CONTRATO Nº 015/2022/SCCC/ALMT

CONTRATO QUE ENTRE SI CELEBRAM A ASSEMBLEIA LEGISLATIVA DO ESTADO DE MATO GROSSO, ATRAVÉS DA MESA DIRETORA E A EMPRESA ADISTEC BRASIL INFORMÁTICA LTDA.

A ASSEMBLEIA LEGISLATIVA DO ESTADO DE MATO GROSSO, doravante denominada **CONTRATANTE**, com sede no Centro Político Administrativo - Cuiabá-MT, inscrita no CNPJ sob nº 03.929.049/0001-11, na Avenida André Antônio Maggi, Lote 06, Setor A, Centro Político Administrativo - CPA, Edifício Governador Dante Martins de Oliveira, Cuiabá – MT., CEP 78049-901, Cuiabá – MT neste ato representado pelo Senhor Presidente Deputado Eduardo Botelho e o Primeiro Secretário, Ordenador de Despesas – Deputado Max Russi, e de outro lado à Empresa **ADISTEC BRASIL INFORMÁTICA LTDA,** inscrita no CNPJ nº 15.457.043/0001-78, com sede na Rua Conceição de Monte Alegre, 198, Conjunto 41, Edifício Acaraí, - Estreito – Monções/SP CEP: 04653-060, telefone: (11) 3504-0600, email: jrodrigues@adistec.com, neste ato representada pelo Senhor **José Roberto Inforzato Rodrigues**, portador do RG nº 10.969.824 SSP/SP e CPF nº 004.767.238-25, doravante denominada **CONTRATADA,** considerando o que consta no Processo Licitatório Pregão Eletrônico Registro de Preços nº 002/2022/ALMT, no Estudo Técnico nº 019/2021/STI, no Termo de Referência nº 022/2021/STI, na Ata de Registro de Preços nº 31/2022/ALMT, Protocolo SGED 2021/6155134910 e sujeitando-se, ainda, às normas da Lei nº 8.666, de 21 de junho de 1993 e suas alterações, e a Lei Complementar Federal nº 101, de 04 de maio de 2.000, demais normas que regem a espécie, RESOLVEM celebrar o presente contrato, nos seguintes termos e condições:

DS JRR

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O presente contrato tem por objeto a contratação de empresa especializada no fornecimento de soluções de T.I contemplando infraestrutura computacional hiperconvergente (hci), como serviços de instalação, configuração, migração, repasse de conhecimento, atualização e manutenção para atender as demandas da assembleia legislativa do estado de mato grosso, conforme especificações do Termo de Referência nº 022/2021/STI, constante no Processo Licitatório Pregão Eletrônico Registro de Preços nº 002/2022/ALMT - Protocolo SGED nº 2021/6155134910.

CLÁUSULA SEGUNDA – DA DESCRIÇÃO DA SOLUÇÃO, ESPECIFICAÇÕES TÉCNICAS, QUANTIDADES E PREÇOS PRATICADOS

2.1. As especificações técnicas dos itens que compõem o objeto deste Contrato, incluindo as normas e padrões de qualidade a serem observados, estão descritas na tabela abaixo:

LOTE 1					
ITEM	**DESCRIÇÃO**	**UND.**	**QTD.**	**VALOR UNITÁRIO R$**	**VALOR TOTAL R$**
1	SOFTWARE PARA NUVEM PRIVADA SW-AOS-ULT-PRD SW-PRS-ULT-NODE SW-FILES-AOS-TiB-PRD SW-OBJECTS-AOS-PRD SW-FLOW-NODE SW-ERA-VCPU-PRD	UNID	2	R$ 2.439.695,00	R$ 4.879.390,00
2	HARDWARE PARA INFRAESTRUTURA EM CLUSTER 7Z84CTO1WW ThinkAgile HX5531	UNID	2	R$ 1.543.139,20	R$ 3.086.278,40
3	COMPUTADORES DE REDE MSN2010-CB2FC Mellanox Spectrum	UNID	2	R$ 260.870,00	R$ 521.740,00

DS JRR

4	SERVIÇOS DE INSTALAÇÃO	UNID	2	R$ 125.400,00	R$ 250.800,00
5	SERVIÇOS DE MIGRAÇÃO	Terabyte	113	R$ 5.263,80	R$ 594.809,40
6	SERVIÇOS DE CUSTOMIZAÇÃO DE SEGURANÇA E PREVENÇÃO RANSONWARE	UND	2	R$ 508.396,00	R$ 1.016.792,00
VALOR TOTAL DO LOTE				**R$ 10.349.809,80 (dez milhões, trezentos e quarenta e nove mil, oitocentos e nove reais e oitenta centavos.)**	

2.3. O valor global do presente contrato é de **R$ 10.349.809,80 (dez milhões, trezentos e quarenta e nove mil, oitocentos e nove reais e oitenta centavos)**.

