar o posicionamento de máquinas virtuais (VMs) em um ambiente de virtualização, onde, a política de afinidade VM-Host deve permitir a restrição da execução de uma VM específica somente em hosts listados na política de afinidade, proporcionando controle sobre o local de execução da VM durante operações de inicialização ou migração. Por outro lado, a política de anti-afinidade VM-VM deve permitir a separação preferencial de

VMs específicas para garantir que, em caso de problemas com um host, não ocorra a perda simultânea de todas as VMs associadas.

1.2.35. Deve suportar uma experiência de rede contínua e segura, com capacidades de sobreposição, suportando: Virtual LANs, Virtual Private Cloud (VPC), Virtual Private Network (VPN), extensões de rede virtual de Layer 2 usando VPN ou VTEP, e Border Gateway Protocol sessions.

1.2.36. Deve ser fornecido solução de segurança de rede avançado para prover visibilidade na rede virtual, proteção baseada em aplicativos contra ameaças de rede, malware e ransomware, além de monitoramento de segurança e conformidade, com no mínimo as seguintes características:

1.2.36.1. Deve permitir a inspeção de tráfego que tem origem e destino dentro de um data center, eliminando a necessidade de firewalls leste-oeste adicionais dentro do data center.

1.2.36.2. Deve possuir funcionalidade para garantir que apenas o tráfego permitido entre camadas de aplicativos ou outras fronteiras lógicas seja autorizado, protegendo contra ameaças avançadas na virtualização.

1.2.36.3. Deve possuir uma visualização detalhada das comunicações entre VMs, facilitando a categorização e agrupamento das cargas de trabalho para estabelecer políticas apropriadas.

1.2.36.4. Deve possuir capacidade para configurar políticas de rede associadas a cargas de trabalho (como VMs, aplicações ou vNICs específicas), ou a grupos lógicos de entidades (como Grupos de Entidades ou VPCs categorizadas).

1.2.36.5. As políticas de segurança devem ser aplicadas a categorias (grupo lógico de VMs) para garantir que o tráfego associado às VMs na categoria é protegido automaticamente, sem intervenção administrativa.

1.2.36.6. Deve possuir políticas de quarentena para isolar uma VM comprometida ou infectada e, opcionalmente, sujeitá-la a processos forenses.

1.2.36.7. Deve possuir políticas de isolamento para bloquear todo o tráfego, independentemente da direção, entre dois grupos de VMs identificados por sua categoria.

1.2.36.8. Deve possuir políticas para proteger uma aplicação especificando fontes e destinos de tráfego permitidos.

1.2.36.9. Deve possuir opção para permitir ou bloquear tráfego IPv6.

1.2.36.10. A solução de segurança de rede deve permitir a criação de políticas de segurança com escopo "Global", abrangendo simultaneamente VMs em VLANs gerenciadas pelo Network Controller e VMs em Virtual Private Clouds (VPCs).

1.2.36.11. A solução deve fornecer capacidade para atribuir políticas de segurança de rede distintas a vNICs específicas dentro da mesma VM, utilizando a categorização de sub-redes.

1.2.36.12. Deve suportar a criação de "Grupos de Entidades" que combinem múltiplos tipos de entidades (como VMs, sub-redes e categorias de VPC) em um único grupo lógico.

1.2.37. Deve possuir API REST que permita a criação de scripts para executar comandos de administração do sistema no cluster, utilizando HTTP requests para obter informações sobre o cluster e efetuar alterações na configuração.

1.2.38. Deve incluir um conjunto de recursos de análise preditiva e automação de suporte, que de-vem oferecer informações sobre a saúde do sistema e identifiquem possíveis problemas com base em dados coletados do cluster. Além disso, esta plataforma de suporte deve, dinamicamente, analisar as configurações do cluster em relação às melhores práticas, fornecendo tendências preditivas, orientações para configurações ideais, práticas recomendadas para aplicativos e suporte automatizado, com a capacidade de identificar lacunas na configuração do cluster que possam afetar a confiabilidade, disponibilidade ou desempenho a longo prazo e tomar ações recomendadas para corrigir essas questões, incluindo a geração automática de casos de suporte em situações graves ou complexas.

1.3. Deve ser fornecido com software para gerenciamento com no mínimo as seguintes características:

1.3.1. As especificações a seguir visam apresentar os requisitos necessários e funcionalidades para a solução de gerenciamento avançado para nuvem privada e demais funções necessárias para atendimento do projeto. Visando mitigar os esforços dispendidos no desenvolvimento de integrações, é preferível que as licitantes proponentes optem por fornecer uma solução única, entretanto, considerando a especificidades de algumas características e visando a liberdade de oferta ao certame, será admitido a junção de múltiplas soluções para integração entre si, com objetivo de atendimento igualitário ao de uma solução única. Caso seja realizado por integração com soluções de parceiros tecnológicos, esta solução deve estar homologada com o fabricante da solução de gerenciamento avançado para nuvem privada para garantir total integração entre as soluções e fabricantes, sendo que essas informações de compatibilidade entre as soluções devem estar publicadas no site oficial de ambos os fabricantes ou caberão aos fabricantes selecionados pela licitante emitirem carta de conformidade em nome da comissão de licitação deste processo concorrencial, citando o número do processo e data, devidamente assinada pelo responsável técnico a nível nacional, citando o nome da licitante proponente, descrevendo o nome do produto ofertado, e expressando quais ações de integração serão realizadas com outras soluções, assumindo o compromisso de compatibilidade, visando o correto funcionamento e garantindo que a proponente apta para atender estes requisitos por meio de compatibilidade

total e completa entre todos os produtos. Não serão aceitas soluções ou funcionalidades implementadas via software ainda em fase de desenvolvimento, ou seja, aquelas que ainda não foram homologadas pelo fabricante para ambiente de produção.

1.3.2. Deve possuir funcionalidade para gerenciamento de relatórios para permitir a configuração e entrega de relatórios históricos contendo informações sobre os recursos de infraestrutura computacional com no mínimo as seguintes características:

1.3.2.1. Deve incluir informações sobre métricas de desempenho, como uso da CPU, uso de memória, largura de banda de E/S, contagem de máquinas virtuais, contagem de hosts, contagem de clusters, resumo de licenças e outros dados relevantes.

1.3.2.2. Deve possuir capacidade de compartilhar relatórios com outros usuários.

1.3.2.3. Deve adicionar diferentes visualizações para personalizar o que é exibido e como os dados são representados.

1.3.2.4. Deve possuir capacidade para agendar a geração de relatórios, com a possibilidade de definir apenas uma programação para cada definição de relatório.

1.3.2.5. Deve possuir capacidade para retenção de relatórios por um período especificado.

1.3.2.6. Deve verificar os detalhes do registro de relatório para obter informações sobre o status do relatório e mensagens de erro, se a geração do relatório falhar.

1.3.2.7. Deve possibilitar a definição da aparência visual do relatório, incluindo opções como cor de fundo, logotipos e outros elementos de design.

1.3.2.8. Deve permitir diferentes formas de representar os dados, incluindo visualizações pré-definidas, personalizáveis e salvas.

1.3.2.9. Deve permitir criar definições de relatório com base em definições de relatórios existentes.

1.3.2.10. Deve exportar e importar configurações de relatório.

1.3.2.11. Deve permitir o download dos relatórios nos formatos PDF e CSV.

1.3.2.12. Deve enviar relatórios por e-mail como anexos nos formatos PDF e CSV.

1.3.3. Deve possuir funcionalidade para realizar a capacidade, previsão e planejamento para recursos de infraestrutura computacional com no mínimo as seguintes características:

1.3.3.1. Deve possuir capacidade para monitorar, calcular, prever e planejar a capacidade de recursos de armazenamento, CPU e memória. Deve ser capaz de registrar o histórico de consumo desses recursos.

1.3.3.2. Deve calcular e apresentar uma representação gráfica do período restante antes que um recurso específico seja completamente consumido.

1.3.3.3. Os cálculos de capacidade devem ser baseados em algoritmos avançados que utilizam dados históricos e continuam a coletar dados para previsões precisas.

1.3.3.4. Deve reter dados de capacidade por um período estendido para análise aprofundada.

1.3.3.5. Deve possuir capacidade para fornecer recursos para o planejamento de recursos da seguinte forma:

1.3.3.5.1. Quando não for possível recuperar recursos suficientes ou quando for necessário expandir o ambiente, deve ser capaz de fazer recomendações com base em nós para atender a um período de capacidade específico.

1.3.3.5.2. Deve permitir a modelagem da adição de novos workloads ao ambiente para avaliar o impacto na capacidade.

1.3.3.5.3. Deve suportar vários tipos de workloads, incluindo: SQL Server, VMs, VDI e variações de porcentagem de crescimento ou redução.

1.3.3.5.4. Deve possuir capacidade para ajustar a capacidade do cluster em tempo real com base na modelagem de novos workloads e fornecer recomendações para a expansão do cluster.

1.3.3.6. Deve possuir capacidade para gerenciar vários clusters e permitir a modelagem da expansão de workloads em diferentes clusters.

1.3.3.7. Deve suportar funcionalidade que, ao modelar um novo workload, seja capaz de analisá-lo em um cluster específico e, se necessário, recomendar a adição de recursos (como nós) a esse mesmo cluster para atender à demanda.

1.3.4. Deve possuir funcionalidade de detecção de ineficiência de recursos e adequação em um ambiente virtualizado com no mínimo os seguintes recursos:

1.3.4.1. Deve possuir capacidade para identificar ineficiências de recursos em VMs e recomendar ações para otimizar o uso de recursos.

1.3.4.2. Deve possuir capacidade para identificar ineficiências de recursos em todo o ambiente virtualizado, bem como em nível de máquina virtual (VM).

1.3.4.3. Deve possuir capacidade para fornecer recomendações para resolver ineficiências globais, seja adicionando capacidade ou recuperando recursos existentes.

1.3.4.4. Deve identificar VMs candidatas para recuperação de recursos não utilizados e fornecer recomendações para devolver esses recursos ao cluster.

1.3.4.5. Deve apresentar as VMs identificadas em categorias de eficiência para facilitar a identificação e a tomada de decisão. As categorias de eficiência devem incluir:

1.3.4.5.1. VMs que estão usando uma quantidade mínima de recursos atribuídos.

1.3.4.5.2. VMs que foram desligadas por um período ou que estão em execução, mas não consomem CPU, memória ou recursos de E/S.

1.3.4.5.3. VMs que poderiam se beneficiar de melhorias de desempenho com recursos adicionais.

1.3.4.5.4. VMs que estão consumindo uma quantidade excessiva de recursos, afetando outras VMs no ambiente.

1.3.4.5.5. Deve apresentar as recomendações de recuperação de recursos em um formato claro e organizado, mostrando a quantidade total de CPU e memória configurada em comparação com os picos de uso de CPU e memória para cada VM.

1.3.5. Deve possuir funcionalidade para permitir aos administradores automatizarem tarefas operacionais rotineiras com no mínimo as seguintes características:

1.3.5.1. Deve permitir aos administradores criarem workflows (playbooks) personalizados, combinando gatilhos e ações a partir de um catálogo fornecido.

1.3.5.2. Deve possuir subscrições de eventos (gatilhos) configuráveis, ou seja, condições que desencadeiam a execução de um workflow automatizado.

1.3.5.3. Deve haver suporte para subscrições de eventos como alerta-based (baseados em alertas do sistema ou definidos pelo usuário) e subscrições de eventos manuais (iniciados explicitamente por administradores).

1.3.5.4. Deve fornecer um catálogo de ações pré-definidas que os administradores podem selecionar para criar seus workflows. As ações devem abranger uma variedade de tarefas operacionais.

1.3.5.5. Os administradores devem ter a capacidade de personalizar ações para realizar procedimentos mais avançados, usando diferentes métodos de código.

1.3.5.6. Deve oferecer uma variedade de ações que podem ser usadas em workflows, incluindo, mas não se limitando a:

1.3.5.6.1. A capacidade de iniciar ou desligar máquinas virtuais.

1.3.5.6.2. A possibilidade de ajustar recursos de CPU e memória de VMs.

1.3.5.6.3. A capacidade de criar um snapshot de uma VM.

1.3.5.6.4. Ação para remover alertas do sistema.

1.3.5.6.5. Ação para enviar notificações, como e-mails, para equipes ou administradores.

1.3.5.6.6. A capacidade de executar código personalizado, incluindo PowerShell, APIs ou CLI, para realizar tarefas específicas.

1.3.5.7. Os workflows devem ser compostos de subscrições de eventos e ações, com a capacidade de incluir várias ações em um fluxo lógico.

1.3.6. Deve suportar a capacidade de monitorar bancos de dados SQL por meio de um método sem agente, estabelecendo conexões com servidores SQL para coletar dados e fornecer insights sobre bancos de dados, consultas e métricas, onde esses dados devem alimentar um mecanismo para detecção de anomalias e aprendizado de comportamento, para permitir a criação de fluxos de trabalho de automação específicos para ambientes Microsoft SQL.

1.3.7. Deve realizar a descoberta de aplicativos, sem agentes, com base em dados IPFIX para identificar VMs e portas de comunicação, além de possuir a capacidade para configurar políticas de descoberta personalizadas com base em assinaturas de portas TCP ou UDP.

1.3.8. Deve possuir funcionalidade baseado em machine learning para fornecer workflows (playbooks) e reduzir a sobrecarga da equipe técnica no qual deve possuir as seguintes características:

1.3.8.1. Deve oferecer aos administradores a capacidade de escolher uma métrica de infraestrutura específica e definir uma faixa de limites ideais para essa métrica, no qual esses limites devem atuar como pontos de referência para o sistema, assegurando o desempenho desejado.

1.3.8.2. Deve oferecer aos administradores a capacidade de especificar um período de monitoramento para o Indicador-Chave de Desempenho (KPI) associado à métrica de infraestrutura escolhida, no qual esse intervalo de tempo deve permitir a observação e avaliação contínua do desempenho da métrica.

1.3.8.3. Deve oferecer aos administradores a capacidade de poder de definir um conjunto de ações predefinidas que o sistema pode executar autonomamente em resposta a desvios na métrica, no qual essas ações devem ser configuradas para garantir que o sistema mantenha um comportamento previsível ao lidar com desvios na métrica de infraestrutura.

1.3.8.4. Deve oferecer aos administradores a capacidade de poder de estabelecer um limite máximo para o número de correções autônomas que o sistema pode realizar antes de exigir intervenção manual, no qual essa salvaguarda deve evitar ajustes automatizados excessivos e mantém o controle dos administradores.

1.3.8.5. Deve avaliar de forma inteligente os parâmetros de infraestrutura, monitorar continuamente a métrica especificada e realizar ações corretivas de forma autônoma para garantir que a métrica permaneça dentro dos limites ideais previamente estabelecidos.

1.3.9. Deve ser fornecida uma solução para governança de custos que permita o gerenciamento de gastos em recursos dos serviços de nuvem privada com no mínimo as seguintes características:

1.3.9.1. Deve refletir os custos real de possuir uma infraestrutura dos serviços de nuvem privada, incluindo: hardware, software, instalações e administração.

1.3.9.2. Deve ser capaz de calcular o custo total de propriedade (TCO), fornecer métricas de custo diárias e mensais, e permitir a criação de relatórios de rateio de custos e alertas de orçamento para fins de governança financeira.

1.3.10. Deve ser fornecida solução de gerenciamento de VMs on-premise e suportar multicloud que possui no mínimo as seguintes características:

1.3.10.1. Deve simplificar a configuração e gerenciamento personalizado por meio de blue-prints que incorporam elementos essenciais, como máquinas virtuais.

1.3.10.2. Deve possibilitar que as equipes de infraestrutura criem blueprints que tornem a implantação e o gerenciamento de VMs comuns repetíveis, eliminando a complexidade das tarefas operacionais.

1.3.10.5. Deve disponibilizar um marketplace com blueprints pré-configurados que as equipes de infraestrutura podem usar para provisionar VMs individuais instantaneamente.

1.3.10.6. Deve oferecer a capacidade de publicar workflows (runbooks) compartilháveis, que são coleções de tarefas executadas sequencialmente.

1.3.10.7. Deve permitir que equipes de infraestrutura definam esses workflows (runbooks) para automatizar tarefas e procedimentos comuns em várias VMs.

1.3.10.8. Deve capacitar grupos na organização a gerenciar suas próprias VMs, oferecendo uma alternativa atrativa aos serviços de nuvem pública.

1.3.11. Deve suportar capacidade para operar em um ambiente de alta disponibilidade a fim de assegurar a continuidade das operações em situações de desastres naturais, falhas de rede ou quedas de energia, permitindo a restauração da infraestrutura central quando necessário.

1.3.12. Deve ser fornecido uma solução de gerenciamento centralizado que permita a monitorização e gestão eficiente de múltiplos clusters por meio de uma única interface web com no mínimo as seguintes características:

1.3.12.1. Deve possuir autenticação única (single sign on) para permitir que os usuários acessem todos os clusters registrados com uma única credencial de login.

1.3.12.2. Deve possuir um painel principal de resumo que abrange todos os clusters e pode ser personalizado de acordo com as necessidades específicas.

1.3.12.3. As visualizações de resumo estão disponíveis para os principais tipos de entidades, com a capacidade de acessar informações detalhadas sobre entidades individuais por meio de opções de detalhamento.

1.3.12.4. Deve possuir resumos de alertas multi-cluster com opções de detalhamento, permitindo que os administradores identifiquem e compreendam problemas em potencial em todos os clusters.

1.3.12.5. Deve possuir capacidade de configurar individualmente os clusters por meio de ações diretas a partir do sistema central ou de um acesso simplificado aos consoles web dos clusters.

1.3.12.6. Deve suportar operações inteligentes, incluindo configuração de rede, segurança, proteção de dados, monitoramento de desempenho, descoberta de aplicativos e gerenciamento de relatórios.

1.3.13. Deve possuir controle de acesso baseado em funções (RBAC) que permita a configuração de permissões de acesso personalizadas para usuários com base em suas funções atribuídas, com no mínimo as seguintes características:

1.3.13.1. Deve suportar funções pré-definidas e a capacidade de criar funções personalizadas.

1.3.13.2. Deve suportar mapeamento de funções para personalizar essas permissões.

1.3.13.3. Deve permitir a atribuição de funções a usuários ou grupos específicos, aplicáveis a conjuntos definidos de entidades.

1.3.13.4. Deve possuir capacidade de atribuir permissões de operação detalhadas para máquinas virtuais (VMs) com base em requisitos específicos, como "Permitir Inicialização de VM" ou "Permitir Desligamento de VM," deve ser oferecida por meio do recurso RBAC Granular, permitindo a criação de funções personalizadas com permissões mais específicas em comparação às categorias de permissões mais abrangentes.

1.3.14. Deve possuir recursos para aprimorar a eficiência e confiabilidade das atualizações de infraestrutura de TI em nuvem privada (datacenter), no qual deve possuir capacidade de determinar dependências de software e firmware, priorizar atualizações de forma inteligente e automatizar todo o processo de atualização em nós(host) agrupados, sem impacto nas aplicações ou disponibilidade de dados. Deve realizar de forma unificada o upgrade para os seguintes itens ofertados: sistema operacional da plataforma de nuvem privada, hypervisor, plataforma para gerenciamento de arquivos, plataforma para gerenciamento de objetos e plataforma para gerenciamento de aplicativos on-premise e multicloud.

1.3.15. Serão aceitas soluções que operem em conjunto com o software para nuvem privada ofertado.

2. Armazenamento Unificado de Arquivos e Objetos

2.1. Deve ser fornecido 1 (um) cluster/grid/conjunto de, no mínimo, 3 (três) equipamentos do tipo servidor físico, com possibilidade de expansão, onde cada um deve ser fornecido com no mínimo a seguinte configuração bruta:

2.1.1. Deve ser fornecido com 2 (dois) processadores físicos padrão x86. Cada processador deve possuir, no mínimo, 32(trinta e dois) núcleos físicos. Referência: Intel Xeon Gold 6548Y+ ou superior. Para fins de referência, considerar-se-á superior o processador que contenha ao menos o número especificado de núcleos e “Single Thread Rating” superior ao do processador de referência no site www.cpubenchmark.net.