CLÁUSULA TERCEIRA – DOS RECURSOS ORÇAMENTÁRIOS

3.1. As despesas decorrentes do presente procedimento licitatório correrão pela dotação orçamentária – Exercício de 2022 da Assembleia Legislativa do Estado de Mato Grosso, a seguir:

	Número	Histórico
Reduzida	**36**	-
Projeto/Atividade	2.009	Manutenção de Ações de Informática
Elemento de Despesa	3.3.90.39.00.00	Outros Serviços de Terceiros – Pessoa Jurídica
Fonte de Recurso	100	Recursos do Tesoiro - Ordinários

3.2. No(s) exercício(s) seguinte(s), as despesas correspondentes correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro.

DS JRR

CLÁUSULA QUARTA – DOS PRAZOS DE VIGÊNCIA E EXECUÇÃO

4.1. O presente Instrumento de Contrato terá a vigência de 12 (doze) meses, a contar da data de sua assinatura, tendo validade e eficácia legal após a publicação de seu extrato no Diário Oficial Eletrônico da ALMT.

4.2. A **CONTRATANTE** providenciará a publicação do presente Contrato, em extrato, no Diário Oficial Eletrônico da Assembleia Legislativa do Estado de Mato Grosso, conforme determina o Parágrafo Único, do artigo 61, da Lei nº 8.666/93.

CLÁUSULA QUINTA – DAS CONDIÇÕES DE FORNECIMENTO E RECEBIMENTO DO OBJETO

5.1. A **CONTRATADA** deverá entregar os produtos conforme cronograma abaixo, sendo que os prazos estabelecidos serão contados a partir da data de assinatura do Contrato:

Etapa	Descrição	Prazo em dias
1	Entrega dos equipamentos	45 dias
2	Instalação e entrega do termo de garantia	15 dias (após entrega dos equipamentos)

5.2. O fornecimento deverá ser realizado das 08h00min às 12h00min e das 14h00min às 18h00min, de segunda à sexta-feira.

5.3. A **CONTRATADA** deverá fornecer o objeto em estrita conformidade com disposições e especificações do edital da licitação, de acordo com o Contrato, Termo de Referência e à proposta de preços apresentada.

5.4. A entrega do objeto será na forma do cronograma de execução, definido no Item 5.1.

5.5. Todo o equipamento e/ou material fornecido deverá estar acondicionado em embalagens apropriada, e em perfeitas condições de armazenamento e uso, de forma que garanta a sua integridade e não sejam danificados durante as operações de transporte, carga e descarga, conforme determina a Legislação vigente, podendo, os produtos serem devolvidos sem quaisquer ônus ao município, caso as exigências não sejam atendidas.

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS JRR

5.6. Os produtos deverão estar de acordo com as exigências do Código de Defesa do Consumidor, especialmente no tocante aos vícios de qualidade ou quantidade que os tomem impróprios ou inadequados ao uso a que se destinam ou lhes diminuam o valor, conforme diploma legal.

5.7. No ato da entrega, os materiais serão analisados em sua totalidade, sendo que aquele(s) que não satisfazer(em) à especificação exigida ser(ão) devolvido(s) à **CONTRATADA**.

5.8. Verificada alguma falha no fornecimento, a **CONTRATADA** obriga-se a reparar, corrigir, remover, reconstruir, ou substituir, os produtos entregues e não aceitos pelo **CONTRATANTE**, em função da existência de irregularidades, incorreções, no prazo de 48 (quarenta e oito) horas, contados da notificação que lhe for entregue oficialmente, sem ônus adicional para a **CONTRATANTE**, sem o que será convocada a segunda classificada, sem prejuízo da aplicação das sanções previstas nos artigos 86 a 88 da Lei 8.666/93 e artigos 20 e 56 a 80 do Código de Defesa do Consumidor.

5.9. O objeto deste Contrato será entregue na Secretaria de Tecnologia da Informação – Edifício Dante Martins de Oliveira, Piso Térreo, Avenida André Antônio Maggi, Lote 06, Setor A, CPA, CEP 78049-901 – Cuiabá, Mato Grosso, Brasil, das 08h00min às 12h00min e das 14h00min às 18h00min, de segunda à sexta-feira, com "pré-agendamento" pelo telefone (65) 3313-6450.

5.10. O objeto deste Contrato será recebido e avaliado com o escopo de verificar sua conformidade quanto à quantidade, qualidade e especificações descritas e nos termos dos artigos 69 e 73 a 76 da Lei n.º 8.666, de 21 de junho de 1993 e suas alterações, da seguinte forma:

5.10.1. **Provisório**, rigorosamente conforme descrito na especificação, deste Contrato, conforme o quantitativo da Nota de Empenho e Requisição (Nota de Autorização de Despesa), dentro do prazo estabelecido pela Assembleia Legislativa do Estado de Mato Grosso.

a) O Almoxarifado da Secretaria de Tecnologia da Informação da **CONTRATANTE**, limitar-se-á a verificar a sua conformidade com o discriminado na Nota Fiscal, fazendo constar na mesma a data de recebimento dos equipamentos e, se for o caso, as irregularidades observadas;

b) A simples assinatura do servidor em canhoto de fatura ou conhecimento de transporte implica apenas recebimento provisório.

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS JRR

5.10.2. **Definitivo**, no prazo de até 05 (cinco) dias corridos, contados a partir do recebimento provisório, um servidor designado pela **CONTRATANTE**, como Gestor e/ou Fiscal do Contrato, procederá ao recebimento definitivo, verificando a quantidade e a conformidade com o exigido neste Contrato, no Termo de Referência, Edital e com o constante na respectiva proposta de preço da licitante vencedora.

5.11. Em caso de divergência entre as quantidades, dimensões e qualidades, a fiscalização, sob consulta prévia, definirá o procedimento correto.

a) Caso satisfatório as verificações deste inciso, o servidor atestará a efetivação da entrega do serviço ou material na Nota Fiscal e a encaminhará a Secretaria de Planejamento, Orçamento e Finanças, para fins de pagamento;

b) Caso insatisfatório as verificações, o material deverá ser substituído, no prazo de até 10 (dez) dias contados da comunicação formal desta Administração;

c) Caso a substituição não ocorra no prazo acima determinado, ou caso o novo material também seja rejeitado, estará à **CONTRATADA** incorrendo em atraso na entrega, sujeita à aplicação de penalidades;

d) Os custos de substituição do produto rejeitado correrão exclusivamente a expensas da **CONTRATADA**.

5.12. Não será definitivamente recebido e, consequentemente, será colocado à disposição do fornecedor, o objeto que não for compatível com as características exigidas neste Contrato e no Termo de Referência, ou ainda, que apresente qualquer tipo de avaria e/ou falha.

5.13. A **CONTRATADA** deverá, obrigatoriamente, entregar os materiais em sua totalidade para cada localidade solicitada, não sendo admitido objeto incompleto ou parcelado, sob pena das sanções legais cabíveis.

5.14. O objeto deverá observar as discriminações contidas neste Contrato, sem defeitos ou avarias, sendo aplicadas todas as normas e exigências do Código de Defesa do Consumidor.

5.15. O aceite do objeto pelo setor competente da **CONTRATANTE** não exclui a responsabilidade do fornecedor por vícios de qualidade ou técnicos, aparentes ou ocultos, ou por desacordo com as especificações estabelecidas neste Contrato, e verificadas posteriormente.

DS
JRR

5.16. Demais condições de fornecimento (omissas na ata de registro de preços, no termo de referência, e neste contrato) deverão estar de acordo com o que prevê o código do consumidor.

5.17. A **CONTRATANTE** não caberá qualquer ônus pela rejeição dos produtos ou serviços considerados inadequados ou em desconformidade com a especificação registrada neste Contrato.

5.18. O prazo de entrega do produto poderá ser prorrogado, desde que devidamente justificado o motivo, nos termos do art. 57, §1º e seus incisos, da Lei nº 8.666/1993.

5.19. Após recebidos, os objetos serão conferidos pelo setor competente. Se constatada qualquer irregularidade, a empresa deverá substituí-los, no prazo máximo de 10 (dez) dias, a contar do recebimento da notificação formal emitida pela **CONTRATANTE**.

5.20. Em caso de divergência entre as quantidades, dimensões e qualidades, a fiscalização, sob consulta prévia, definirá o procedimento correto, com a devida aprovação e autorização da Secretaria de Tecnologia da Informação.