2.1.2. Deve ser fornecido com 1024GB (um mil quinhentos e vinte e quatro gigabytes) de memória RAM.

2.1.3. Deve ser fornecido com dispositivo (ou um conjunto de dispositivos) de armazenamento de alto desempenho, com no mínimo 61,44TB (sessenta e um virgula quarenta e quatro tera-bytes) brutos, compostos por pelo menos 4 SSDs do tipo NVMe. Se houver necessidade de licenciamento para utilizar a capacidade total do armazenamento, este deverá ser incluído e fornecido junto com o equipamento.

2.1.4. Deve ser fornecido com dispositivo (ou um conjunto de dispositivos) de armazenamento de capacidade de alto desempenho, com no mínimo 480TB (quatrocentos e oitenta terabytes) brutos, compostos por discos pelo menos 16 SSDs do tipo NVMe. Se houver necessidade de licenciamento para utilizar a capacidade total do armazenamento, este deverá ser incluído e fornecido junto com o equipamento.

2.1.5. Deve possuir 2 (duas) placas adaptadoras de rede, cada uma com 2 (duas) portas 25GbE do tipo SFP28.

2.1.6. Deve acompanhar 2 (dois) transceivers compatíveis com os servidores fornecidos e também outros 2 (dois) transceivers compatíveis com Switches Fortinet (FN-TRAN-SFP28-SR), todos no padrão 25GBASE-SR para 25Gbps full-duplex;

2.1.7. Deve acompanhar 2 (dois) cordões ópticos de 15 metros do tipo multimodo OM4 50/125 duplex com conectores LC/LC;

2.1.8. Deve acompanhar 1 (um) Patch Cord UTP Cat6A de no mínimo 2,5m (dois metros e meio) e 1 (uma) interface 1000BASE-T compatível com os serviços de conectividade ofertados.

2.1.9. A depender dos acréscimos especificados nos itens subsequentes, a configuração do servidor será alterada. Nesse caso, será aceita a utilização de equipamentos com maior capacidade, desde que do mesmo fabricante e linha de produtos ofertada e que esses equipamentos permitam formar um cluster entre si.

2.1.10. No caso de projetos de múltiplos nós, se a configuração for compatível com plataformas de hardware que suportam múltiplos nós por chassi, o serviço deverá ser fornecido com tantos nós quando possível no mesmo chassi, a fim de oportunizar espaço.

2.2. Cada appliance do Armazenamento Unificado de Arquivos e Objetos deve ser fornecido com no mínimo a seguinte configuração de software:

2.2.1. As especificações a seguir visam apresentar os requisitos necessários e funcionalidades para o software do Appliances de Armazenamento Unificado de Arquivos e Objetos e demais funções necessárias para atendimento do projeto. Visando mitigar os esforços dispendidos no desenvolvimento de integrações, é preferível que as licitantes proponentes optem por fornecer uma solução única, entretanto, considerando a especificidades de algumas características e visando a liberdade de oferta ao certame, será admitido, para as funcionalidades expressamente indicadas, a junção de múltiplas soluções para integração entre si, com objetivo de atendimento igualitário ao de uma solução única.

2.2.1.1. Caso seja realizado por integração com soluções de parceiros tecnológicos, esta solução deve estar homologada com o fabricante do software para nuvem privada para garantir total integração entre as soluções e fabricantes, sendo que essas informações de compatibilidade entre as soluções devem estar publicadas no site oficial de ambos os fabricantes ou caberão aos fabricantes selecionados pela licitante emitirem carta de conformidade em nome da comissão de licitação deste processo concorrencial, citando o número do processo e data, devidamente assinada pelo responsável técnico a nível nacional, citando o nome da licitante proponente, descrevendo o nome do produto ofertado, e expressando quais ações de integração serão realizadas com outras soluções, assumindo o compromisso de compatibilidade, visando o correto funcionamento e garantindo que a proponente apta para atender estes requisitos por meio de compatibilidade total e completa entre todos os produtos.

2.2.1.2. Não serão aceitas soluções ou funcionalidades implementadas via software ainda em fase de desenvolvimento, ou seja, aquelas que ainda não foram homologadas pelo fabricante para ambiente de produção.

2.2.2. O serviço deve suportar uma infraestrutura de armazenamento para nuvem privada de alta disponibilidade em configuração de cluster para ambiente de virtualização partindo de pelo menos 03 (três) nós (appliance/hardware físico), cada qual com sua respectiva capacidade de processamento, armazenamento, comunicação de rede.

2.2.3. Conforme disposto no inciso V do artigo 40 da lei 14.133, de 01 de abril de 2021, tanto os hardwares quanto os softwares desta solução deverão ser fornecidos por um único fabricante, o qual será responsável também, pelo suporte e garantia da plataforma como um todo ou fornecido hardware (servidores) que sejam homologados em formato OEM pelo fabricante da solução, desde que, o suporte seja unificado e prestado pelo fabricante, não sendo aceito por empresas parceiras e/ou licitantes.

2.2.4. O software da solução de armazenamento deve incorporar segurança em conformidade com padrões governamentais e internacionais de segurança e privacidade: NIST SP800-53, FIPS 140-2, Common Criteria EAL2+, constar na lista de produtos aprovados pela rede de informação do Departamento de Defesa norte americano (DoDIN APL), além de permitir o emprego de configurações baseadas no Guia de Implementação Técnica de Segurança (STIG) da Agência de Sistemas de Informação do Departamento de Defesa dos EUA (DISA).

2.2.5. Deve suportar escalabilidade horizontal de 32 (trinta e dois) nós por cluster, isso é, a adição de novos nós ao cluster com gerenciamento através de uma console gráfica, sem a parada do ambiente de produção, aumentando como um todo a capacidade de armazenamento, processamento e memória disponibilizados ao Hypervisor. Deve ser permitida a inclusão futura de novos equipamentos, mesmo que de gerações e configurações diferentes ao cluster implantado.

2.2.6. Deve possuir capacidade de manter múltiplas cópias dos dados em diferentes locais. No caso de um cluster formado pelo menos por 3 (três) nós, a solução deve possibilitar 2 (duas cópias) de dados em nós distintos do cluster para garantir tolerância de falha em até 1 (um) nó. E no caso de um cluster formado pelo menos por 5 (cinco) nós, a solução deve possibilitar até 3 (três cópias) de dados em nós distintos do cluster para garantir tolerância de falha em até 2(dois) nós.

2.2.7. Deve possuir funcionalidade de compressão de dados inline aos appliances ofertados.

2.2.8. Deve possuir deduplicação para otimização de desempenho aos appliances ofertados.

2.2.9. Para permitir um melhor aproveitamento dos recursos de armazenamento do cluster, deve suportar método de proteção de dados Erasure Coding, no qual os dados são divididos em fragmentos, estendidos e codificados com pedaços de dados redundantes e armazenados em diferentes nós.

2.2.10. Caso a solução ofertada não possua funcionalidades para otimização de armazenamento, como compressão, deduplicação e erasure coding, o licitante deverá fornecer 60% a mais de dispositivos de armazenamento em sua proposta comercial, garantindo assim a capacidade necessária para atender às demandas de armazenamento.

2.2.11. Deve possuir funcionalidade para expor recursos de armazenamento diretamente para sistemas operacionais virtualizados e hosts físicos utilizando o protocolo iSCSI.

2.2.12. Deve ser fornecido serviço de armazenamento de objetos com no mínimo as seguintes características:

2.2.12.1. Deve ser compatível com a API REST do Amazon Web Services Simple Storage Service (AWS S3).

2.2.12.2. Deve possuir a capacidade de criar ""buckets"" com políticas WORM, que impeçam a modificação ou exclusão de dados enquanto a política estiver ativa.

2.2.12.3. Os dados armazenados na solução, especialmente aqueles sob políticas WORM, devem ser imutáveis e não podem ser alterados ou excluídos.

2.2.12.4. Deve oferecer suporte ao versionamento de objetos, permitindo que múltiplas versões de um mesmo objeto sejam mantidas. As versões mais antigas não devem ser sobrescritas.

2.2.12.5. Deve permitir a definição de políticas de retenção baseadas na idade dos dados para cumprir regulamentações específicas, além disso deve ser possível definir quando os dados serão excluídos automaticamente.

2.2.12.6. Deve permitir a divisão de grandes conjuntos de dados em partes menores para aumentar a eficiência no processo de upload e facilitar a retomada de uploads interrompidos.

2.2.12.7. Deve oferecer recursos de gerenciamento de identidade e acesso, permitindo o controle granular sobre quem pode acessar os "buckets" e objetos. Deve ser possível revogar e regenerar chaves de acesso conforme necessário.

2.2.12.8. Deve oferecer suporte para a criação de "buckets" usando protocolos S3 e NFS. O suporte ao protocolo NFS deve ser nativamente implementado e interoperável com o protocolo S3.

2.2.12.9. Possuir painel de visualização de performance que demonstre a quantidade de requisições por segundo, banda utilizada (MB/s) e tempo de leitura de operação de leitura (GET).

2.2.12.10. Permitir a configuração de serviços de diretórios compatíveis com Microsoft Active Directory e OpenLDAP, para adicionar usuários com acesso aos objetos.

2.2.12.11. A plataforma deve permitir a criação de um namespace único e federado que abranja múltiplas instâncias do serviço de armazenamento de objetos, incluindo aquelas que residem em diferentes localizações geográficas ou diferentes clusters.

2.2.12.12. Deve ser ofertado o licenciamento para prover pelo menos 315TB de armazenamento de objetos ou arquivos em todo o cluster adquirido. Com suporte durante 12 (doze) meses em operação 24x7. Caso a solução exija um appliance externo para oferecer essa funcionalidade, o licitante deve fornecer este appliance de forma redundante na proposta comercial, garantindo alta disponibilidade e resiliência.

2.2.13. Deve ser fornecido serviços de armazenamento de arquivos com características específicas para atender às necessidades de armazenamento de dados não estruturados, incluindo home directories, perfis de usuário, compartilhamento de departamentos, dados de aplicativos, logs de aplicativos, backups e arquivos de arquivo com no mínimo as seguintes características:

2.2.13.1. Deve ser uma solução de armazenamento definida por software, escalável e integrada infraestrutura computacional ofertada. Deve ser capaz de fornecer alta disponibilidade, resiliência de dados e recuperação de desastres.

2.2.13.2. Deve oferecer suporte aos protocolos SMB 2.1 e NFSv3 para clientes e servidores.

2.2.13.3. Deve ser integrada com o Active Directory para fornecer autenticação, enumeração baseada em acesso, quotas e a capacidade de auto-recuperação de versões anteriores de arquivos (Windows Previous Versions).

2.2.13.4. Deve ser compatível com ambientes de virtualização ofertado.

2.2.13.5. Deve suportar técnicas de eficiência de dados, incluindo Erasure Coding e compressão.

2.2.13.6. Deve ser capaz de fornecer relatórios detalhados sobre o uso de armazenamento, capacidade, idade de dados e atividades de arquivo.

2.2.13.7. Deve oferecer recursos avançados de análise de arquivos e auditoria para melhorar a visibilidade e a segurança dos dados armazenados.

2.2.13.8. Deve incluir uma ferramenta de análise de arquivos que forneça os seguintes recursos:

2.2.13.8.1.1. Tendência de capacidade de armazenamento.

2.2.13.8.1.2. Relatório dos principais usuários ativos.

2.2.13.8.1.3. Relatório dos principais arquivos acessados.

2.2.13.8.1.4. Análise de idade de dados.

2.2.13.8.1.5. Distribuição de arquivos por tamanho.

2.2.13.8.1.6. Distribuição de arquivos por tipo.

2.2.13.8.1.7. Detecção de anomalias, incluindo eventos que excedem limites definidos.

2.2.13.8.1.8. Registro de permissões negadas.

2.2.13.9. Deve incluir uma funcionalidade de análise de idade de dados que permita aos administradores visualizarem com que frequência os usuários acessam os dados ao longo do tempo. Os intervalos de idade dos dados devem ser personalizáveis, e a solução deve mostrar o crescimento percentual em cada categoria.

2.2.13.10. Deve oferecer capacidades avançadas de auditoria de trilhas que permitam aos administradores pesquisarem atividades de arquivos específicos por usuário, tipo de operação e horário. Deve ser possível filtrar e exportar essas informações para fins de relatório.

2.2.13.11. Deve permitir a definição de alertas de anomalias para operações específicas executadas por usuários ou no servidor de arquivos como um todo.

Os eventos de anomalias devem ser configuráveis em termos de tipos de eventos, porcentagem de operações e contagem de operações. Também deve ser possível especificar os destinatários de notificações por e-mail para eventos de anomalias.

2.2.13.12. Deve ser capaz de bloquear a criação e a renomeação de arquivos com extensões específicas. Deve ser possível definir políticas de bloqueio de arquivos com base em extensões de arquivo e nomes de arquivo usando curingas. A solução deve incluir uma lista de extensões de arquivo conhecidas de ransomware e bloquear automaticamente qualquer tentativa de criação ou renomeação de arquivos com essas extensões.

2.2.13.13. Deve permitir estender o armazenamento de arquivos através de um namespace unificado que alavanca o armazenamento de múltiplos servidores de arquivos, acessíveis através de um ponto de acesso único.

2.2.14. Deve possuir opções para proteção de dados e recuperação de desastres em nível de compartilhamento (share-level data protection), permitindo possibilidades de agendamento de re-plicação de dados com base nas seguintes categorias de Recovery Point Objective (RPO):

2.2.14.1. Agendamento próximo de síncrono com RPO entre 1 (um) e 15 (quinze) minutos.

2.2.14.2. Agendamento assíncrono, com RPO de 60 minutos ou superior, que podem utilizar snapshots completos e permitem configurações em termos de horas, dias, semanas e meses.

2.2.15. Deve possuir a funcionalidade, para plano de recuperação que possa orquestrar a restauração de compartilhamentos (shares) e servidores de arquivos em um site de recuperação (zona de recuperação), com no mínimo as seguintes características:

2.2.15.1. Deve consistir em procedimentos pré-definidos que garantam a recuperação eficiente dos compartilhamentos e servidores de arquivos no cluster de recuperação. Isso inclui a ativação dos compartilhamentos protegidos no site secundário e o redirecionamento do acesso de clientes.

2.2.15.2. Deve permitir a sincronização bidirecional de dados entre as zonas de recuperação e a possibilidade de retornar à zona primária utilizando políticas de replicação reversa (reverse replication policies), que podem ser configuradas após um failover para facilitar o failback.

2.2.16. Deve implementar a autenticação de clientes possibilitando o acesso seguro através da troca de um certificado digital. Além disso deve validar que o certificado seja assinado por uma Autoridade Certificadora (CA) confiável.

2.2.17. A plataforma deve oferecer análise da saúde do sistema, identificação de problemas baseados em dados de cluster (incluindo detecção de anomalias e alertas detalhados com causas/resoluções), e fornecer

orientações de melhores práticas para segurança e desempenho, incluindo a geração automática de casos de suporte em situações graves ou complexas.

3. Instalação do Appliance de Nuvem Privada

3.1. Deve ser feita a montagem em rack padrão 19", alimentação elétrica e conexão do equipamento à rede de dados.

3.2. O serviço de instalação consiste na colocação do equipamento em pleno funcionamento, em conformidade com o disposto nesta especificação técnica, no Edital e seus Anexos e em perfeitas condições de operação, de forma integrada ao ambiente de infraestrutura de informática da Contratante e deve contemplar, no mínimo, o seguinte:

3.2.1. Montagem em rack padrão 19" indicado pela contratante, alimentação elétrica e conexão do equipamento à rede de dados.

3.2.2. Conexão e configuração do(s) nó(s) nos equipamentos de rede do Contratante;

3.2.3. Instalação do software HCI especificado no termo de referência.

3.2.4. Atualização de softwares, firmwares e drives que compõem a solução;

3.2.5. Instalação, configuração e aplicação das licenças aplicáveis;

3.2.6. Configuração do cluster HCI e da rede virtual com pelo menos dois switches virtuais ou grupos de portas.

3.2.7. Ativação e configuração dos serviços do armazenamento unificado (iSCSI, NFS, SMB, S3).

3.2.8. Empregar configurações de segurança respeitando a conformidade com pelo menos os seguintes requisitos:

3.2.8.1. Common Criteria EAL2+: estes critérios foram produzidos predominantemente para que as empresas que vendem soluções de TI para o mercado governamental possam avaliá-los em relação a um conjunto de padrões.

3.2.8.2. As publicações especiais do Instituto Nacional de Padrões e Tecnologia (NIST – National Institute of Standards and Technology) para controles de segurança e privacidade (SP) para sistemas e organizações federais de informação (NIST SP 800.53).

3.2.8.3. O Guia de Implementação Técnica de Segurança (STIG) da Agência de Sistemas de Informação do Departamento de Defesa dos EUA (DISA).

3.2.9. Deverá implantar todas as atualizações e correções de software conforme previsto nos alertas e recomendações do Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) para toda a solução ofertada, incluindo a camada de virtualização, SDS e seu respectivos serviços de

armazenamento. Não serão aceitas soluções de contorno para vulnerabilidades conhecidas no momento da implementação.

3.2.10. Deverá implantar as seguintes configurações:

3.2.10.1. Proibir o login direto como usuário root.

3.2.10.2. Bloquear contas do sistema que não sejam root.

3.2.10.3. Impor detalhes de manutenção de senha.

3.2.10.4. Configurar cautelosamente o acesso via SSH. Deverá ser configurado método de autenticação de usuário administrador que permita o acesso à linha de comando através de chaves SSH, impedindo o uso de senhas. Ativar o bloqueio de tela.

3.2.11. Após o emprego destas configurações a solução deverá dispor de uma estrutura para automação do gerenciamento de configuração de segurança para garantir que os serviços sejam constantemente inspecionados quanto à variação da política de segurança:

3.2.11.1. A solução deverá estabelecer um ambiente avançado de detecção de intrusões (AIDE) gerando uma base de dados contendo todos os arquivos de configuração. O sistema deverá permitir a verificação da integridade dos arquivos e diretórios por meio de comparação com snapshot capturado da base de dados. No caso de alterações inesperadas, a solução deverá gerar um relatório para revisão. Para o caso de alterações válidas, o administrador poderá atualizar a base de dados.

3.2.11.2. Caso a solução não disponha de tal funcionalidade, deverá ser ofertada ferramenta para gestão de configurações baseadas no conceito de Configuration Management Database (CMDB) em que são guardadas todas as informações importantes sobre itens de configuração (ICs) utilizados pelo CONTRATANTE. A ferramenta deverá estar licenciada para toda a capacidade do cluster sem restrições de uso e seguindo o mesmo nível de atendimento do suporte, sendo também necessário o treinamento da equipe técnica do CONTRATANTE para gestão da solução ofertada.

3.2.12. Serviço para ativação e configuração da solução de criptografia dos dados no nível do cluster HCI. Caso a solução de armazenamento de objetos e arquivos seja externa ao cluster HCI, deverá obedecer aos requisitos de criptografia dos dados especificados neste termo de referência.

3.2.13. Reunir e documentar os requisitos, restrições, suposições, dependências e decisões da solução.

3.2.14. Configurar a criptografia dos dados armazenados no SDS.

3.2.15. Configurar o serviço de gerenciamento de chaves (KMS) localmente no cluster HCI ou externamente ao cluster, em ambos os casos com redundância objetivando alta disponibilidade. Para solução externa, deverão ser

fornecidos todos os componentes de hardware, software, serviços de instalação e treinamento da equipe técnica do CONTRATANTE.