CLÁUSULA SEXTA – DO SOFTWARE PARA NUVEM PRIVADA

6.1. REQUISITOS DE SEGURANÇA E PRIVACIDADE

6.1.1. A Autoridade Nacional de Proteção de Dados (ANPD) é um órgão da administração pública direta federal do Brasil que faz parte da Presidência da República e possui atribuições relacionadas a proteção de dados pessoais e da privacidade e, sobretudo, deve realizar a fiscalização do cumprimento da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD). A ANPD reconhece esquemas internacionais de certificação de privacidade como capacitadores de transferência internacional, uma vez que eles exigem que as organizações certificadas implementem uma série de medidas de proteção de dados de alto padrão. Neste sentido, a solução ofertada deverá contemplar ferramentas e permitir o emprego de configurações aderentes aos seguintes esquemas internacionais:

6.1.1.1. Common Criteria: estes critérios foram produzidos predominantemente para que as empresas que vendem produtos de informática para o mercado governamental (principalmente para uso de Defesa ou Inteligência) precisassem apenas avaliá-los em relação a um conjunto de padrões. Deverá ser comprovada a certificação Common Criteria EAL2+ do hipervisor e do sistema de armazenamento definido por software;

DS
JRR

6.1.1.2. As publicações especiais do Instituto Nacional de Padrões e Tecnologia (NIST) para controles de segurança e privacidade (SP) para sistemas e organizações federais de informação (NIST SP 800.53);

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

6.1.2. Adicionalmente, embora não sejam utilizados inicialmente, a solução deverá suportar o emprego de discos auto-criptografáveis (*Self Encrypting Drives* ou SED) validados por FIPS 140-2 Level 2;

6.1.3. 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. A solução deverá garantir que os dados nos drives sejam seguramente destruídos. 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.

6.1.4. Caso a tecnologia de armazenamento definida por software não seja efetiva para otimização dos dados (desduplicação e compressão) enquanto empregar a criptografia dos mesmos a licitante não poderá considerar estes ganhos no dimensionamento da solução.

6.1.5. A **CONTRATADA** deverá considerar serviços profissionais do fabricante da solução para empregar configurações de segurança a fim de estabelecer conformidade com o Guia de Implementações Técnicas de Segurança (STIG). Deverá prever também todas as atualizações e correções conforme previsto nos alertas do Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) para a camada de virtualização, automação e orquestração de infraestrutura. Não serão aceitas configurações de contorno para vulnerabilidades conhecidas no momento da implementação.

DS JRR

6.1.6. Após o emprego destas configurações 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:

6.1.6.1. Tanto para o hipervisor ofertado como para o sistema de armazenamento definido por software, a solução deverá permitir estabelecer um modelo padrão com todas as configurações empregadas no cluster de modo que a solução possa corrigir automaticamente qualquer desvio da configuração de segurança do sistema operacional e do hipervisor para permanecer em conformidade. Se algum componente for considerado não compatível, o componente deverá ser restaurado às configurações de segurança suportadas sem nenhuma intervenção do administrador.

6.1.6.2. 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*.

6.1.6.3. 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.

6.1.6.4. 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 pela **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 da **CONTRATANTE** para gestão da solução ofertada.

6.1.7. O fabricante da solução deverá publicar avisos de segurança com informações detalhadas sobre atualizações, correções de segurança, descrição das vulnerabilidades e as versões de software impactadas.

6.1.8. A solução deverá permitir estabelecer regras de autenticação, tais como:

6.1.8.1. Proibir o *login* direto como usuário *root;*

6.1.8.2. Bloquear contas do sistema que não sejam *root*;

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03.929.049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br | FaceALMT | (65) 3313-6411

DS JRR

6.1.8.3. Impor detalhes de manutenção de senha;

6.1.8.4. Configurar cautelosamente o acesso via SSH;

6.1.8.5. Ativar o bloqueio de tela.

6.1.9. A solução também deverá suportar a configuração de diferentes métodos de autenticação à interface de gerenciamento centralizado:

6.1.9.1. Autenticação através de usuário local;

6.1.9.2. *Active Directory* com possibilidade de autenticação de usuários com *Common Access Card* (CAC), permitindo a autenticação e controle de acesso através da combinação de dispositivos de segurança física e senhas de acesso;

6.1.9.3. *Security Assertion Markup Language* (SAML) através de um provedor externo de identidade.