3.2.16. Em ambos os casos, deverão ser abordados os procedimentos para:

3.2.16.1. Troca de chaves em momentos arbitrários para aumento de segurança.

3.2.16.2. Realizar a cópia de segurança da chave de criptografia.

3.2.17. Revisar os requisitos de RPO e RTO.

3.2.18. Revisar o dimensionamento da solução para comportar as retenções necessárias dos snap-shots realizados.

3.2.19. Configuração do call-home;

3.2.20. Documentação do ambiente configurado e instalado.

3.3. A ativação e configuração da solução deve ser realizada segundo as boas práticas do fabricante, disponibilizando o ambiente de virtualização em condições de pleno funcionamento.

3.4. Não compreende a migração das aplicações eventualmente existentes em outra infraestrutura.

4. Instalação do Armazenamento Unificado de Arquivos e Objetos

4.1. Deve ser feita a montagem em rack padrão 19", alimentação elétrica e conexão dos equipamentos à rede de dados.

4.2. O serviço de instalação consiste na colocação dos equipamentos em pleno funcionamento, em conformidade com o disposto nesta especificação técnica, no Edital e seus Anexos e em perfeitas condições de operação, de forma integrada ao ambiente de infraestrutura de informática da Contratante e deve contemplar, no mínimo, o seguinte:

4.2.1. Montagem em rack padrão 19" indicado pela contratante, alimentação elétrica e conexão do equipamento à rede de dados.

4.2.2. Conexão e configuração do(s) nó(s) nos equipamentos de rede do Contratante;

4.2.3. Instalação do software especificado neste termo de referência.

4.2.4. Atualização de softwares, firmwares e drives que compõem a solução;

4.2.5. Instalação, configuração e aplicação das licenças aplicáveis;

4.2.6. Configuração do cluster HCI e da rede virtual com switches virtuais e grupos de portas.

4.2.7. Ativação e configuração dos serviços do armazenamento unificado (iSCSI, NFS, SMB, S3).

4.2.8. Empregar configurações de segurança respeitando a conformidade com pelo menos os seguintes requisitos:

4.2.8.1. Common Criteria EAL2+: estes critérios foram produzidos predominantemente para que as empresas que vendem soluções de TI para o mercado governamental possam avaliá-los em relação a um conjunto de padrões.

4.2.8.2. As publicações especiais do Instituto Nacional de Padrões e Tecnologia (NIST – National Institute of Standards and Technology) para controles de segurança e privacidade (SP) para sistemas e organizações federais de informação (NIST SP 800.53).

4.2.8.3. O Guia de Implementação Técnica de Segurança (STIG) da Agência de Sistemas de Informação do Departamento de Defesa dos EUA (DISA).

4.2.9. Deverá implantar todas as atualizações e correções de software conforme previsto nos alertas e recomendações do Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) para toda a solução ofertada SDS e seus respectivos serviços de armazenamento. Não serão aceitas soluções de contorno para vulnerabilidades conhecidas no momento da implementação.

4.2.10. Deverão ser revisadas e implantadas, em conjunto com a equipe técnica do CONTRATANTE, as configurações presentes no Guia de Segurança do fabricante da solução HCI. Para soluções HCI com Hipervisor VMware, deverá incluir, mas não se limitar, às seguintes regras STIG:

4.2.10.1. Limitar o número de sessões concorrentes para o máximo de 10 (dez) contas e/ou tipos de contas habilitando modo de bloqueio.

4.2.10.2. Empregar configuração global no cluster para que o daemon SSH dos hosts ESXi não permita logins de usuários como root, adicionando exceções para endereços IP ou sub-redes administrativas.

4.2.10.3. O host ESXi deve proteger a confidencialidade e integridade das informações transmitidas, protegendo o tráfego de gerenciamento do ESXi.

4.2.10.4. O host ESXi deve proteger a confidencialidade e integridade das informações transmitidas, protegendo o tráfego de gerenciamento baseado em IP através da segmentação de rede.

4.2.10.5. O firewall do host ESXi deve restringir o acesso aos serviços em execução no host.

4.2.10.6. O firewall do host ESXi deve bloquear o tráfego de rede por padrão.

4.2.11. Para qualquer solução HCI, as regras STIG deverão ser capazes de proteger o carregador de inicialização (boot loader), pacotes, sistema de arquivos, controle de serviço e inicialização, propriedade de arquivos, autenticação, kernel e log.

4.2.12. Deverá implantar as seguintes configurações:

- 4.2.12.1. Proibir o login direto como usuário root.
- 4.2.12.2. Bloquear contas do sistema que não sejam root.
- 4.2.12.3. Impor detalhes de manutenção de senha.
- 4.2.12.4. Configurar o acesso via SSH. Deverá ser configurado método de autenticação de usuário administrador que permita o acesso à linha de comando através de chaves SSH, impedindo o uso de senhas. Ativar o bloqueio de tela.
- 4.2.13. Após o emprego destas configurações a solução deverá dispor de uma estrutura para automação do gerenciamento de configuração de segurança para garantir que os serviços sejam constantemente inspecionados quanto à variação da política de segurança:
 - 4.2.13.1. A solução deverá estabelecer um ambiente avançado de detecção de intrusões (AIDE) gerando uma base de dados contendo todos os arquivos de configuração. O sistema deverá permitir a verificação da integridade dos arquivos e diretórios por meio de comparação com snapshot capturado da base de dados. No caso de alterações inesperadas, a solução deverá gerar um relatório para revisão. Para o caso de alterações válidas, o administrador poderá atualizar a base de dados.
 - 4.2.13.2. Caso a solução não disponha de tal funcionalidade, deverá ser ofertada ferramenta para gestão de configurações baseadas no conceito de Configuration Management Database (CMDB) em que são guardadas todas as informações importantes sobre itens de configuração (ICs) utilizados pelo CONTRATANTE. A ferramenta deverá estar licenciada para toda a capacidade do cluster sem restrições de uso e seguindo o mesmo nível de atendimento do suporte, sendo também necessário o treinamento da equipe técnica do CONTRATANTE para gestão da solução ofertada.
- 4.2.14. Serviço para ativação e configuração da solução de criptografia dos dados no nível do cluster HCI. Caso a solução de armazenamento de objetos e arquivos seja externa ao cluster HCI, deverá obedecer aos requisitos de criptografia dos dados especificados neste termo de referência.
- 4.2.15. Reunir e documentar os requisitos, restrições, suposições, dependências e decisões da solução.
- 4.2.16. Configurar a criptografia dos dados SDS.
- 4.2.17. Configurar o serviço de gerenciamento de chaves (KMS) localmente no cluster HCI ou externamente ao cluster, em ambos os casos com redundância objetivando alta disponibilidade. Para solução externa, deverão ser fornecidos todos os componentes de hardware, software, serviços de instalação e treinamento da equipe técnica do CONTRATANTE.
- 4.2.18. Em ambos os casos, deverão ser abordados os procedimentos para:

- 4.2.18.1. Troca de chaves em momentos arbitrários para aumento de segurança.
- 4.2.18.2. Realizar a cópia de segurança da chave de criptografia.
- 4.2.19. Serviço para ativação e configuração da solução de proteção dos dados para as máquinas virtuais no cluster HCI.
- 4.2.20. Revisar os requisitos de RPO e RTO.
- 4.2.21. Revisar o dimensionamento da solução para comportar as retenções necessárias dos snap-shots realizados.
- 4.2.22. Configurar políticas de proteção SmartDR.
- 4.2.23. Associar as máquinas virtuais às políticas de proteção conforme necessário.
- 4.2.24. Testar e validar a recuperação das políticas de proteção SmartDR e VMs, conforme necessário.
- 4.2.25. Configuração do call-home;
- 4.2.26. Documentação do ambiente configurado e instalado.
- 4.3. A ativação e configuração da solução deve ser realizada segundo as boas práticas do fabricante, disponibilizando o ambiente de virtualização em condições de pleno funcionamento.
- 4.4. Não compreende a migração das aplicações eventualmente existentes em outra infraestrutura.

ANEXO II

MODELO DE PROPOSTA DE PREÇOS

(em papel timbrado da empresa)

À

ADVOCACIA-GERAL DA UNIÃO

Departamento de Tecnologia da Informação (DTI)

Advocacia-Geral da União - Departamento de Tecnologia da Informação - Setor de Indústrias Gráficas SIG, Quadra 06, Lote 800 – Brasília - DF, CEP: 70610-460.

Referência: Pregão Eletrônico **SRP** nº ____/____.

Proposta que faz a empresa _____, inscrita no CNPJ nº _____ e inscrição estadual nº _____, estabelecida no(a) _____, para eventual **<contratação/aquisição de>** para atender às necessidades da **ADVOCACIA-GERAL DA UNIÃO (AGU)**, de acordo com as especificações e condições constantes do Pregão em referência, bem como do respectivo Edital e seus Anexos.

PLANILHA DE PROPOSTA DE PREÇOS

Grupo/Lote	Item	Descrição	Unidade de Medida/Métrica	Quantidade	Valor Unit. (R\$)	Valor Total (R\$)
1	1					
	2					
	3					
	4					
VALOR TOTAL (R\$)						

DA SOLUÇÃO OFERTADA

Item	Descrição	Nome da Solução / Fabricante	Link
1			
2			

Nota: A proposta deverá ser apresentada acompanhada da documentação técnica da solução e o link de internet em que se encontra hospedada a documentação necessária que possibilite a verificação dos requisitos técnicos/funcionais da solução.

SOFTWARE: (deverá ser informado, **obrigatoriamente**, o detalhamento dos softwares a serem fornecidos, quando for o caso, acompanhados dos respectivos *datasheets*)

Nome do Software: _____ Versão: _____

Nome do Fabricante: _____

Procedência: 1. Nacional [] 2. Importado: []

Sítio na WEB do Fabricante: _____

Responsável: _____ Telefone Contato: _____

DO EQUIPAMENTO OFERTADO

Item	Descrição	Fabricante	Marca/Modelo	Link
1				
2				

Nota: A proposta deverá ser apresentada acompanhada da documentação técnica do equipamento e o link de internet em que se encontra hospedada a documentação necessária que possibilite a verificação das especificações técnicas do equipamento.

HARDWARE: (deverá ser informado, **obrigatoriamente**, o detalhamento dos hardwares a serem fornecidos, quando for o caso, acompanhados dos respectivos *datasheets*)

Nome do Hardware: _____ Marca: _____ Modelo: _____

Nome do Fabricante: _____

Procedência: 1. Nacional [] 2. Importado: []

Sítio na WEB do Fabricante: _____

Responsável: _____ Telefone Contato: _____

1) Dados da Proposta:

Valor Total: R\$ _____ (**VALOR POR EXTENSO**).

2) Validade da Proposta: 60 (sessenta) dias, a contar da data de sua apresentação.

3) Informamos, por oportuno, que nos preços apresentados acima já estão computados todos os custos necessários decorrentes da prestação dos serviços, bem como já incluídos todos os impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, seguros, deslocamentos de pessoal e quaisquer outros que incidam direta ou indiretamente.

4) Dados da empresa:

a) Razão Social:

b) CNPJ (MF) nº

c) Inscrição Estadual nº:

d) Endereço:

e) Telefone: _____ **Fax:** _____ **e-mail:**

f) Cidade: _____ **Estado:** _____

g) CEP: _____

h) Representante(s) legal(is) com poderes para assinar o contrato:

a. Nome: _____

b. Cargo: _____

c. CPF: _____ RG: _____ - _____

i) Dados Bancários:

a. Banco: _____

b. Agência: _____

c. Conta Corrente: _____

j) Dados para Contato:

a. Nome: _____

b. Telefone/Ramal: _____

Declaramos, para todos os fins e efeitos legais, aceitar, irrestritamente, todas as condições e exigências estabelecidas no Edital da licitação em referência e do Contrato a ser celebrado, cuja minuta constitui o Anexo “___” do Edital.

Declaramos, ainda, que inexistente qualquer vínculo de natureza técnica, comercial, econômica, financeira ou trabalhista com servidor ou dirigente da Advocacia Geral da União (AGU); não sendo admitidas, em hipótese alguma, alegações posteriores de desenvolvimento dos serviços e de dificuldades técnicas não previstas.

<Local>, <dia> de <mês> de <ano>.

Responsável/Representante da Empresa

<Nome do Responsável>

Cargo

CPF: <nº do CPF>

ANEXO III
PLANILHA PONTO-A-PONTO

1.	Appliance para Nuvem Privada	Conformidade
1.1.	Deve ser fornecido 6 (seis) equipamentos do tipo servidor físico (appliance/nó para nuvem privada), com possibilidade de expansão e, no mínimo, a seguinte configuração bruta cada:	
1.1.1.	Deve ser fornecido com 2 (dois) processadores físicos padrão x86. Cada processador deve possuir, no mínimo, 32 (trinta e dois) núcleos físicos. Referência: Intel Xeon Gold 6548Y+ ou superior. Para fins de referência, considerar-se-á superior o processador que contenha ao menos o número especificado de núcleos e "Single Thread Rating" superior ao do processador de referência no site www.cpubenchmark.net .	
1.1.2.	Deve ser fornecido com 1.536GB (um mil quinhentos e trinta e seis gigabytes) de memória RAM.	
1.1.3.	Deve ser fornecido com dispositivo (ou um conjunto de dispositivos) de armazenamento de alto desempenho, com no mínimo 92,16TB (noventa e dois virgula dezesseis terabytes) brutos, compostos por pelo menos 6 SSDs do tipo NVMe. Se houver necessidade de licenciamento para utilizar a capacidade total do armazenamento, este deverá ser incluído e fornecido junto com o equipamento.	
1.1.4.	Deve possuir 2 (duas) placas adaptadoras de rede, cada uma com 2 (duas) portas 25GbE do tipo SFP28.	
1.1.5.	Deve acompanhar 2 (dois) transceivers compatíveis com os servidores fornecidos e também outros 2 (dois) transceivers compatíveis com Switches Fortinet (FN-TRAN-SFP28-SR), todos no padrão 25GBASE-SR para 25Gbps full-duplex;	
1.1.6.	Deve acompanhar 2 (dois) cabos ópticos de 15 metros do tipo multimodo OM4 50/125 duplex com conectores LC/LC;	
1.1.7.	Deve acompanhar 1 (um) Patch Cord UTP Cat6A de no mínimo 2,5m (dois metros e meio) e 1 (uma) interface 1000BASE-T compatível com os serviços de conectividade ofertados.	
1.1.8.	A depender dos acréscimos especificados nos itens subsequentes, a configuração do servidor será alterada. Nesse caso, será aceita a utilização de equipamentos com maior capacidade, desde que do mesmo fabricante e linha de produtos ofertada e que esses equipamentos permitam formar um cluster entre si.	N/A
1.1.9.	No caso de projetos de múltiplos nós, se a configuração for compatível com plataformas de hardware que suportam múltiplos nós por chassi, o serviço deverá ser fornecido com tantos nós quando possível no mesmo chassi, a fim de oportunizar espaço.	N/A
1.2.	Cada appliance deve ser fornecido com no mínimo a seguinte configuração de software:	
1.2.1.	As especificações a seguir visam apresentar os requisitos necessários e funcionalidades para o software para nuvem privada e demais funções necessárias para atendimento do projeto. Visando mitigar os esforços dispendidos no desenvolvimento de integrações, é preferível que as licitantes proponham opções por fornecer uma solução única, entretanto, considerando a especificidades de algumas características e visando a liberdade de oferta ao certame, será admitido, para as funcionalidades expressamente indicadas, a junção de múltiplas soluções para integração entre si, com objetivo de atendimento igualitário ao de uma solução única. Caso seja realizado por integração com soluções de parceiros tecnológicos, esta solução deve estar homologada com o fabricante do software para nuvem privada para garantir total integração entre as soluções e fabricantes, sendo que essas informações de compatibilidade entre as soluções devem estar publicadas no site oficial de ambos os fabricantes ou caberão aos fabricantes selecionados pela licitante emitirem carta de conformidade em nome da comissão de licitação deste processo concorrencial, citando o número do processo e data, devidamente assinada pelo responsável técnico a nível nacional, citando o nome da licitante proponente, descrevendo o nome do produto ofertado, e expressando quais ações de integração serão realizadas com outras soluções, assumindo o compromisso de compatibilidade, visando o correto funcionamento e garantindo que a proponente apta para atender estes requisitos por meio de compatibilidade total e completa entre todos os produtos. Não serão aceitas soluções ou funcionalidades implementadas via software ainda em fase de desenvolvimento, ou seja, aquelas que ainda não foram homologadas pelo fabricante para ambiente de produção.	N/A
1.2.2.	O serviço deve suportar uma infraestrutura computacional para nuvem privada de alta disponibilidade em configuração de cluster para ambiente de virtualização partindo de pelo menos 03 (três) nós (appliance/hardware físico), cada qual com sua respectiva capacidade de processamento, armazenamento, comunicação de rede.	
1.2.3.	Conforme disposto no inciso V do artigo 40 da lei 14.133, de 01 de abril de 2021, tanto os hardwares quanto os softwares desta solução deverão ser fornecidos por um único fabricante, o qual será responsável também, pelo suporte e garantia da plataforma como um todo ou fornecido hardware (servidores) que sejam homologados em formato OEM pelo fabricante da solução, desde que, o suporte seja unificado e prestado pelo fabricante, não sendo aceito por empresas parceiras e/ou licitantes.	
1.2.4.	O software hiperconvergente deve incorporar segurança em conformidade com padrões governamentais e internacionais de segurança e privacidade: NIST SP800-53, FIPS 140-2, Common Criteria EAL2+, constar na lista de produtos aprovados pela rede de informação do Departamento de Defesa norte americano (DoDIN APL), além de permitir o emprego de configurações baseadas no Guia de Implementação Técnica de Segurança (STIG) da Agência de Sistemas de Informação do Departamento de Defesa dos EUA (DISA).	
1.2.5.	Tanto para cluster com dados, como para cluster vazio, a solução deverá permitir configurar criptografia de dados durante a ingestão (inline) ou após a gravação na camada de armazenamento (data-at-rest encryption) com gerenciador de chaves (KMS), local ou externo (sem ponto único de falha em ambos os cenários), que suporte a troca da chave mestre de criptografia em períodos arbitrários para aumento de segurança, para que os dados sejam inacessíveis em caso de roubo de um disco ou equipamento. Caso a solução dependa exclusivamente de um serviço externo para gerenciamento de chaves criptográficas, este deverá ser fornecido sem ponto único de falha juntamente com a solução. Caso esta funcionalidade requeira licenciamento de software ou componentes de hardware adicionais, estes deverão ser fornecidos com a solução garantindo a redundância entre os sites do CONTRATANTE.	
1.2.6.	Permitir a realização de snapshots através do SDS com consistência para os dados da aplicação (application-consistent), tanto para VMs com sistema operacional Linux como para VMs com sistema operacional Windows, através de tecnologia VSS e semelhantes.	
1.2.7.	Permitir que o próprio administrador da máquina virtual realize a recuperação granular de arquivos sem a necessidade de envolvimento da equipe responsável pela gestão das cópias de segurança (backup).	
1.2.8.	Deve suportar escalabilidade horizontal de 32 (trinta e dois) nós por cluster, isso é, a adição de novos nós ao cluster com gerenciamento através de uma console gráfica, sem a parada do ambiente de produção, aumentando como um todo a capacidade de armazenamento, processamento e memória disponibilizados ao Hypervisor. Deve ser permitida a inclusão futura de novos equipamentos, mesmo que de gerações e configurações diferentes ao cluster implantado.	
1.2.9.	Deve possuir capacidade para realizar snapshots granulares em nível de máquina virtual (VM) para permitir a proteção de dados abrangendo todos os discos virtuais. Além disso, deve haver a capacidade de criar clones de snapshots de VM para testes de software, bem como suporte para recuperação granular de nível de arquivo diretamente da VM, com o mínimo de intervenção nas operações de infraestrutura.	
1.2.10.	Deve possuir capacidade de manter múltiplas cópias dos dados em diferentes locais. No caso de um cluster formado pelo menos por 3 (três) nós, a solução deve possibilitar 2 (duas cópias) de dados em nós distintos do cluster para garantir tolerância de falha em até 1 (um) nó. E no caso de um cluster formado pelo menos por 5 (cinco) nós, a solução deve possibilitar até 3 (três cópias) de dados em nós distintos do cluster para garantir tolerância de falha em até 2(dois) nós.	
1.2.11.	No caso de aquisições de múltiplos nós, se a configuração for compatível com plataformas de hardware que suportam múltiplos nós por chassi, o serviço deverá ser fornecido com tantos nós quando possível no mesmo chassi, a fim de oportunizar espaço.	N/A
1.2.12.	Deve possuir capacidade para criar cópias redundantes de dados e distribuí-las em nós que não compartilham o mesmo bloco. Além disso, deve ser capaz de manter as máquinas virtuais operando mesmo após uma falha em um bloco, devido à existência de cópias redundantes de dados e metadados em outros blocos.	
1.2.13.	Deve possuir capacidade para criar cópias redundantes de dados e distribuí-las em nós que não compartilham o mesmo rack. A redundância de dados deve ser assegurada em situações de falhas, como a falha de todas as fontes de alimentação em um rack, a falha de um switch top-of-rack (TOR), ou a ocorrência de uma partição de rede que torne um rack inacessível a partir de outros racks. Além disso, deve ser capaz de manter a operação contínua de máquinas virtuais, mesmo na falha de um rack ou na falha de dois racks, garantindo que as cópias redundantes dos dados e metadados das máquinas virtuais estejam disponíveis em outros racks quando ocorrer a falha de um rack.	
1.2.14.	Deve possuir funcionalidade de compressão de dados após a escrita (com a flexibilidade de ajustar o tempo de atraso) e compressão inline aos appliances ofertados.	
1.2.15.	Deve possuir deduplicação de cache para otimização de desempenho aos appliances ofertados, bem como a possibilidade de ativar a deduplicação de capacidade para dados persistentes, visando a redução do uso de armazenamento em disco rígido.	
1.2.16.	Deve permitir a configuração de diferentes combinações de compressão e deduplicação para diferentes cargas de trabalho (storage profiles, storage containers, entre outros).	

1.2.17.	Para permitir um melhor aproveitamento dos recursos de armazenamento do cluster, deve suportar método de proteção de dados Erasure Coding, no qual os dados são divididos em fragmentos, estendidos e codificados com pedaços de dados redundantes e armazenados em diferentes nós.	
1.2.18.	Caso a solução ofertada não possua funcionalidades para otimização de armazenamento, como compressão, deduplicação e erasure coding, o licitante deverá fornecer 60% a mais de dispositivos de armazenamento em sua proposta comercial, garantindo assim a capacidade ne-cessária para atender às demandas de armazenamento.	
1.2.19.	Deve permitir adição de nós que incrementem apenas o armazenamento do cluster de forma independente do processamento e memória.	
1.2.20.	No caso de movimentação de VMs (máquinas virtuais) entre os nós do cluster, a solução deve manter os dados das máquinas virtuais no armazenamento local do próprio nó, além disso os dados devem ser movidos, caso necessário, em segundo plano, para esse novo servidor, buscando o melhor desempenho possível através do acesso local ao dado.	N/A
1.2.21.	Deve possuir funcionalidade para expor recursos de armazenamento diretamente para sistemas operacionais virtualizados e hosts físicos utilizando o protocolo iSCSI.	
1.2.22.	Deve ser fornecido serviço de armazenamento de objetos com no mínimo as seguintes características:	N/A
1.2.22.1.	Deve ser compatível com a API REST do Amazon Web Services Simple Storage Service (AWS S3).	
1.2.22.2.	Deve possuir a capacidade de criar ""buckets"" com políticas WORM, que impeçam a modificação ou exclusão de dados enquanto a política estiver ativa.	
1.2.22.3.	Os dados armazenados na solução, especialmente aqueles sob políticas WORM, devem ser imutáveis e não podem ser alterados ou excluídos.	N/A
1.2.22.4.	Deve oferecer suporte ao versionamento de objetos, permitindo que múltiplas versões de um mesmo objeto sejam mantidas. As versões mais antigas não devem ser sobrescritas.	
1.2.22.5.	Deve permitir a definição de políticas de retenção baseadas na idade dos dados para cumprir regulamentações específicas, além disso deve ser possível definir quando os dados serão excluídos automaticamente.	
1.2.22.6.	Deve permitir a divisão de grandes conjuntos de dados em partes menores para aumentar a eficiência no processo de upload e facilitar a retomada de uploads interrompidos.	
1.2.22.7.	Deve oferecer recursos de gerenciamento de identidade e acesso, permitindo o controle granular sobre quem pode acessar os "buckets" e objetos. Deve ser possível revogar e regenerar chaves de acesso conforme necessário.	
1.2.22.8.	Deve oferecer suporte para a criação de "buckets" usando protocolos S3 e NFS. O suporte ao protocolo NFS deve ser nativamente implementado e interoperável com o protocolo S3.	
1.2.22.9.	Deve ser ofertado o licenciamento para prover pelo menos 1TB de armazenamento de objetos para cada appliance adquirido. Caso a solução exija um appliance externo para oferecer essa funcionalidade, o licitante deve fornecer este appliance de forma redundante na proposta comercial, garantindo alta disponibilidade e resiliência.	
1.2.23.	Deve ser fornecido serviços de armazenamento de arquivos com características específicas para atender às necessidades de armazenamento de dados não estruturados, incluindo home directories, perfis de usuário, compartilhamento de departamentos, dados de aplicativos, logs de aplicativos, backups e arquivos de arquivo com no mínimo as seguintes características:	
1.2.23.1.	Deve ser uma solução de armazenamento definida por software, escalável e integrada infraestrutura computacional ofertada. Deve ser capaz de fornecer alta disponibilidade, resiliência de dados e recuperação de desastres.	
1.2.23.2.	Deve oferecer suporte aos protocolos SMB e NFS para clientes e servidores.	
1.2.23.3.	Deve ser integrada com o Active Directory para fornecer autenticação, enumeração baseada em acesso, quotas e a capacidade de auto-recuperação de versões anteriores de arquivos (Windows Previous Versions).	
1.2.23.4.	Deve ser compatível com ambientes de virtualização ofertado.	
1.2.23.5.	Deve suportar técnicas de eficiência de dados, incluindo Erasure Coding e compressão.	
1.2.23.6.	Deve ser capaz de fornecer relatórios detalhados sobre o uso de armazenamento, capacidade, idade de dados e atividades de arquivo.	
1.2.23.7.	Deve oferecer recursos avançados de análise de arquivos e auditoria para melhorar a visibilidade e a segurança dos dados armazenados.	
1.2.23.8.	Deve incluir uma ferramenta de análise de arquivos que forneça os seguintes recursos:	
1.2.23.8.1.	Tendência de capacidade de armazenamento.	
1.2.23.8.2.	Relatório dos principais usuários ativos.	
1.2.23.8.3.	Relatório dos principais arquivos acessados.	
1.2.23.8.4.	Análise de idade de dados.	
1.2.23.8.5.	Distribuição de arquivos por tamanho.	
1.2.23.8.6.	Distribuição de arquivos por tipo.	
1.2.23.8.7.	Deteção de anomalias, incluindo eventos que excedem limites definidos.	
1.2.23.8.8.	Registro de permissões negadas.	
1.2.23.9.	Deve incluir uma funcionalidade de análise de idade de dados que permita aos administradores visualizarem com que frequência os usuários acessam os dados ao longo do tempo. Os intervalos de idade dos dados devem ser personalizáveis, e a solução deve mostrar o crescimento percentual em cada categoria.	
1.2.23.10.	Deve oferecer capacidades avançadas de auditoria de trilhas que permitam aos administradores pesquisarem atividades de arquivos específicos por usuário, tipo de operação e horário. Deve ser possível filtrar e exportar essas informações para fins de relatório.	
1.2.23.11.	Deve permitir a definição de alertas de anomalias para operações específicas executadas por usuários ou no servidor de arquivos como um todo. Os eventos de anomalias devem ser configuráveis em termos de tipos de eventos, porcentagem de operações e contagem de operações. Também deve ser possível especificar os destinatários de notificações por e-mail para eventos de anomalias.	
1.2.23.12.	Deve ser capaz de bloquear a criação e a renomeação de arquivos com extensões específicas. Deve ser possível definir políticas de bloqueio de arquivos com base em extensões de arquivo e nomes de arquivo usando curingas. A solução deve incluir uma lista de extensões de arquivo conhecidas de ransomware e bloquear automaticamente qualquer tentativa de criação ou renomeação de arquivos com essas extensões.	
1.2.23.13.	Deve ser ofertado o licenciamento para prover pelo menos 1TB para armazenamento de arquivos para cada appliance adquirido. Caso a solução exija um appliance ex-terno para oferecer essa funcionalidade, o licitante deve fornecer este appliance de forma redundante na proposta comercial, garantindo alta disponibilidade e resiliência.	
1.2.24.	Deve possuir opções de agendamento de replicação de dados para Disaster Recovery (DR), com base em categorias de RPO (Recovery Point Objective) com no mínimo as seguintes características:	
1.2.24.1.	Agendamento síncrono, com RPO zero, deve realizar replicação de dados em tempo real entre dois locais em uma configuração de disponibilidade metropolitana (Stretched Cluster/ Metro).	
1.2.24.2.	Agendamento próximo de síncrono com RPO entre 1 (um) e 15 (quinze) minutos.	
1.2.24.3.	Agendamento assíncrono, com RPO de 60 minutos ou superior, que podem utilizar snapshots completos e permitem configurações em termos de horas, dias, semanas e meses.	
1.2.25.	Deve possuir a funcionalidade, sem nenhuma limitação de licenciamento em o número VMs protegidas, para plano de recuperação que possa orquestrar a restauração de grupos de proteção (entidades protegidas) em um site de recuperação (zona de recuperação) com no mínimo as seguintes características:	
1.2.25.1.	Deve consistir em procedimentos pré-definidos que garantam a recuperação eficiente das entidades no cluster de recuperação, com a capacidade de especificar estágios de reinício para máquinas virtuais e atrasos entre esses estágios.	
1.2.25.2.	Deve permitir a sincronização bidirecional entre zonas de recuperação e a possibilidade de retornar à zona primária usando o mesmo plano.	
1.2.25.3.	Deve permitir a criação de planos de recuperação que possam ser validados e testados para garantir que o sistema possa se recuperar em caso de failover.	
1.2.25.4.	Caso o licenciamento para esta funcionalidade seja determinado pelo número de máquinas virtuais, deverá ser considerado o mínimo de 100 (cem) máquinas virtuais por equipamento ou host pertencente ao cluster.	
1.2.26.	Deve implementar a autenticação de clientes possibilitando o acesso seguro através da troca de um certificado digital. Além disso deve validar que o certificado seja assinado por uma Autoridade Certificadora (CA) confiável.	
1.2.27.	Deve oferecer um recurso que permita reforçar a segurança e restringir o acesso não autorizado à solução de infraestrutura computacional, no qual deve desativar a autenticação por senha para SSH e deve ser restrito a usuários autenticados com base em chaves públicas, onde apenas usuários com credenciais de chave pública autorizadas devem ter permissão para acessar recursos do sistema.	
1.2.28.	Deve ser fornecido hypervisor, plenamente licenciado, para permitir a abstração de aplicativos do hardware subjacente, viabilizando o provisionamento, atualização e gerenciamento escalável de Máquinas Virtuais (VMs). Além disso, deve possibilitar um modelo operacional consistente em ambientes híbridos, abrangendo nuvem privada (data centers) e suporte nuvens públicas.	

1.2.29.	Com o objetivo de aprimorar a eficiência operacional oferecer maior escalabilidade de desempenho, a solução deve implementar uma abordagem de múltiplas filas (multi-queue) para otimizar a transferência de dados entre máquinas virtuais e o armazenamento, resultando em um aumento substancial na capacidade de E/S e uma redução significativa na utilização da CPU. Além disso, as filas de armazenamento devem ser ajustadas automaticamente de acordo com o número de vCPUs configuradas para cada máquina virtual, garantindo um desempenho superior à medida que a carga de trabalho se expande.	
1.2.30.	Deve implementar recurso de segurança Windows Defender Credential Guard em máquinas virtuais Windows, isolando de forma segura as credenciais de usuário do restante do sistema operacional.	
1.2.31.	O cluster deve suportar appliances com Unidades de Processamento Gráfico (GPU), permitindo a instalação de placas de GPU físicas em appliances de nuvem privada e a atribuição a máquinas virtuais (VMs) em modo de passagem direta (GPU Passthrough) e por meio de alocação virtual de GPU (vGPU).	
1.2.32.	Deve possuir funcionalidade para alta disponibilidade para máquinas virtuais para garantir a reinicialização das VMs em um nó (host) alternativo no cluster, em caso de falha no nó (host) original devido a falha completa, isolamento de rede ou falha nos processos de gerenciamento. Além disso, deve possibilitar a reserva espaço em todos os hosts do cluster para garantir que todas as VMs possam reiniciar em outros hosts em caso de falha, com a opção de ativar a reserva de alta disponibilidade.	
1.2.33.	Deve ser fornecido serviço para gerenciamento de Kubernetes básico com no mínimo as seguintes características:	
1.2.33.1.	Deve permitir o provisionamento, operações e gerenciamento de ciclo de vida de clusters Kubernetes.	
1.2.33.2.	Deve suportar o gerenciamento do ciclo de vida de workload clusters.	
1.2.33.3.	Deve possuir múltiplas formas de criação de clusters de workload, incluindo uma interface gráfica amigável (UI), comandos de linha (CLI) e definições YAML.	
1.2.33.4.	Deve integrar o login unificado (Single Sign On) para autenticação de usuários, permitindo uma experiência segura e simplificada para acesso aos clusters Kubernetes.	
1.2.33.5.	Deve possuir controle baseado em funções (RBAC - Role-Based Access Control) deve permitir a criação e gestão de permissões específicas para administradores, restringindo o acesso a apenas os recursos e funcionalidades necessárias.	
1.2.33.6.	Deve suportar ambientes isolados (air-gapped), permitindo a instalação, configuração e operação de clusters Kubernetes sem a necessidade de conexão à internet.	
1.2.33.7.	Deve permitir a implementação de mecanismos de balanceamento de carga para distribuir automaticamente o tráfego de rede entre os nós do cluster.	
1.2.33.8.	Deve fornecer suporte completo ao Container Storage Interface (CSI), permitindo que os orquestradores de contêineres como o Kubernetes interajam de maneira eficiente com os subsistemas de armazenamento, abstraindo a complexidade do provisionamento e gestão de volumes de armazenamento.	
1.2.34.	Deve possuir funcionalidade para configurar políticas de afinidade e anti-afinidade para gerenciar o posicionamento de máquinas virtuais (VMs) em um ambiente de virtualização, onde, a política de afinidade VM-Host deve permitir a restrição da execução de uma VM específica somente em hosts listados na política de afinidade, proporcionando controle sobre o local de execução da VM durante operações de inicialização ou migração. Por outro lado, a política de anti-afinidade VM-VM deve permitir a separação preferencial de VMs específicas para garantir que, em caso de problemas com um host, não ocorra a perda simultânea de todas as VMs associadas.	
1.2.35.	Deve suportar uma experiência de rede contínua e segura, com capacidades de sobreposição, suportando: Virtual LANs, Virtual Private Cloud (VPC), Virtual Private Network (VPN), extensões de rede virtual de Layer 2 usando VPN ou VTEP, e Border Gateway Protocol sessions.	
1.2.36.	Deve ser fornecido solução de segurança de rede avançado para prover visibilidade na rede virtual, proteção baseada em aplicativos contra ameaças de rede, malware e ransomware, além de monitoramento de segurança e conformidade, com no mínimo as seguintes características:	
1.2.36.1.	Deve permitir a inspeção de tráfego que tem origem e destino dentro de um data center, eliminando a necessidade de firewalls leste-oeste adicionais dentro do data center.	
1.2.36.2.	Deve possuir funcionalidade para garantir que apenas o tráfego permitido entre camadas de aplicativos ou outras fronteiras lógicas seja autorizado, protegendo contra ameaças avançadas na virtualização.	
1.2.36.3.	Deve possuir uma visualização detalhada das comunicações entre VMs, facilitando a categorização e agrupamento das cargas de trabalho para estabelecer políticas apropriadas.	
1.2.36.4.	Deve possuir capacidade para configurar políticas de rede associadas a cargas de trabalho (como VMs, aplicações ou vNICs específicas), ou a grupos lógicos de entidades (como Grupos de Entidades ou VPCs categorizadas).	
1.2.36.5.	As políticas de segurança devem ser aplicadas a categorias (grupo lógico de VMs) para garantir que o tráfego associado às VMs na categoria é protegido automaticamente, sem intervenção administrativa.	N/A
1.2.36.6.	Deve possuir políticas de quarentena para isolar uma VM comprometida ou infectada e, opcionalmente, sujeitá-la a processos forenses.	
1.2.36.7.	Deve possuir políticas de isolamento para bloquear todo o tráfego, independentemente da direção, entre dois grupos de VMs identificados por sua categoria.	
1.2.36.8.	Deve possuir políticas para proteger uma aplicação especificando fontes e destinos de tráfego permitidos.	
1.2.36.9.	Deve possuir opção para permitir ou bloquear tráfego IPv6.	
1.2.36.10.	A solução de segurança de rede deve permitir a criação de políticas de segurança com escopo "Global", abrangendo simultaneamente VMs em VLANs gerenciadas pelo Network Controller e VMs em Virtual Private Clouds (VPCs).	
1.2.36.11.	A solução deve fornecer capacidade para atribuir políticas de segurança de rede distintas a vNICs específicas dentro da mesma VM, utilizando a categorização de sub-redes.	
1.2.36.12.	Deve suportar a criação de "Grupos de Entidades" que combinem múltiplos tipos de entidades (como VMs, sub-redes e categorias de VPC) em um único grupo lógico.	
1.2.37.	Deve possuir API REST que permita a criação de scripts para executar comandos de administração do sistema no cluster, utilizando HTTP requests para obter informações sobre o cluster e efetuar alterações na configuração.	
1.2.38.	Deve incluir um conjunto de recursos de análise preditiva e automação de suporte, que de-vem oferecer informações sobre a saúde do sistema e identifiquem possíveis problemas com base em dados coletados do cluster. Além disso, esta plataforma de suporte deve, dinamicamente, analisar as configurações do cluster em relação às melhores práticas, fornecendo tendências preditivas, orientações para configurações ideais, práticas recomendadas para aplicativos e suporte automatizado, com a capacidade de identificar lacunas na configuração do cluster que possam afetar a confiabilidade, disponibilidade ou desempenho a longo prazo e tomar ações recomendadas para corrigir essas questões, incluindo a geração automática de casos de suporte em situações graves ou complexas.	
1.3.	Deve ser fornecido com software para gerenciamento com no mínimo as seguintes características:	
1.3.1.	As especificações a seguir visam apresentar os requisitos necessários e funcionalidades para a solução de gerenciamento avançado para nuvem privada e demais funções necessárias para atendimento do projeto. Visando mitigar os esforços dispendidos no desenvolvimento de integrações, é preferível que as licitantes proponentes optem por fornecer uma solução única, entretanto, considerando a especificidades de algumas características e visando a liberdade de oferta ao certame, será admitido a junção de múltiplas soluções para integração entre si, com objetivo de atendimento igualitário ao de uma solução única. Caso seja realizado por integração com soluções de parceiros tecnológicos, esta solução deve estar homologada com o fabricante da solução de gerenciamento avançado para nuvem privada para garantir total integração entre as soluções e fabricantes, sendo que essas informações de compatibilidade entre as soluções devem estar publicadas no site oficial de ambos os fabricantes ou caberão aos fabricantes selecionados pela licitante emitirem carta de conformidade em nome da comissão de licitação deste processo concorrencial, citando o número do processo e data, devidamente assinada pelo responsável técnico a nível nacional, citando o nome da licitante proponente, descrevendo o nome do produto ofertado, e expressando quais ações de integração serão realizadas com outras soluções, assumindo o compromisso de compatibilidade, visando o correto funcionamento e garantindo que a proponente apta para atender estes requisitos por meio de compatibilidade total e completa entre todos os produtos. Não serão aceitas soluções ou funcionalidades implementadas via software ainda em fase de desenvolvimento, ou seja, aquelas que ainda não foram homologadas pelo fabricante para ambiente de produção.	N/A
1.3.2.	Deve possuir funcionalidade para gerenciamento de relatórios para permitir a configuração e entrega de relatórios históricos contendo informações sobre os recursos de infraestrutura computacional com no mínimo as seguintes características:	
1.3.2.1.	Deve incluir informações sobre métricas de desempenho, como uso da CPU, uso de memória, largura de banda de E/S, contagem de máquinas virtuais, contagem de hosts, contagem de clusters, resumo de licenças e outros dados relevantes.	
1.3.2.2.	Deve possuir capacidade de compartilhar relatórios com outros usuários.	
1.3.2.3.	Deve adicionar diferentes visualizações para personalizar o que é exibido e como os dados são representados.	
1.3.2.4.	Deve possuir capacidade para agendar a geração de relatórios, com a possibilidade de definir apenas uma programação para cada definição de relatório.	
1.3.2.5.	Deve possuir capacidade para retenção de relatórios por um período especificado.	

1.3.2.6.	Deve verificar os detalhes do registro de relatório para obter informações sobre o status do relatório e mensagens de erro, se a geração do relatório falhar.	
1.3.2.7.	Deve possibilitar a definição da aparência visual do relatório, incluindo opções como cor de fundo, logotipos e outros elementos de design.	
1.3.2.8.	Deve permitir diferentes formas de representar os dados, incluindo visualizações pré-definidas, personalizáveis e salvas.	
1.3.2.9.	Deve permitir criar definições de relatório com base em definições de relatórios existentes.	
1.3.2.10.	Deve exportar e importar configurações de relatório.	
1.3.2.11.	Deve permitir o download dos relatórios nos formatos PDF e CSV.	
1.3.2.12.	Deve enviar relatórios por e-mail como anexos nos formatos PDF e CSV.	
1.3.3.	Deve possuir funcionalidade para realizar a capacidade, previsão e planejamento para recursos de infraestrutura computacional com no mínimo as seguintes características:	
1.3.3.1.	Deve possuir capacidade para monitorar, calcular, prever e planejar a capacidade de recursos de armazenamento, CPU e memória. Deve ser capaz de registrar o histórico de consumo desses recursos.	
1.3.3.2.	Deve calcular e apresentar uma representação gráfica do período restante antes que um recurso específico seja completamente consumido.	
1.3.3.3.	Os cálculos de capacidade devem ser baseados em algoritmos avançados que utilizam dados históricos e continuam a coletar dados para previsões precisas.	
1.3.3.4.	Deve reter dados de capacidade por um período estendido para análise aprofundada.	
1.3.3.5.	Deve possuir capacidade para fornecer recursos para o planejamento de recursos da seguinte forma:	
1.3.3.5.1.	Quando não for possível recuperar recursos suficientes ou quando for necessário expandir o ambiente, deve ser capaz de fazer recomendações com base em nós para atender a um período de capacidade específico.	
1.3.3.5.2.	Deve permitir a modelagem da adição de novos workloads ao ambiente para avaliar o impacto na capacidade.	
1.3.3.5.3.	Deve suportar vários tipos de workloads, incluindo: SQL Server, VMs, VDI e variações de porcentagem de crescimento ou redução.	
1.3.3.5.4.	Deve possuir capacidade para ajustar a capacidade do cluster em tempo real com base na modelagem de novos workloads e fornecer recomendações para a expansão do cluster.	
1.3.3.6.	Deve possuir capacidade para gerenciar vários clusters e permitir a modelagem da expansão de workloads em diferentes clusters.	
1.3.3.7.	Deve suportar funcionalidade que, ao modelar um novo workload, seja capaz de analisá-lo em um cluster específico e, se necessário, recomendar a adição de recursos (como nós) a esse mesmo cluster para atender à demanda.	
1.3.4.	Deve possuir funcionalidade de detecção de ineficiência de recursos e adequação em um ambiente virtualizado com no mínimo os seguintes recursos:	
1.3.4.1.	Deve possuir capacidade para identificar ineficiências de recursos em VMs e recomendar ações para otimizar o uso de recursos.	
1.3.4.2.	Deve possuir capacidade para identificar ineficiências de recursos em todo o ambiente virtualizado, bem como em nível de máquina virtual (VM).	
1.3.4.3.	Deve possuir capacidade para fornecer recomendações para resolver ineficiências globais, seja adicionando capacidade ou recuperando recursos existentes.	
1.3.4.4.	Deve identificar VMs candidatas para recuperação de recursos não utilizados e fornecer recomendações para devolver esses recursos ao cluster.	
1.3.4.5.	Deve apresentar as VMs identificadas em categorias de eficiência para facilitar a identificação e a tomada de decisão. As categorias de eficiência devem incluir:	N/A
1.3.4.5.1.	VMs que estão usando uma quantidade mínima de recursos atribuídos.	
1.3.4.5.2.	VMs que foram desligadas por um período ou que estão em execução, mas não consomem CPU, memória ou recursos de E/S.	
1.3.4.5.3.	VMs que poderiam se beneficiar de melhorias de desempenho com recursos adicionais.	
1.3.4.5.4.	VMs que estão consumindo uma quantidade excessiva de recursos, afetando outras VMs no ambiente.	
1.3.4.5.5.	Deve apresentar as recomendações de recuperação de recursos em um formato claro e organizado, mostrando a quantidade total de CPU e memória configurada em comparação com os picos de uso de CPU e memória para cada VM.	
1.3.5.	Deve possuir funcionalidade para permitir aos administradores automatizarem tarefas operacionais rotineiras com no mínimo as seguintes características:	
1.3.5.1.	Deve permitir aos administradores criarem workflows (playbooks) personalizados, combinando gatilhos e ações a partir de um catálogo fornecido.	
1.3.5.2.	Deve possuir subscrições de eventos (gatilhos) configuráveis, ou seja, condições que desencadeiam a execução de um workflow automatizado.	
1.3.5.3.	Deve haver suporte para subscrições de eventos como alerta-based (baseados em alertas do sistema ou definidos pelo usuário) e subscrições de eventos manuais (iniciados explicitamente por administradores).	
1.3.5.4.	Deve fornecer um catálogo de ações pré-definidas que os administradores podem selecionar para criar seus workflows. As ações devem abranger uma variedade de tarefas operacionais.	
1.3.5.5.	Os administradores devem ter a capacidade de personalizar ações para realizar procedimentos mais avançados, usando diferentes métodos de código.	
1.3.5.6.	Deve oferecer uma variedade de ações que podem ser usadas em workflows, incluindo, mas não se limitando a:	N/A
1.3.5.6.1.	A capacidade de iniciar ou desligar máquinas virtuais.	
1.3.5.6.2.	A possibilidade de ajustar recursos de CPU e memória de VMs.	
1.3.5.6.3.	A capacidade de criar um snapshot de uma VM.	
1.3.5.6.4.	Ação para remover alertas do sistema.	
1.3.5.6.5.	Ação para enviar notificações, como e-mails, para equipes ou administradores.	
1.3.5.6.6.	A capacidade de executar código personalizado, incluindo PowerShell, APIs ou CLI, para realizar tarefas específicas.	
1.3.5.7.	Os workflows devem ser compostos de subscrições de eventos e ações, com a capacidade de incluir várias ações em um fluxo lógico.	
1.3.6.	Deve suportar a capacidade de monitorar bancos de dados SQL por meio de um método sem agente, estabelecendo conexões com servidores SQL para coletar dados e fornecer insights sobre bancos de dados, consultas e métricas, onde esses dados devem alimentar um mecanismo para detecção de anomalias e aprendizado de comportamento, para permitir a criação de fluxos de trabalho de automação específicos para ambientes Microsoft SQL.	
1.3.7.	Deve realizar a descoberta de aplicativos, sem agentes, com base em dados IPFIX para identificar VMs e portas de comunicação, além de possuir a capacidade para configurar políticas de descoberta personalizadas com base em assinaturas de portas TCP ou UDP.	
1.3.8.	Deve possuir funcionalidade baseado em machine learning para fornecer workflows (playbooks) e reduzir a sobrecarga da equipe técnica no qual deve possuir as seguintes características:	
1.3.8.1.	Deve oferecer aos administradores a capacidade de escolher uma métrica de infraestrutura específica e definir uma faixa de limites ideais para essa métrica, no qual esses limites devem atuar como pontos de referência para o sistema, assegurando o desempenho desejado.	
1.3.8.2.	Deve oferecer aos administradores a capacidade de especificar um período de monitoramento para o Indicador-Chave de Desempenho (KPI) associado à métrica de infraestrutura escolhida, no qual esse intervalo de tempo deve permitir a observação e avaliação contínua do desempenho da métrica.	
1.3.8.3.	Deve oferecer aos administradores a capacidade de poder de definir um conjunto de ações predefinidas que o sistema pode executar autonomamente em resposta a desvios na métrica, no qual essas ações devem ser configuradas para garantir que o sistema mantenha um comportamento previsível ao lidar com desvios na métrica de infraestrutura.	
1.3.8.4.	Deve oferecer aos administradores a capacidade de poder de estabelecer um limite máximo para o número de correções autônomas que o sistema pode realizar antes de exigir intervenção manual, no qual essa salvaguarda deve evitar ajustes automatizados excessivos e mantém o controle dos administradores.	
1.3.8.5.	Deve avaliar de forma inteligente os parâmetros de infraestrutura, monitorar continuamente a métrica especificada e realizar ações corretivas de forma autônoma para garantir que a métrica permaneça dentro dos limites ideais previamente estabelecidos.	
1.3.9.	Deve ser fornecida uma solução para governança de custos que permita o gerenciamento de gastos em recursos dos serviços de nuvem privada com no mínimo as seguintes características:	
1.3.9.1.	Deve refletir os custos real de possuir uma infraestrutura dos serviços de nuvem privada, incluindo: hardware, software, instalações e administração.	
1.3.9.2.	Deve ser capaz de calcular o custo total de propriedade (TCO), fornecer métricas de custo diárias e mensais, e permitir a criação de relatórios de rateio de custos e alertas de orçamento para fins de governança financeira.	

1.3.10.	Deve ser fornecida solução de gerenciamento de VMs on-premise e suportar multicloud que possui no mínimo as seguintes características:	
1.3.10.1.	Deve simplificar a configuração e gerenciamento personalizado por meio de blue-prints que incorporam elementos essenciais, como máquinas virtuais.	
1.3.10.2.	Deve possibilitar que as equipes de infraestrutura criem blueprints que tornem a implantação e o gerenciamento de VMs comuns repetíveis, eliminando a complexidade das tarefas operacionais.	
1.3.10.5.	Deve disponibilizar um marketplace com blueprints pré-configurados que as equipes de infraestrutura podem usar para provisionar VMs individuais instantaneamente.	
1.3.10.6.	Deve oferecer a capacidade de publicar workflows (runbooks) compartilháveis, que são coleções de tarefas executadas sequencialmente.	
1.3.10.7.	Deve permitir que equipes de infraestrutura definam esses workflows (runbooks) para automatizar tarefas e procedimentos comuns em várias VMs.	
1.3.10.8.	Deve capacitar grupos na organização a gerenciar suas próprias VMs, oferecendo uma alternativa atrativa aos serviços de nuvem pública.	
1.3.11.	Deve suportar capacidade para operar em um ambiente de alta disponibilidade a fim de assegurar a continuidade das operações em situações de desastres naturais, falhas de rede ou quedas de energia, permitindo a restauração da infraestrutura central quando necessário.	
1.3.12.	Deve ser fornecido uma solução de gerenciamento centralizado que permita a monitorização e gestão eficiente de múltiplos clusters por meio de uma única interface web com no mínimo as seguintes características:	
1.3.12.1.	Deve possuir autenticação única (single sign on) para permitir que os usuários acessem todos os clusters registrados com uma única credencial de login.	
1.3.12.2.	Deve possuir um painel principal de resumo que abrange todos os clusters e pode ser personalizado de acordo com as necessidades específicas.	
1.3.12.3.	As visualizações de resumo estão disponíveis para os principais tipos de entidades, com a capacidade de acessar informações detalhadas sobre entidades individuais por meio de opções de detalhamento.	
1.3.12.4.	Deve possuir resumos de alertas multi-cluster com opções de detalhamento, permitindo que os administradores identifiquem e compreendam problemas em potencial em todos os clusters.	
1.3.12.5.	Deve possuir capacidade de configurar individualmente os clusters por meio de ações diretas a partir do sistema central ou de um acesso simplificado aos consoles web dos clusters.	
1.3.12.6.	Deve suportar operações inteligentes, incluindo configuração de rede, segurança, proteção de dados, monitoramento de desempenho, descoberta de aplicativos e gerenciamento de relatórios.	
1.3.13.	Deve possuir controle de acesso baseado em funções (RBAC) que permita a configuração de permissões de acesso personalizadas para usuários com base em suas funções atribuídas, com no mínimo as seguintes características:	
1.3.13.1.	Deve suportar funções pré-definidas e a capacidade de criar funções personalizadas.	
1.3.13.2.	Deve suportar mapeamento de funções para personalizar essas permissões.	
1.3.13.3.	Deve permitir a atribuição de funções a usuários ou grupos específicos, aplicáveis a conjuntos definidos de entidades.	
1.3.13.4.	Deve possuir capacidade de atribuir permissões de operação detalhadas para máquinas virtuais (VMs) com base em requisitos específicos, como "Permitir Inicialização de VM" ou "Permitir Desligamento de VM," deve ser oferecida por meio do recurso RBAC Granular, permitindo a criação de funções personalizadas com permissões mais específicas em comparação às categorias de permissões mais abrangentes.	
1.3.14.	Deve possuir recursos para aprimorar a eficiência e confiabilidade das atualizações de infraestrutura de TI em nuvem privada (datacenter), no qual deve possuir capacidade de determinar dependências de software e firmware, priorizar atualizações de forma inteligente e automatizar todo o processo de atualização em nós(host) agrupados, sem impacto nas aplicações ou disponibilidade de dados. Deve realizar de forma unificada o upgrade para os seguintes itens ofertados: sistema operacional da plataforma de nuvem privada, hypervisor, plataforma para gerenciamento de arquivos, plataforma para gerenciamento de objetos e plataforma para gerenciamento de aplicativos on-premise e multicloud.	
1.3.15.	Serão aceitas soluções que operem em conjunto com o software para nuvem privada ofertado.	N/A
2.	Armazenamento Unificado de Arquivos e Objetos	
2.1.	Deve ser fornecido 1 (um) cluster/grid/conjunto de, no mínimo, 3 (três) equipamentos do tipo servidor físico, com possibilidade de expansão, onde cada um deve ser fornecido com no mínimo a seguinte configuração bruta:	
2.1.1.	Deve ser fornecido com 2 (dois) processadores físicos padrão x86. Cada processador deve possuir, no mínimo, 32(trinta e dois) núcleos físicos. Referência: Intel Xeon Gold 6548Y+ ou superior. Para fins de referência, considerar-se-á superior o processador que contenha ao menos o número especificado de núcleos e "Single Thread Rating" superior ao do processador de referência no site www.cpubenchmark.net .	
2.1.2.	Deve ser fornecido com 1024GB (um mil quinhentos e vinte e quatro gigabytes) de memória RAM.	
2.1.3.	Deve ser fornecido com dispositivo (ou um conjunto de dispositivos) de armazenamento de alto desempenho, com no mínimo 61,44TB (sessenta e um vírgula quarenta e quatro tera-bytes) brutos, compostos por pelo menos 4 SSDs do tipo NVMe. Se houver necessidade de licenciamento para utilizar a capacidade total do armazenamento, este deverá ser incluído e fornecido junto com o equipamento.	
2.1.4.	Deve ser fornecido com dispositivo (ou um conjunto de dispositivos) de armazenamento de capacidade de alto desempenho, com no mínimo 480TB (quatrocentos e oitenta terabytes) brutos, compostos por discos pelo menos 16 SSDs do tipo NVMe. Se houver necessidade de licenciamento para utilizar a capacidade total do armazenamento, este deverá ser incluído e fornecido junto com o equipamento.	
2.1.5.	Deve possuir 2 (duas) placas adaptadoras de rede, cada uma com 2 (duas) portas 25GbE do tipo SFP28.	
2.1.6.	Deve acompanhar 2 (dois) transceivers compatíveis com os servidores fornecidos e também outros 2 (dois) transceivers compatíveis com Switches Fortinet (FN-TRAN-SFP28-SR), todos no padrão 25GBASE-SR para 25Gbps full-duplex.	
2.1.7.	Deve acompanhar 2 (dois) cabos ópticos de 15 metros do tipo multimodo OM4 50/125 duplex com conectores LC/LC.	
2.1.8.	Deve acompanhar 1 (um) Patch Cord UTP Cat6A de no mínimo 2,5m (dois metros e meio) e 1 (uma) interface 1000BASE-T compatível. com os serviços de conectividade ofertados.	
2.1.9.	A depender dos acréscimos especificados nos itens subsequentes, a configuração do servidor será alterada. Nesse caso, será aceita a utilização de equipamentos com maior capacidade, desde que do mesmo fabricante e linha de produtos ofertada e que esses equipamentos permitam formar um cluster entre si.	
2.1.10.	No caso de projetos de múltiplos nós, se a configuração for compatível com plataformas de hardware que suportam múltiplos nós por chassi, o serviço deverá ser fornecido com tantos nós quando possível no mesmo chassi, a fim de oportunizar espaço.	
2.2.	Cada appliance do Armazenamento Unificado de Arquivos e Objetos deve ser fornecido com no mínimo a seguinte configuração de software:	N/A
2.2.1.	As especificações a seguir devem apresentar os requisitos necessários e funcionalidades para o software do Appliances de Armazenamento Unificado de Arquivos e Objetos e demais funções necessárias para atendimento do projeto. Visando mitigar os esforços dispendidos no desenvolvimento de integrações, é preferível que as licitantes proponentes optem por fornecer uma solução única, entretanto, considerando a especificidades de algumas características e visando a liberdade de oferta ao certame, será admitido, para as funcionalidades expressamente indicadas, a junção de múltiplas soluções para integração entre si, com objetivo de atendimento igualitário ao de uma solução única.	
2.2.1.1	Caso seja realizado por integração com soluções de parceiros tecnológicos, esta solução deve estar homologada com o fabricante do software para nuvem privada para garantir total integração entre as soluções e fabricantes, sendo que essas informações de compatibilidade entre as soluções devem estar publicadas no site oficial de ambos os fabricantes ou caberão aos fabricantes selecionados pela licitante emitirem carta de conformidade em nome da comissão de licitação deste processo concorrencial, citando o número do processo e data, devidamente assinada pelo responsável técnico a nível nacional, citando o nome da licitante proponente, descrevendo o nome do produto ofertado, e expressando quais ações de integração serão realizadas com outras soluções, assumindo o compromisso de compatibilidade, visando o correto funcionamento e garantindo que a proponente apta para atender estes requisitos por meio de compatibilidade total e completa entre todos os produtos.	
2.2.1.2	Não serão aceitas soluções ou funcionalidades implementadas via software ainda em fase de desenvolvimento, ou seja, aquelas que ainda não foram homologadas pelo fabricante para ambiente de produção.	
2.2.2.	O serviço deve suportar uma infraestrutura de armazenamento para nuvem privada de alta disponibilidade em configuração de cluster para ambiente de virtualização partindo de pelo menos 03 (três) nós (appliance/hardware físico), cada qual com sua respectiva capacidade de processamento, armazenamento, comunicação de rede.	

2.2.3.	Conforme disposto no inciso V do artigo 40 da lei 14.133, de 01 de abril de 2021, tanto os hardwares quanto os softwares desta solução deverão ser fornecidos por um único fabricante, o qual será responsável também, pelo suporte e garantia da plataforma como um todo ou fornecido hardware (servidores) que sejam homologados em formato OEM pelo fabricante da solução, desde que, o suporte seja unificado e prestado pelo fabricante, não sendo aceito por empresas parceiras e/ou licitantes.	
2.2.4.	O software da solução de armazenamento deve incorporar segurança em conformidade com padrões governamentais e internacionais de segurança e privacidade: NIST SP800-53, FIPS 140-2, Common Criteria EAL2+, constar na lista de produtos aprovados pela rede de informação do Departamento de Defesa norte americano (DoDIN APL), além de permitir o emprego de configurações baseadas no Guia de Implementação Técnica de Segurança (STIG) da Agência de Sistemas de Informação do Departamento de Defesa dos EUA (DISA).	
2.2.5.	Deve suportar escalabilidade horizontal de 32 (trinta e dois) nós por cluster, isso é, a adição de novos nós ao cluster com gerenciamento através de uma console gráfica, sem a parada do ambiente de produção, aumentando como um todo a capacidade de armazenamento, processamento e memória disponibilizados ao Hypervisor. Deve ser permitida a inclusão futura de novos equipamentos, mesmo que de gerações e configurações diferentes ao cluster implantado.	
2.2.6.	Deve possuir capacidade de manter múltiplas cópias dos dados em diferentes locais. No caso de um cluster formado pelo menos por 3 (três) nós, a solução deve possibilitar 2 (duas cópias) de dados em nós distintos do cluster para garantir tolerância de falha em até 1 (um) nó. E no caso de um cluster formado pelo menos por 5 (cinco) nós, a solução deve possibilitar até 3 (três cópias) de dados em nós distintos do cluster para garantir tolerância de falha em até 2(dois) nós.	
2.2.7.	Deve possuir funcionalidade de compressão de dados inline aos appliances ofertados.	
2.2.8.	Deve possuir deduplicação para otimização de desempenho aos appliances ofertados.	
2.2.9.	Para permitir um melhor aproveitamento dos recursos de armazenamento do cluster, deve suportar método de proteção de dados Erasure Coding, no qual os dados são divididos em fragmentos, estendidos e codificados com pedaços de dados redundantes e armazenados em diferentes nós.	
2.2.10.	Caso a solução ofertada não possua funcionalidades para otimização de armazenamento, como compressão, deduplicação e erasure coding, o licitante deverá fornecer 60% a mais de dispositivos de armazenamento em sua proposta comercial, garantindo assim a capacidade necessária para atender às demandas de armazenamento.	
2.2.11.	Deve possuir funcionalidade para expor recursos de armazenamento diretamente para sistemas operacionais virtualizados e hosts físicos utilizando o protocolo iSCSI.	
2.2.12.	Deve ser fornecido serviço de armazenamento de objetos com no mínimo as seguintes características:	N/A
2.2.12.1.	Deve ser compatível com a API REST do Amazon Web Services Simple Storage Service (AWS S3).	
2.2.12.2.	Deve possuir a capacidade de criar ""buckets"" com políticas WORM, que impeçam a modificação ou exclusão de dados enquanto a política estiver ativa.	
2.2.12.3.	Os dados armazenados na solução, especialmente aqueles sob políticas WORM, devem ser imutáveis e não podem ser alterados ou excluídos.	
2.2.12.4.	Deve oferecer suporte ao versionamento de objetos, permitindo que múltiplas versões de um mesmo objeto sejam mantidas. As versões mais antigas não devem ser sobrescritas.	
2.2.12.5.	Deve permitir a definição de políticas de retenção baseadas na idade dos dados para cumprir regulamentações específicas, além disso deve ser possível definir quando os dados serão excluídos automaticamente.	
2.2.12.6.	Deve permitir a divisão de grandes conjuntos de dados em partes menores para aumentar a eficiência no processo de upload e facilitar a retomada de uploads interrompidos.	
2.2.12.7.	Deve oferecer recursos de gerenciamento de identidade e acesso, permitindo o controle granular sobre quem pode acessar os "buckets" e objetos. Deve ser possível revogar e regenerar chaves de acesso conforme necessário.	
2.2.12.8.	Deve oferecer suporte para a criação de "buckets" usando protocolos S3 e NFS. O suporte ao protocolo NFS deve ser nativamente implementado e interoperável com o protocolo S3.	
2.2.12.9.	Possuir painel de visualização de performance que demonstre a quantidade de requisições por segundo, banda utilizada (MB/s) e tempo de leitura de operação de leitura (GET).	
2.2.12.10.	Permitir a configuração de serviços de diretórios compatíveis com Microsoft Active Directory e OpenLDAP, para adicionar usuários com acesso aos objetos.	
2.2.12.11.	A plataforma deve permitir a criação de um namespace único e federado que abranja múltiplas instâncias do serviço de armazenamento de objetos, incluindo aquelas que residem em diferentes localizações geográficas ou diferentes clusters.	
2.2.12.12.	Deve ser ofertado o licenciamento para prover pelo menos 315TB de armazenamento de objetos ou arquivos em todo o cluster adquirido. Com suporte durante 12 (doze) meses em operação 24x7. Caso a solução exija um appliance externo para oferecer essa funcionalidade, o licitante deve fornecer este appliance de forma redundante na proposta comercial, garantindo alta disponibilidade e resiliência.	
2.2.13.	Deve ser fornecido serviços de armazenamento de arquivos com características específicas para atender às necessidades de armazenamento de dados não estruturados, incluindo home directories, perfis de usuário, compartilhamento de departamentos, dados de aplicativos, logs de aplicativos, backups e arquivos de arquivo com no mínimo as seguintes características:	
2.2.13.1.	Deve ser uma solução de armazenamento definida por software, escalável e integrada infraestrutura computacional ofertada. Deve ser capaz de fornecer alta disponibilidade, resiliência de dados e recuperação de desastres.	
2.2.13.2.	Deve oferecer suporte aos protocolos SMB 2.1 e NFSv3 para clientes e servidores.	
2.2.13.3.	Deve ser integrada com o Active Directory para fornecer autenticação, enumeração baseada em acesso, quotas e a capacidade de auto-recuperação de versões anteriores de arquivos (Windows Previous Versions).	
2.2.13.4.	Deve ser compatível com ambientes de virtualização ofertado.	
2.2.13.5.	Deve suportar técnicas de eficiência de dados, incluindo Erasure Coding e compressão.	
2.2.13.6.	Deve ser capaz de fornecer relatórios detalhados sobre o uso de armazenamento, capacidade, idade de dados e atividades de arquivo.	
2.2.13.7.	Deve oferecer recursos avançados de análise de arquivos e auditoria para melhorar a visibilidade e a segurança dos dados armazenados.	
2.2.13.8.	Deve incluir uma ferramenta de análise de arquivos que forneça os seguintes recursos:	N/A
2.2.13.8.1.1.	Tendência de capacidade de armazenamento.	
2.2.13.8.1.2.	Relatório dos principais usuários ativos.	
2.2.13.8.1.3.	Relatório dos principais arquivos acessados.	
2.2.13.8.1.4.	Análise de idade de dados.	
2.2.13.8.1.5.	Distribuição de arquivos por tamanho.	
2.2.13.8.1.6.	Distribuição de arquivos por tipo.	
2.2.13.8.1.7.	Deteção de anomalias, incluindo eventos que excedem limites definidos.	
2.2.13.8.1.8.	Registro de permissões negadas.	
2.2.13.9.	Deve incluir uma funcionalidade de análise de idade de dados que permita aos administradores visualizarem com que frequência os usuários acessam os dados ao longo do tempo. Os intervalos de idade dos dados devem ser personalizáveis, e a solução deve mostrar o crescimento percentual em cada categoria.	
2.2.13.10.	Deve oferecer capacidades avançadas de auditoria de trilhas que permitam aos administradores pesquisarem atividades de arquivos específicos por usuário, tipo de operação e horário. Deve ser possível filtrar e exportar essas informações para fins de relatório.	
2.2.13.11.	Deve permitir a definição de alertas de anomalias para operações específicas executadas por usuários ou no servidor de arquivos como um todo. Os eventos de anomalias devem ser configuráveis em termos de tipos de eventos, porcentagem de operações e contagem de operações. Também deve ser possível especificar os destinatários de notificações por e-mail para eventos de anomalias.	
2.2.13.12.	Deve ser capaz de bloquear a criação e a renomeação de arquivos com extensões específicas. Deve ser possível definir políticas de bloqueio de arquivos com base em extensões de arquivo e nomes de arquivo usando curingas. A solução deve incluir uma lista de extensões de arquivo conhecidas de ransomware e bloquear automaticamente qualquer tentativa de criação ou renomeação de arquivos com essas extensões.	
2.2.13.13.	Deve permitir estender o armazenamento de arquivos através de um namespace unificado que alavanca o armazenamento de múltiplos servidores de arquivos, acessíveis através de um ponto de acesso único.	
2.2.14.	Deve possuir opções para proteção de dados e recuperação de desastres em nível de compartilhamento (share-level data protection), permitindo possibilidades de agendamento de re-plicação de dados com base nas seguintes categorias de Recovery Point Objective (RPO):	N/A
2.2.14.1.	Agendamento próximo de síncrono com RPO entre 1 (um) e 15 (quinze) minutos.	
2.2.14.2.	Agendamento assíncrono, com RPO de 60 minutos ou superior, que podem utilizar snapshots completos e permitem configurações em termos de horas, dias, semanas e meses.	

2.2.15.	Deve possuir a funcionalidade, para plano de recuperação que possa orquestrar a restauração de compartilhamentos (shares) e servidores de arquivos em um site de recuperação (zona de recuperação), com no mínimo as seguintes características:	N/A
2.2.15.1.	Deve consistir em procedimentos pré-definidos que garantam a recuperação eficiente dos compartilhamentos e servidores de arquivos no cluster de recuperação. Isso inclui a ativação dos compartilhamentos protegidos no site secundário e o redirecionamento do acesso de clientes.	
2.2.15.2.	Deve permitir a sincronização bidirecional de dados entre as zonas de recuperação e a possibilidade de retornar à zona primária utilizando políticas de replicação reversa (reverse replication policies), que podem ser configuradas após um failover para facilitar o failback.	
2.2.16.	Deve implementar a autenticação de clientes possibilitando o acesso seguro através da troca de um certificado digital. Além disso deve validar que o certificado seja assinado por uma Autoridade Certificadora (CA) confiável.	
2.2.17.	A plataforma deve oferecer análise da saúde do sistema, identificação de problemas baseados em dados de cluster (incluindo detecção de anomalias e alertas detalhados com causas/resoluções), e fornecer orientações de melhores práticas para segurança e desempenho, incluindo a geração automática de casos de suporte em situações graves ou complexas.	
3.	Instalação do Appliance de Nuvem Privada	
3.1.	Deve ser feita a montagem em rack padrão 19", alimentação elétrica e conexão do equipamento à rede de dados.	
3.2.	O serviço de instalação consiste na colocação do equipamento em pleno funcionamento, em conformidade com o disposto nesta especificação técnica, no Edital e seus Anexos e em perfeitas condições de operação, de forma integrada ao ambiente de infraestrutura de informática da Contratante e deve contemplar, no mínimo, o seguinte:	N/A
3.2.1.	Montagem em rack padrão 19" indicado pela contratante, alimentação elétrica e conexão do equipamento à rede de dados.	
3.2.2.	Conexão e configuração do(s) nó(s) nos equipamentos de rede do Contratante;	
3.2.3.	Instalação do software HCI especificado neste termo de referência.	
3.2.4.	Atualização de softwares, firmwares e drives que compõem a solução;	
3.2.5.	Instalação, configuração e aplicação das licenças aplicáveis;	
3.2.6.	Configuração do cluster HCI e da rede virtual com pelo menos dois switches virtuais ou grupos de portas.	
3.2.7.	Ativação e configuração dos serviços do armazenamento unificado (iSCSI, NFS, SMB, S3).	
3.2.8.	Empregar configurações de segurança respeitando a conformidade com pelo menos os seguintes requisitos:	N/A
3.2.8.1.	Common Criteria EAL2+: estes critérios foram produzidos predominantemente para que as empresas que vendem soluções de TI para o mercado governamental possam avaliá-los em relação a um conjunto de padrões.	
3.2.8.2.	As publicações especiais do Instituto Nacional de Padrões e Tecnologia (NIST – National Institute of Standards and Technology) para controles de segurança e privacidade (SP) para sistemas e organizações federais de informação (NIST SP 800.53).	
3.2.8.3.	O Guia de Implementação Técnica de Segurança (STIG) da Agência de Sistemas de Informação do Departamento de Defesa dos EUA (DISA).	
3.2.9.	Deverá implantar todas as atualizações e correções de software conforme previsto nos alertas e recomendações do Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) para toda a solução ofertada, incluindo a camada de virtualização, SDS e seu respectivos serviços de armazenamento. Não serão aceitas soluções de contorno para vulnerabilidades conhecidas no momento da implementação.	
3.2.10.	Deverá implantar as seguintes configurações:	N/A
3.2.10.1.	Proibir o login direto como usuário root.	
3.2.10.2.	Bloquear contas do sistema que não sejam root.	
3.2.10.3.	Impor detalhes de manutenção de senha.	
3.2.10.4.	Configurar cautelosamente o acesso via SSH. Deverá ser configurado método de autenticação de usuário administrador que permita o acesso à linha de comando através de chaves SSH, impedindo o uso de senhas. Ativar o bloqueio de tela.	
3.2.11.	Após o emprego destas configurações a solução deverá dispor de uma estrutura para automação do gerenciamento de configuração de segurança para garantir que os serviços sejam constantemente inspecionados quanto à variação da política de segurança:	N/A
3.2.11.1.	A solução deverá estabelecer um ambiente avançado de detecção de intrusões (AIDE) gerando uma base de dados contendo todos os arquivos de configuração. O sistema deverá permitir a verificação da integridade dos arquivos e diretórios por meio de comparação com snapshot capturado da base de dados. No caso de alterações inesperadas, a solução deverá gerar um relatório para revisão. Para o caso de alterações válidas, o administrador poderá atualizar a base de dados.	
3.2.11.2.	Caso a solução não disponha de tal funcionalidade, deverá ser ofertada ferramenta para gestão de configurações baseadas no conceito de Configuration Management Database (CMDB) em que são guardadas todas as informações importantes sobre itens de configuração (ICs) utilizados pelo CONTRATANTE. A ferramenta deverá estar licenciada para toda a capacidade do cluster sem restrições de uso e seguindo o mesmo nível de atendimento do suporte, sendo também necessário o treinamento da equipe técnica do CONTRATANTE para gestão da solução ofertada.	
3.2.12.	Serviço para ativação e configuração da solução de criptografia dos dados no nível do cluster HCI. Caso a solução de armazenamento de objetos e arquivos seja externa ao cluster HCI, deverá obedecer aos requisitos de criptografia dos dados especificados neste termo de referência.	
3.2.13.	Reunir e documentar os requisitos, restrições, suposições, dependências e decisões da solução.	
3.2.14.	Configurar a criptografia dos dados armazenados no SDS.	
3.2.15.	Configurar o serviço de gerenciamento de chaves (KMS) localmente no cluster HCI ou externamente ao cluster, em ambos os casos com redundância objetivando alta disponibilidade. Para solução externa, deverão ser fornecidos todos os componentes de hardware, software, serviços de instalação e treinamento da equipe técnica do CONTRATANTE.	
3.2.16.	Em ambos os casos, deverão ser abordados os procedimentos para:	N/A
3.2.16.1.	Troca de chaves em momentos arbitrários para aumento de segurança.	N/A
3.2.16.2.	Realizar a cópia de segurança da chave de criptografia.	N/A
3.2.17.	Revisar os requisitos de RPO e RTO.	N/A
3.2.18.	Revisar o dimensionamento da solução para comportar as retenções necessárias dos snap-shots realizados.	N/A
3.2.19.	Configuração do call-home;	N/A
3.2.20.	Documentação do ambiente configurado e instalado.	N/A
3.3.	A ativação e configuração da solução deve ser realizada segundo as boas práticas do fabricante, disponibilizando o ambiente de virtualização em condições de pleno funcionamento.	
3.4.	Não compreende a migração das aplicações eventualmente existentes em outra infraestrutura.	
4.	Instalação do Armazenamento Unificado de Arquivos e Objetos	
4.1.	Deve ser feita a montagem em rack padrão 19", alimentação elétrica e conexão dos equipamentos à rede de dados.	
4.2.	O serviço de instalação consiste na colocação dos equipamentos em pleno funcionamento, em conformidade com o disposto nesta especificação técnica, no Edital e seus Anexos e em perfeitas condições de operação, de forma integrada ao ambiente de infraestrutura de informática da Contratante e deve contemplar, no mínimo, o seguinte:	N/A
4.2.1.	Montagem em rack padrão 19" indicado pela contratante, alimentação elétrica e conexão do equipamento à rede de dados.	
4.2.2.	Conexão e configuração do(s) nó(s) nos equipamentos de rede do Contratante;	
4.2.3.	Instalação do software especificado neste termo de referência.	
4.2.4.	Atualização de softwares, firmwares e drives que compõem a solução;	
4.2.5.	Instalação, configuração e aplicação das licenças aplicáveis;	
4.2.6.	Configuração do cluster HCI e da rede virtual com switches virtuais e grupos de portas.	
4.2.7.	Ativação e configuração dos serviços do armazenamento unificado (iSCSI, NFS, SMB, S3).	
4.2.8.	Empregar configurações de segurança respeitando a conformidade com pelo menos os seguintes requisitos:	N/A
4.2.8.1.	Common Criteria EAL2+: estes critérios foram produzidos predominantemente para que as empresas que vendem soluções de TI para o mercado governamental possam avaliá-los em relação a um conjunto de padrões.	
4.2.8.2.	As publicações especiais do Instituto Nacional de Padrões e Tecnologia (NIST – National Institute of Standards and Technology) para controles de segurança e privacidade (SP) para sistemas e organizações federais de informação (NIST SP 800.53).	
4.2.8.3.	O Guia de Implementação Técnica de Segurança (STIG) da Agência de Sistemas de Informação do Departamento de Defesa dos EUA (DISA).	

4.2.9.	Deverá implantar todas as atualizações e correções de software conforme previsto nos alertas e recomendações do Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) para toda a solução ofertada SDS e seu respectivos serviços de armazenamento. Não serão aceitas soluções de contorno para vulnerabilidades conhecidas no momento da implementação.	
4.2.10.	Deverão ser revisadas e implantadas, em conjunto com a equipe técnica do CONTRATANTE, as configurações presentes no Guia de Segurança do fabricante da solução HCI. Para soluções HCI com Hipervisor VMware, deverá incluir, mas não se limitar, às seguintes regras STIG:	N/A
4.2.10.1.	Limitar o número de sessões concorrentes para o máximo de 10 (dez) contas e/ou tipos de contas habilitando modo de bloqueio.	
4.2.10.2.	Empregar configuração global no cluster para que o daemon SSH dos hosts ESXi não permita logins de usuários como root, adicionando exceções para endereços IP ou sub-redes administrativas.	
4.2.10.3.	O host ESXi deve proteger a confidencialidade e integridade das informações transmitidas, protegendo o tráfego de gerenciamento do ESXi.	
4.2.10.4.	O host ESXi deve proteger a confidencialidade e integridade das informações transmitidas, protegendo o tráfego de gerenciamento baseado em IP através da segmentação de rede.	
4.2.10.5.	O firewall do host ESXi deve restringir o acesso aos serviços em execução no host.	
4.2.10.6.	O firewall do host ESXi deve bloquear o tráfego de rede por padrão.	
4.2.11.	Para qualquer solução HCI, as regras STIG deverão ser capazes de proteger o carregador de inicialização (boot loader), pacotes, sistema de arquivos, controle de serviço e inicialização, propriedade de arquivos, autenticação, kernel e log.	
4.2.12.	Deverá implantar as seguintes configurações:	N/A
4.2.12.1.	Proibir o login direto como usuário root.	
4.2.12.2.	Bloquear contas do sistema que não sejam root.	
4.2.12.3.	Impor detalhes de manutenção de senha.	
4.2.12.4.	Configurar cautelosamente o acesso via SSH. Deverá ser configurado método de autenticação de usuário administrador que permita o acesso à linha de comando através de chaves SSH, impedindo o uso de senhas. Ativar o bloqueio de tela.	
4.2.13.	Após o emprego destas configurações a solução deverá dispor de uma estrutura para automação do gerenciamento de configuração de segurança para garantir que os serviços sejam constantemente inspecionados quanto à variação da política de segurança:	N/A
4.2.13.1.	A solução deverá estabelecer um ambiente avançado de detecção de intrusões (AIDE) gerando uma base de dados contendo todos os arquivos de configuração. O sistema deverá permitir a verificação da integridade dos arquivos e diretórios por meio de comparação com snapshot capturado da base de dados. No caso de alterações inesperadas, a solução deverá gerar um relatório para revisão. Para o caso de alterações válidas, o administrador poderá atualizar a base de dados.	
4.2.13.2.	Caso a solução não disponha de tal funcionalidade, deverá ser ofertada ferramenta para gestão de configurações baseadas no conceito de Configuration Management Database (CMDB) em que são guardadas todas as informações importantes sobre itens de configuração (ICs) utilizados pelo CONTRATANTE. A ferramenta deverá estar licenciada para toda a capacidade do cluster sem restrições de uso e seguindo o mesmo nível de atendimento do suporte, sendo também necessário o treinamento da equipe técnica do CONTRATANTE para gestão da solução ofertada.	
4.2.14.	Serviço para ativação e configuração da solução de criptografia dos dados no nível do cluster HCI. Caso a solução de armazenamento de objetos e arquivos seja externa ao cluster HCI, deverá obedecer aos requisitos de criptografia dos dados especificados neste termo de referência.	
4.2.15.	Reunir e documentar os requisitos, restrições, suposições, dependências e decisões da solução.	
4.2.16.	Configurar a criptografia dos dados SDS.	
4.2.17.	Configurar o serviço de gerenciamento de chaves (KMS) localmente no cluster HCI ou externamente ao cluster, em ambos os casos com redundância objetivando alta disponibilidade. Para solução externa, deverão ser fornecidos todos os componentes de hardware, software, serviços de instalação e treinamento da equipe técnica do CONTRATANTE.	
4.2.18.	Em ambos os casos, deverão ser abordados os procedimentos para:	N/A
4.2.18.1.	Troca de chaves em momentos arbitrários para aumento de segurança.	
4.2.18.2.	Realizar a cópia de segurança da chave de criptografia.	
4.2.19.	Serviço para ativação e configuração da solução de proteção dos dados para as máquinas virtuais no cluster HCI.	
4.2.20.	Revisar os requisitos de RPO e RTO.	
4.2.21.	Revisar o dimensionamento da solução para comportar as retenções necessárias dos snap-shots realizados.	
4.2.22.	Configurar políticas de proteção SmartDR.	
4.2.23.	Associar as máquinas virtuais às políticas de proteção conforme necessário.	
4.2.24.	Testar e validar a recuperação das políticas de proteção SmartDR e VMs, conforme necessário.	
4.2.25.	Configuração do call-home;	
4.2.26.	Documentação do ambiente configurado e instalado.	
4.3.	A ativação e configuração da solução deve ser realizada segundo as boas práticas do fabricante, disponibilizando o ambiente de virtualização em condições de pleno funcionamento.	
4.4.	Não compreende a migração das aplicações eventualmente existentes em outra infraestrutura.	

ANEXO IV

MODELO DE PLANO DE IMPLANTAÇÃO

(em papel timbrado da empresa)

1. Disposições Finais

1.1. Este modelo tem caráter meramente exemplificativo, destinado a ilustrar, no Termo de Referência, o conteúdo mínimo que a CONTRATADA deverá apresentar em seu Plano de Implantação da Solução de Infraestrutura Hiperconvergente (HCI) para hospedagem do Portal EVA da ESAGU. Os prazos, equipes e quantitativos são meramente exemplificativos.

1.2. O Plano de Implantação definitivo, a ser elaborado e apresentado pela CONTRATADA, deverá ser compatível com o escopo, os prazos e as condições contratuais estabelecidas no Edital e seus Anexos.

1.3. Este documento é um modelo genérico. O plano definitivo deverá atender aos critérios M1 a M4 especificados na sequência deste documento.

1.4. Qualquer alteração de escopo ou prazo deverá ser formalmente solicitada e aprovada pela Fiscalização antes de sua implementação.

1.5. O não cumprimento dos prazos, entregáveis e critérios de aceite sujeitará a CONTRATADA às penalidades previstas no instrumento contratual.

2. Objetivo

2.1. Este Plano de Implantação estabelece as diretrizes, etapas, responsabilidades e critérios de aceite para a execução dos serviços de fornecimento, instalação, configuração e ativação da solução de Infraestrutura Hiperconvergente (HCI) no datacenter da Advocacia-Geral da União (AGU), destinada à hospedagem do Portal da Escola Virtual da AGU (EVA), plataforma de estudos da Escola Superior da AGU (ESAGU).

2.2. A solução contempla servidores de aplicação de plataforma de estudos, servidores de banco de dados em cluster, armazenamento (storage), servidores de mídia para streaming, infraestrutura CDN e os respectivos componentes de rede, segurança e balanceamento de carga, conforme especificado no Estudo Técnico Preliminar 70/2025.

3. Escopo dos Serviços

3.1. O plano abrange, de forma não exaustiva, os seguintes serviços:

- a) Fornecimento e transporte de todos os nós HCI, módulos ópticos e acessórios até o datacenter da AGU;
- b) Instalação física dos equipamentos em racks, incluindo cabeamento elétrico redundante e cabeamento de dados (cobre e fibra);
- c) Montagem e configuração do cluster hiperconvergente (hypervisor, storage distribuído, rede virtual);
- d) Configuração dos servidores de aplicação de plataforma de estudos com balanceamento de carga e autoescalonamento;
- e) Configuração do cluster de banco de dados (com replicação);
- f) Configuração do armazenamento integrado;

- g) Configuração dos servidores de mídia e streaming;
- h) Configuração de CDN para distribuição de conteúdo;
- i) Implementação de segurança: firewall, WAF, criptografia em repouso e em trânsito, MFA, SSL/TLS;
- j) Configuração de cache;
- k) Configuração de backup automático com snapshots diários e restauração ponto a ponto;
- l) Testes de alta disponibilidade (HA), failover, desempenho e segurança;
- m) Entrega de documentação técnica as-built completa;
- n) Transferência de conhecimento à equipe técnica da CONTRATANTE.

4. Fases e Etapas da Implantação

4.1. A implantação será organizada nas seguintes fases sequenciais:

Fase	Etapa	Descrição	Responsável
1	Mobilização e Planejamento	Designação formal da equipe técnica; levantamento do ambiente físico (racks, infraestrutura elétrica, climatização, cabeamento); validação do projeto executivo junto à CONTRATANTE; obtenção de autorizações de acesso ao datacenter.	Contratada / Contratante
	Aprovação do Cronograma	Submissão e aprovação do cronograma detalhado de execução, incluindo janelas de manutenção e dependências com a infraestrutura existente.	Contratada / Fiscalização
2	Recebimento de Equipamentos	Recebimento, conferência física e técnica (modelo, número de série, versão de firmware, integridade) de todos os nós HCI, transceivers e componentes. Geração do Relatório de Recebimento.	Contratada
	Inspeção Pré-Instalação	Vistoria dos locais de instalação: disponibilidade de espaço em rack (Us livres), alimentação elétrica (PDU, circuitos dedicados, redundância), aterramento, temperatura ambiente, disponibilidade de portas nos switches existentes e cabeamento.	Contratada / Fiscalização
3	Instalação Física dos Nós HCI	Montagem dos nós hiperconvergentes em rack, fixação com trilhos, conexão de cabos de alimentação redundantes, instalação de módulos ópticos (SFP+/SFP28), conexão dos cabos de dados e de gerenciamento.	Contratada
	Atualização de Firmware	Atualização de todos os nós para a versão de firmware homologada pelo fabricante e aprovada pela CONTRATANTE, anterior a qualquer configuração lógica do cluster.	Contratada
	Configuração do Cluster HCI	Criação do cluster hiperconvergente: configuração do hypervisor, storage distribuído, rede virtual (VLANs, vSwitches), pools de recursos, domínios de falha e políticas de resiliência.	Contratada
	Configuração de Segurança	Implementação de criptografia em repouso (AES-256) e em trânsito (TLS 1.3), configuração de firewall distribuído, WAF, MFA para acesso administrativo, hardening dos nós, configuração de auditoria e logs.	Contratada
4	Provisionamento de VMs e Serviços	Criação e configuração das máquinas virtuais: servidores para a plataforma de estudos, servidores de banco de dados em cluster, servidores de mídia, serviços de cache, balanceador de carga.	Contratada
	Configuração da Plataforma Moodle	Instalação e configuração da plataforma de estudos, integração com autenticação (caso solicitado), configuração do armazenamento, integração com CDN, configuração de streaming de vídeo.	Contratada

5	Testes e Homologação	Execução dos testes: failover de nó HCI, failover de cluster de BD, desempenho (IOPS/latência), conectividade iSCSI/S3, validação de criptografia em repouso, teste de carga da plataforma de estudos (15.000 usuários simultâneos), teste de streaming, validação de backup/restore. Resultados registrados em Relatório de Testes.	Contratada / Fiscalização
	Correção de Não Conformidades	Tratamento das falhas identificadas nos testes, com novo ciclo de validação até aprovação da Fiscalização.	Contratada
6	Documentação As-Built	Entrega do dossiê técnico: diagramas físicos e lógicos atualizados, inventário de equipamentos (números de série, firmware), topologia de rede, configurações do cluster HCI, políticas de storage e segurança, manual de operação e manutenção.	Contratada
	Transferência de Conhecimento	Transferência de conhecimento à equipe técnica da CONTRATANTE para operação, monitoramento e manutenção básica da solução HCI, incluindo gerenciamento do cluster, expansão de nós, procedimentos de backup/restore e troubleshooting.	Contratada
	Aceite Final	Apresentação formal dos resultados à Fiscalização.	Contratada / Fiscalização

5. Cronograma de Execução

5.1. O cronograma executivo detalhado deverá ser elaborado pela CONTRATADA e submetido à aprovação da Fiscalização por ocasião da reunião inicial. O cronograma deverá:

- Apresentar todas as etapas descritas na Seção 3, com datas de início e término;
- Indicar dependências entre etapas e marcos de entrega;
- Respeitar o prazo para entrega dos equipamentos, contado a partir da emissão da OFB;
- Prever que o início dos serviços de instalação (Fase 3) somente ocorrerá após a aprovação formal do Plano de Implantação;
- Prever janelas de trabalho fora do horário comercial para atividades que impactem o ambiente em produção;
- Ser atualizado sempre que necessário e encaminhado à Fiscalização.

5.2. O prazo total para conclusão da implantação não poderá exceder 15 (quinze) dias, contado a partir da Ordem de Serviço (OS).

6. Equipe Técnica

6.1. Os serviços deverão ser prestados por profissionais devidamente capacitados e habilitados para o objeto especificado neste Termo de Referência.

7. Documentação e Entregáveis

Documento / Entregável	Conteúdo Mínimo	Momento de Entrega
Plano de Implantação	Cronograma detalhado, equipe, metodologia, riscos e plano de rollback	Reunião inicial
Relatório de Recebimento de Equipamentos	Conferência de itens, números de série, versões de firmware, estado físico	Após recebimento dos equipamentos

Projeto Executivo Validado	Diagramas físicos e lógicos do cluster HCI, topologia de rede, tabela de VLANs, políticas de storage e replicação	Antes do início da Fase 3
Relatório de Testes e Homologação	Resultados de failover de nó, desempenho NVMe, conectividade iSCSI/S3, criptografia, teste de carga da plataforma de estudos (15.000 usuários), streaming, backup/restore	Ao término da Fase 5
Dossiê Técnico As-Built	Inventário, diagramas finais, configurações do cluster, políticas de segurança, manual operacional	Antes do aceite final
Registro de Transferência de Conhecimento	Relatório abordando conhecimentos transmitidos e áreas atendidas.	Ao término da atividade
Termo de Aceite	Declaração formal de conclusão e aceite da Fiscalização por meio do Termo de Recebimento Definitivo (TRD)	Ao final da Fase 6

8. Critérios de Aceite da implantação e configuração

Item	Critério de Aceite
Formação do Cluster HCI	Todos os nós integrados ao cluster com status saudável; storage distribuído operacional com políticas de resiliência configuradas e validadas.
Alta Disponibilidade (HA)	Failover automático de nó com migração de VMs sem interrupção de serviço.
Failover de Banco de Dados	Cluster com failover automático validado; consistência de dados após falha simulada de nó.
Desempenho/Storage	IOPS e latência dentro das especificações do fabricante; throughput de storage compatível com carga de 15.000 usuários simultâneos.
Conectividade iSCSI/S3	Conexão validada entre os nós HCI e o armazenamento (storage)
Criptografia	Criptografia em repouso (AES-256) e em trânsito (TLS 1.3) validadas e auditadas.
Teste de Carga da plataforma de estudos	Plataforma operacional com 15.000 usuários simultâneos sem degradação de performance.
Streaming de Vídeo	Transmissão ao vivo e sob demanda operacional; distribuição via CDN validada com latência aceitável em diferentes regiões.
Integração	Autenticação funcional e validada com usuários de teste, caso solicitado pela Administração.
Backup e Restore	Snapshots diários configurados; teste de restauração ponto a ponto concluído com sucesso.
Segurança	Hardening; WAF e firewall operacionais; MFA ativo para acessos administrativos; auditoria de logs funcional.
Documentação As-Built	Documentação técnica completa, revisada e aprovada pela Fiscalização antes do aceite final.

9. Gestão de Riscos

9.1. A CONTRATADA deverá incluir no Plano de Implantação uma seção de gestão de riscos contemplando, no mínimo:

- Identificação dos principais riscos técnicos: incompatibilidade de firmware dos switches existentes com os protocolos do cluster HCI, falhas de hardware DOA, incompatibilidade de transceivers;
- Riscos logísticos: atrasos na entrega, restrições de acesso ao datacenter, capacidade elétrica ou de climatização insuficiente;

- c) Riscos de prazo: dependências com aprovações internas da CONTRATANTE, janelas de manutenção limitadas;
- d) Avaliação de probabilidade e impacto de cada risco;
- e) Ações preventivas e planos de contingência (equipamento reserva, janelas de reversão de configuração);
- f) Plano de rollback documentado para cada fase crítica da implantação, especialmente: configuração do cluster HCI, criptografia em repouso, migração de dados e configuração de rede;
- g) Responsável pelo monitoramento de cada risco.

9.2. A matriz de alocação de riscos de incompatibilidade é parte integrante deste plano e deve ser observada pela CONTRATADA na elaboração do plano definitivo.

10. Comunicação e Governança no que tange à implantação

- a) Reunião de kick-off com a Fiscalização ao início dos serviços;
- b) Reuniões de acompanhamento com apresentação de status, sempre que necessário;
- c) Comunicação formal (ofício ou e-mail institucional) para pendências, mudanças de escopo ou ocorrências relevantes;
- d) Relatório de progresso à Fiscalização, sempre que solicitado;
- e) Reunião de encerramento para validação dos entregáveis finais.

11. Procedimentos de Aprovação e Reprovação

- a) O Fiscal Técnico comunicará o resultado ao preposto da CONTRATADA em até 5 (cinco) dias úteis contados do recebimento do plano, mediante relatório fundamentado;
- b) Em caso de Aprovado com ressalva, a CONTRATADA deverá entregar as complementações em até 2 (dois) dias úteis;
- c) Em caso de reprovação, a CONTRATADA terá 5 (cinco) dias úteis para reapresentar o plano corrigido;
- d) O prazo para entrega dos equipamentos corre a partir da OFB, independentemente do status de aprovação do plano;
- e) O início dos serviços de instalação somente ocorrerá após a aprovação formal do plano.

Critérios objetivos para o plano de implantação para que a administração aceite, procedimento na hipótese de rejeição/ajustes, efeitos sobre o cronograma de execução do contrato

1. Critérios objetivos de aprovação do Plano de Implantação

1.1. Verificada a completude formal, o Fiscal Técnico avaliará o mérito do Plano de Implantação nos seguintes critérios, atribuindo Aprovado, Aprovado com ressalva ou Reprovado em cada um:

Critério	Referência	Aprovado	Aprovado com Ressalva	Reprovado
M1	Aderência Técnica ao TR	Requisitos do Anexo I, necessários à implantação, identificados no plano de implementação com solução de atendimento explícita.	Até 3 requisitos com aplicação genérica ou insuficientemente detalhada, admitindo complementação.	Ausência de mapeamento de implantação de requisito mandatório.
M2	Exequibilidade do Cronograma	Todos os marcos respeitam prazos contratuais; dependências razoáveis para o ambiente da AGU.	Folgas insuficientes no caminho crítico, porém recuperáveis com ajuste de recurso sem extrapolação do prazo final.	O cronograma prevê conclusão após o prazo contratual de entrega; ou prevê atividades paralelas fisicamente impossíveis (ex.: configuração de cluster antes da chegada dos nós).
M3	Plano de Testes	Casos de teste cobrem os indicadores IAE, ITI e as funcionalidades críticas (HA, failover, desempenho NVMe, segurança).	Lacunas em funcionalidades secundárias, cobertas por declaração de realização adicional.	Ausência de teste de failover de nó, de validação de criptografia em repouso ou de teste de conectividade iSCSI/S3.
M4	Gestão de Riscos e Rollback	todos os riscos técnicos com plano de resposta e rollback documentados; responsável identificado.	Até 2 (dois) riscos sem plano de resposta completo, com compromisso de complementação em 2 dias úteis	Ausência de plano de rollback para fase de configuração do cluster ou de criptografia.

1.2. Resultado consolidado:

Plano *aprovado* se todos os critérios forem Aprovado ou Aprovado com ressalva.

Plano *reprovado* se qualquer critério for Reprovado. Deve ser refeito ou ajustado para o pleno atendimento.

2. Procedimento em caso de reprovação ou ressalva

2.1. O Fiscal Técnico comunicará o resultado ao preposto da CONTRATADA em até 5 (cinco) dias úteis contados do recebimento do plano, mediante relatório fundamentado identificando cada critério com o resultado e a deficiência específica.

2.2. Em caso de Aprovado com ressalva, a CONTRATADA deverá entregar as complementações apontadas em até 2 (dois) dias úteis da comunicação. O Fiscal Técnico decidirá sobre as complementações em até 2 (dois) dias úteis após nova entrega. Aprovadas as complementações, o plano é considerado aprovado na data da comunicação de resultado das complementações.

2.3. Em caso de reprovação, a CONTRATADA terá 5 (cinco) dias úteis para reapresentar o plano corrigido. O Fiscal Técnico avaliará a nova versão em até 2 (dois) dias úteis.

3. Efeitos sobre o cronograma de execução do contrato

3.1. O prazo de até 60 (sessenta) dias para entrega dos equipamentos corre a partir da data de emissão da OFB, independentemente do status de aprovação do plano.

3.2. O início dos serviços de instalação somente ocorrerá após a aprovação formal do plano.

Mecanismo para assegurar o prévio conhecimento das condições do datacenter e para garantir a compatibilidade da solução com a infraestrutura da AGU.

Visita técnica ao datacenter, levantamento de compatibilidade e alocação de riscos

1. Visita técnica — caráter e realização

1.1. A Contratada terá o direito a realizar visita técnica ao datacenter da AGU, onde será instalada a solução objeto deste Termo de Referência.

1.2. Durante a visita, a AGU disponibilizará as seguintes informações técnicas do ambiente existente:

- a) Quantidade e modelo dos switches de rede existentes, com indicação das portas disponíveis e versão de firmware;
- b) Topologia de rede atual (na medida do necessário à solução) incluindo VLANs configuradas, esquema de endereçamento IP e capacidade de trunking disponível;
- c) Espaço físico disponível nos racks;
- d) Capacidade elétrica disponível por rack;
- e) Condicionamento de ar;
- f) Topologia de cabeamento estruturado disponível.

2. Matriz de alocação de riscos de incompatibilidade

2.1. Os riscos de incompatibilidade entre a solução contratada e a infraestrutura existente da AGU são alocados para a CONTRATADA conforme a matriz abaixo, que integra a Matriz de Riscos da contratação:

Risco	Causa raiz	Responsável	Consequência contratual
R1 — Switches existentes suportam os protocolos, mas a CONTRATADA ofertou equipamentos incompatíveis com os switches disponíveis	Contratada optou por não vistoriar ou vistoriou e ofertou solução incompatível	CONTRATADA	Sem prorrogação de prazo; custo do adaptador ou substituição dos cabos/transceivers a cargo da CONTRATADA
R2 — Espaço físico de rack insuficiente para acomodar todos os equipamentos	Proposta de equipamento com dimensões superiores às informadas pelos fabricante	CONTRATADA	Responsável arca com custo de rack adicional e eventual prorrogação
R3 — Capacidade elétrica suficiente, mas CONTRATADA subestimou consumo real na proposta	Erro de dimensionamento da CONTRATADA	CONTRATADA	Sem prorrogação; CONTRATADA providencia solução em seus equipamentos sem ônus para a AGU

R4 — Incompatibilidad e de firmware do switch com o protocolo de controle do cluster HCI	Versão de firmware inferior à mínima homologada pelo fabricante HCI, identificável na visita técnica	CONTRATADA	Responsável arca com atualização do firmware ou fornecimento de switch compatível
R5 — Incompatibilidad e descoberta durante a instalação, não identificável na visita técnica por se tratar de característica latente do ambiente (ex.: interferência eletromagnética, temperatura ambiente acima do especificado)	Condição ambiental não aparente e não mensurável na visita	Risco compartilhado	As partes negociarão solução de mitigação; custo rateado na proporção da contribuição causal apurada pelo Gestor do Contrato
R6 — CONTRATADA não realizou a visita técnica e encontra incompatibilidad e de qualquer natureza	Omissão da CONTRATADA	CONTRATADA	Sem prorrogação; sem reequilíbrio; CONTRATADA soluciona às suas expensas dentro do prazo original

2.2. Para fins de apuração da causa raiz nos riscos, o Gestor do Contrato instaurará procedimento com prazo de 10 (dez) dias úteis, no qual ambas as partes poderão apresentar documentação técnica (ficha técnica do equipamento, laudo do fabricante, ata da visita técnica etc).

2.3. Procedimento para incompatibilidade identificada durante a instalação

Identificada qualquer incompatibilidade durante a execução dos serviços de instalação:

- a) A CONTRATADA comunicará o Fiscal Técnico imediatamente e por escrito, descrevendo tecnicamente a incompatibilidade, sua causa provável e o impacto estimado no cronograma;
- b) O Fiscal Técnico convocará reunião com a CONTRATADA em até 2 (dois) dias úteis para análise conjunta;
- c) As partes formalizarão, em até 5 (cinco) dias úteis da reunião, um Plano de Ação de Compatibilização com solução técnica, responsável e prazo de execução.

ANEXO V

MODELO DE TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

INTRODUÇÃO

O Termo de Compromisso de Manutenção de Sigilo registra o comprometimento formal da Contratada em cumprir as condições estabelecidas no documento relativas ao acesso e utilização de informações sigilosas da Contratante em decorrência de relação contratual, vigente ou não.

Referência: Art. 18, Inciso V, alínea “a” da IN SGD/ME Nº 94/2022.

Pelo presente instrumento a ADVOCACIA GERAL DA UNIÃO, sediada no Setor de Indústrias Gráficas SIG, Quadra 06, Lote 800 – Brasília - DF, CEP: 70610-460, doravante denominado **CONTRATANTE**, e, de outro lado, a **<NOME DA EMPRESA>**, sediada em **<ENDEREÇO>**, CNPJ nº **<Nº do CNPJ>**, doravante denominada **CONTRATADA**.

CONSIDERANDO que, em razão do **CONTRATO N.º <nº do contrato>** doravante denominado **CONTRATO PRINCIPAL**, a **CONTRATADA** poderá ter acesso a informações sigilosas do **CONTRATANTE**.

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação e Privacidade da **CONTRATANTE**;

Resolvem celebrar o presente **TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO**, doravante **TERMO**, vinculado ao **CONTRATO PRINCIPAL**, mediante as seguintes cláusulas e condições abaixo discriminadas.

1 - OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas disponibilizadas pela CONTRATANTE e a observância às normas de segurança da informação e privacidade por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em

acordo com o que dispõem a Lei 12.527, de 18 de novembro de 2011, Lei nº 13.709, de 14 de agosto de 2018, e os Decretos 7.724, de 16 de maio de 2012, e 7.845, de 14 de novembro de 2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

2 - CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

3 - DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: *know-how*, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

4 - DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

5 - DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento prévio e expresso da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmos judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

6 - VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

7 - PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES,

devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme previsto nos arts. 155 a 163 da Lei nº. 14.133, de 2021.

8 - DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo

firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações, conforme definição do item 3 deste documento, disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

9 - FORO

A CONTRATANTE elege o foro da Justiça Federal - Seção Judiciária do Distrito Federal, em Brasília-DF, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

10 - ASSINATURAS

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

CONTRATADA

CONTRATANTE

<Nome>
<Qualificação>

<Nome>
<Cargo>

TESTEMUNHAS

<Nome>
<Qualificação>

<Nome>
<Qualificação>

<Local>, <dia> de <mês> de <ano>.

ANEXO VI

MODELO DE DECLARAÇÃO DE VISTORIA

DECLARO, para fins de participação no Pregão Eletrônico **SRP** nº ____/____, que eu _____, portador do RG nº _____ e do CPF nº _____, representante da _____ empresa _____, estabelecida no _____, como seu **(sua)** representante legal para os fins da presente declaração, compareci perante o representante da **ADVOCACIA GERAL DA UNIÃO - AGU**, tomei conhecimento de todas as informações necessárias à execução do objeto, e que vistoriei os locais de execução dos serviços, tomando ciência das condições e grau de dificuldade existentes.

<Local>, <dia> de <mês> de <ano>.

Responsável/Representante da Empresa

<Nome do Responsável>
CPF: <nº do CPF>

Responsável/Representante da AGU

<Nome do Responsável>

ANEXO VII

MODELO DE DECLARAÇÃO DE RECUSA DE VISTORIA

DECLARO, para fins de participação no Pregão Eletrônico **SRP** nº ____/____, que a empresa _____, CNPJ nº _____, sito à _____ na cidade de _____ UF _____, **OPTOU PELA NÃO REALIZAÇÃO DA VISTORIA TÉCNICA NAS INSTALAÇÕES FÍSICAS DA ADVOCACIA GERAL DA UNIÃO - AGU**, tendo ciência que não poderá alegar em qualquer fase da licitação ou vigência da relação contratual que não realizará os serviços em conformidade com a qualidade e requisitos exigidos.

Responsável/Representante da Empresa

<Nome do Responsável>
CPF: <nº do CPF>

<Local>, <dia> de <mês> de <ano>.

ANEXO VIII

MODELO DE ORDEM DE SERVIÇO (OS)/FORNECIMENTO DE BENS (OFB)

INTRODUÇÃO					
<p>Por intermédio da Ordem de Serviço (OS)/Fornecimento de Bens (OFB) será solicitado formalmente à Contratada a prestação de serviço/o fornecimento do bem relativos ao objeto do contrato.</p> <p>O encaminhamento das demandas deverá ser planejado visando garantir que os prazos para entrega final de todos os serviços/bens estejam compreendidos dentro do prazo de vigência contratual.</p> <p>Referência: Art. 32 IN SGD Nº 94/2022.</p>					
1 - IDENTIFICAÇÃO					
Nº da OS/OFB	<nº da OS/OFB>		Data de emissão	<dd/mm/aaaa>	
CONTRATO/NOTA DE EMPENHO nº	<nº do contrato/nº da NE>				
Objeto do Contrato	<objeto do contrato>				
Contratada	<nome da contratada>	CNPJ	<nº do CNPJ>		
Preposto	<nome do preposto>				
Início vigência	<dd/mm/aaaa>		Fim vigência	<dd/mm/aaaa>	
ÁREA REQUISITANTE					
Unidade	<Sigla – Nome da unidade>				
Solicitante	<nome do solicitante>		Solicitante	<nome do solicitante>	
2 - ESPECIFICAÇÃO DOS BENS/SERVIÇOS E VOLUMES ESTIMADOS					
Item	Descrição do bem ou serviço	Métrica	Valor unitário (R\$)	Qtde/Vol .	Valor Total (R\$)
1
...
Valor total estimado da OS/OFB					
3 - <INSTRUÇÕES/ESPECIFICAÇÕES> COMPLEMENTARES					
<Incluir instruções complementares à execução da OS/OFB>					

<Ex.: Contatar a área solicitante para agendamento do horário de entrega>
<Ex.: Conforme consta no Termo de Referência, o recebimento provisório está condicionado à entrega do código no ambiente de homologação, e a documentação do software no repositório oficial de gestão de projetos>

4 - DATAS E PRAZOS PREVISTOS

Data de Início:	<dd/mm/aaaa>	Data do Fim:	<dd/mm/aaaa>
-----------------	--------------	--------------	--------------

CRONOGRAMA DE EXECUÇÃO/ENTREGA

Item	Tarefa/entrega	Início	Fim
1		<dd/mm/aaaa>	<dd/mm/aaaa>
...		<dd/mm/aaaa>	<dd/mm/aaaa>

5 - ARTEFATOS / PRODUTOS

Fornecidos	A serem gerados e/ou atualizados

6 - ASSINATURA E ENCAMINHAMENTO DA DEMANDA

Autoriza-se a <execução dos serviços / entrega dos bens> correspondentes à presente <OS/OFB>, no período e nos quantitativos acima identificados.

<Nome>
**<Responsável pela demanda/
Fiscal Requisitante>**
Matrícula SIAPE: <Nº da
matrícula>

<Nome>
Gestor do Contrato
Matrícula SIAPE: <Nº da
matrícula>

<Local>, <dia> de <mês> de <ano>.

ANEXO IX

MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO – SERVIÇOS DE TIC

INTRODUÇÃO
O Termo de Recebimento Provisório trata-se de termo detalhado que declarará que os serviços foram prestados ou que os bens foram entregues e atendem às exigências de caráter técnico, sem prejuízo de posterior verificação de sua conformidade com as exigências contratuais, baseada nos requisitos e nos critérios de aceitação definidos no Modelo de Gestão do Contrato.
Referência: Inciso XXI, art. 2º, e alínea “i”, inciso II, art. 33 da IN SGD/ME Nº 94/2022.

1 – IDENTIFICAÇÃO	
CONTRATO Nº	<nº do contrato>
CONTRATADA	<nome da contratada> CNPJ <nº do CNPJ>
Nº DA OS/ OFB	<nº da OS/ OFB >
DATA EMISSÃO DA	<dd/mm/aaaa>

2 – ESPECIFICAÇÃO DOS BENS /SERVIÇOS E VOLUMES DE EXECUÇÃO			
SOLUÇÃO DE TIC			
<Descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>			
ITE M	DESCRIÇÃO DO BEM OU SERVIÇO	MÉTRICA	QUANTIDAD E
1	<Descrição igual ao da OS de abertura>	<Ex.: PF>	<n>
...
...
...
TOTAL DE ITENS			

3 – RECEBIMENTO
Para fins de cumprimento do disposto no art. 33, inciso II, alínea “i”, da IN SGD/ME nº 94/2022, por este instrumento ATESTO que os serviços/ bens correspondentes à < OS/OFB > acima identificada, conforme definido no Modelo de Execução do Contrato supracitado, foram executados/ entregues e

<atende(m)/atende(m) parcialmente/não atende(m)> às respectivas exigências de caráter técnico discriminadas abaixo. Não obstante, estarão sujeitos à avaliação específica para verificação do atendimento às demais exigências contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Contrato.

Ressaltamos que o recebimento definitivo desses serviços/bens ocorrerá somente após a verificação desses requisitos e das demais condições contratuais, desde que não se observem inconformidades ou divergências quanto às especificações constantes do Termo de Referência e do Contrato acima identificado que ensejem correções por parte da **CONTRATADA**. Por fim, reitera-se que o objeto poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.

ITEM	ESPECIFICAÇÃO TÉCNICA	ATENDIMENTO	OBSERVAÇÃO
1	<exigências técnicas definidas no TR>
...
...

4 - ASSINATURA

FISCAL TÉCNICO

<Nome do Fiscal Técnico do Contrato>

PREPOSTO

<Nome do Preposto do Contrato>

<Local>, <dia> de <mês> de <ano>.

ANEXO X

MODELO DE TERMO DE RECEBIMENTO DEFINITIVO

INTRODUÇÃO
<p>O Termo de Recebimento Definitivo declarará formalmente à Contratada que os serviços prestados ou que os bens fornecidos foram devidamente avaliados e atendem às exigências contratuais, de acordo com os requisitos e critérios de aceitação estabelecidos.</p> <p>Referência: Inciso XXII, Art. 2º e alínea “h” inciso I do art. 33, da IN SGD/ME Nº 94/2022.</p>

1 - IDENTIFICAÇÃO			
CONTRATO/NOTA DE EMPENHO Nº	<nº do contrato/nº NE>		
CONTRATADA	<nome da contratada>	CNPJ	<nº do CNPJ>
Nº DA OS/OFB	<nº da OS/OFB>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2 - ESPECIFICAÇÃO DOS PRODUTO(S)/BEM(S)/SERVIÇOS E VOLUMES DE EXECUÇÃO				
SOLUÇÃO DE TIC				
<descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>				
ITEM	DESCRIÇÃO DO BEM OU SERVIÇO	MÉTRICA	QUANTIDADE	TOTAL
1	<descrição igual à da OS/OFB de abertura>	<Ex.: PF>	<n>	<total>
...				
TOTAL DE ITENS				

3 - ATESTE DE RECEBIMENTO
<p>Para fins de cumprimento do disposto no art. 33, inciso II, alínea “h”, da IN SGD/ME nº 94/2022, por este instrumento ATESTO/ATESTAMOS que o(s) <serviço(s)/ bem(s)> correspondentes à <OS/OFB> acima identificada</p>

foram <prestados/entregues> pela **CONTRATADA** e ATENDEM às exigências contratuais, discriminadas abaixo, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Contrato acima indicado.

ITEM	EXIGÊNCIA CONTRATUAL	ATENDI- MENTO	OBSERVA- ÇÃO
1	<exigência contratual estabelecida no TR >
...
...
...

4 - DESCONTOS EFETUADOS E VALOR A LIQUIDAR

De acordo com os critérios de aceitação e demais termos contratuais, <não> há incidência de descontos por desatendimento dos indicadores de níveis de serviços definidos.

<Não foram / Foram> identificadas inconformidades técnicas ou de negócio que ensejam indicação de glosas e sanções, <cuja instrução corre em processo administrativo próprio (nº do processo)>.

Por conseguinte, o valor a liquidar correspondente à <OS/OFB> acima identificada monta em R\$ <valor> (<valor por extenso>).

Referência: <Relatório de Fiscalização nº _____ ou Nota Técnica nº _____>.

5 - ASSINATURA

GESTOR DO CONTRATO

<Nome do Gestor do Contrato>
Matrícula Siape: <nº da matrícula SIAPE>

<Local>, <dia> de <mês> de <ano>

6- AUTORIZAÇÃO PARA FATURAMENTO

Nos termos da alínea “n”, inciso I, art. 33, da IN SGD/ME nº 94/2022, AUTORIZA-SE a **CONTRATADA** a <faturar os serviços executados / apresentar as notas fiscais dos bens entregues> relativos à supracitada <OS/OFB>, no valor discriminado no item 4, acima.

GESTOR DO CONTRATO

<Nome do Gestor do Contrato>

<Local>, <dia> de <mês> de <ano>

7 - CIÊNCIA

PREPOSTO

<Nome do Preposto do Contrato>

<Local>, <dia> de <mês> de <ano>

ANEXO XI

MODELO DE TERMO DE CIÊNCIA

INTRODUÇÃO

O Termo de Ciência visa obter o comprometimento formal dos empregados da Contratada diretamente envolvidos na contratação quanto ao conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes no órgão/entidade.

No caso de substituição ou inclusão de empregados da contratada, o preposto deverá entregar ao Fiscal Administrativo do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados.

Referência: Art. 18, Inciso V, alínea “b” da IN SGD/ME Nº 94/2022.

1 – IDENTIFICAÇÃO

CONTRATO Nº	<nº do contrato>		
OBJETO	<objeto do contrato>		
CONTRATADA	<nome da contratada>	CNPJ	<nº do CNPJ>
PREPOSTO	<Nome do Preposto da Contratada>		
GESTOR DO CONTRATO	<Nome do Gestor do Contrato>	MATR	<nº da Matrícula SIAPE>

2 – CIÊNCIA

Por este instrumento, os funcionários abaixo identificados declaram ter ciência e conhecer o inteiro teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes da Contratante.

Funcionários da CONTRATADA		
Nome	Matrícula	Assinatura
<Nome do(a) Funcionário(a)>	<nº da Matrícula>	
<Nome do(a) Funcionário(a)>	<nº da Matrícula>	

<Local>, <dia> de <mês> de <ano>.

ANEXO XII

MODELO DE TERMO DE ENCERRAMENTO DO CONTRATO

1 – IDENTIFICAÇÃO			
CONTRATO Nº	<nº do contrato>		
OBJETO	<objeto do contrato>		
CONTRATADA	<nome da contratada>	CNPJ	<nº do CNPJ>
PREPOSTO	<Nome do Preposto da Contratada>		
GESTOR DO CONTRATO	<Nome do Gestor do Contrato>	MATR .	<nº da Matrícula SIAPE>

2 - LISTA DE VERIFICAÇÃO

ITEM	ATEN-DIDO	NÃO ATEN-DIDO	NÃO APLICÁ-VEL
Os recursos humanos e materiais foram preparados para a continuidade do negócio por parte da Administração?			
A contratada entregou as versões finais dos produtos e a documentação?			
Houve a transferência final de conhecimentos sobre a execução e manutenção da solução?			
A contratada devolveu os recursos que foram oferecidos para operacionalizar o contrato?			
Foram revogados os perfis de acesso dos funcionários da contratada?			
Foram eliminadas as caixas postais que foram oferecidas à contratada?			
<outras que se apliquem ao objeto da contratação>			

Por este instrumento, as partes abaixo identificadas resolvem registrar o encerramento do contrato em epígrafe e ressaltar o que segue:

O presente contrato está sendo encerrado por motivo de <motivo>.

As partes concedem-se mutuamente plena, geral, irrestrita e

irrevogável quitação de todas as obrigações diretas e indiretas decorrentes do Contrato, não restando mais nada a reclamar de parte a parte, exceto as relacionadas no parágrafo a seguir.

Não estão abrangidas pela quitação ora lançada e podem ser objeto de exigência ou responsabilização, mesmo após o encerramento do vínculo contratual:

- I. As obrigações relacionadas a processos iniciados de penalização contratual;
- II. As garantias sobre bens e serviços entregues ou prestados, tanto legais quanto convencionais;
- III. A reclamação de qualquer tipo sobre defeitos ocultos nos produtos ou serviços entregues ou prestados;
- IV. *<inserir pendências, se houver>.*

E assim, tendo lido e concordado com todos os seus termos, firmam as partes o presente instrumento, em duas vias iguais, para que surta seus efeitos jurídicos.

Gestor do Contrato

<Nome>

Representante da Área Requisitante

<Nome>

Fiscal Técnico do Contrato

<Nome>

Representante Legal da Empresa

<Nome>
<CPF>

<Local>, <dia> de <mês> de <ano>.