6.1.10. Deverão estar disponíveis os seguintes tipos de usuários e suas respectivas funções:

6.1.10.1. Visualização - Não permite nenhuma alteração na configuração;

6.1.10.2. Administrador do Cluster - Pode realizar todas as operações disponíveis, exceto criar ou modificar os usuários;

6.1.10.3. Administrador de Usuários - Pode realizar todas as operações disponíveis.

6.1.11. Com o objetivo de proporcionar maior segurança, o sistema operacional também deverá oferecer uma funcionalidade de impedir o acesso ao terminal de linha de comando;

6.1.12. A console Web deve suportar o acesso via HTTPS utilizando certificados.

6.1.13. A solução deve disponibilizar acesso ao sistema operacional da solução através do protocolo padrão SSH (Secure Shell);

6.1.14. A interface de administração WEB e SSH deverá ser configurada em alta-disponibilidade e sem ponto único de falha, garantindo que mesmo em caso de falha ou indisponibilidade de equipamento, a interface de administração continue disponível;

6.1.15. A solução ofertada deverá estar habilitada para uso de microssegmentação, provendo controle granular e governança de todo o tráfego de entrada e saída de uma máquina virtual (VM) e de grupos de máquinas virtuais (VMs).

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03.929.049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS JRR

6.1.15.1. A microssegmentação deverá permitir a associação de políticas de rede a VMs e aplicativos ao invés de segmentos de rede específicos (por exemplo VLANs) ou identificadores (endereços IP ou MAC).

6.1.15.2. Deverá prover visualização de todo tráfego e relacionamentos com a descoberta automática dos fluxos entre as máquinas virtuais.

6.1.15.3. Deverá prover uma estrutura de segurança orientada por políticas que inspeciona o tráfego dentro do data center, da seguinte maneira:

6.1.15.3.1. As políticas de segurança inspecionam o tráfego originado e terminado dentro de um datacenter, ajudando a eliminar a necessidade de firewalls adicionais no datacenter.

6.1.15.3.2. A estrutura deve utilizar uma abordagem centrada na carga de trabalho em vez de uma abordagem centrada na rede, permitindo examinar o tráfego de, e para as VMs, independentemente de como as configurações de rede mudam e onde residem no data center.

6.1.15.3.3. Deverá prover uma abordagem agnóstica a estrutura de rede, centrada na carga de trabalho, permitindo que a equipe de virtualização implemente essas políticas de segurança sem depender de equipes de segurança de rede.

6.1.15.3.4. As políticas de segurança deverão ser aplicadas às categorias (um agrupamento lógico de VMs) e não às próprias VMs, não importando quantas VMs são inicializadas em uma determinada categoria. O tráfego associado às VMs em uma categoria deverá ser protegido sem intervenção administrativa, em qualquer escala.

6.1.15.3.5. A interface de gerenciamento deve oferecer uma abordagem baseada em visualização para configurar políticas e monitorar o tráfego ao qual uma determinada política se aplica:

6.1.15.3.5.1. Política de Segurança de Aplicação: quando for necessário proteger um aplicativo especificando origens e destinos de tráfego permitidos.

6.1.15.3.5.2. Política de Isolamento do Ambiente: quando for necessário bloquear todo o tráfego, independentemente da direção, entre dois grupos de VMs identificados por sua categoria. VMs dentro de um grupo podem se comunicar umas com as outras.

6.1.15.3.5.3. Política de Quarentena: quando for necessário isolar uma VM comprometida ou infectada e, opcionalmente, desejar submetê-la à perícia.

DS
JRR

6.1.15.3.6. Deverá garantir que seja apenas permitido o tráfego entre camadas de aplicativos ou outros limites lógicos, garantindo a proteção contra ameaças avançadas para que não sejam propagadas no ambiente virtual.

6.1.15.3.7. Deverá permitir a atualização automática durante todo o ciclo de vida da VM, eliminando a carga do gerenciamento de mudanças de políticas.

6.1.15.3.8. A Solução deve permitir categorizar as Máquinas Virtuais de forma a permitir a criação políticas de segurança com no mínimo as seguintes funções:

6.1.15.3.8.1. Isolar o tráfego de dados entre Máquinas Virtuais de Diferentes categorias

6.1.15.3.8.2. Isolar o tráfego de dados de Máquinas Virtuais específicas para modo de quarentena, tanto forense quanto restrita, de forma a prover uma rápida reação ao time de infraestrutura em caso de Máquinas Virtuais contaminadas ou pertencentes a usuários que foram desligados ou sob procedimento de custódia de dados.

6.1.15.3.8.3. Mapear o tráfego de entrada, entre as camadas e de saída de aplicações, permitindo ao administrador determinar quais servidores tem acesso de entrada na aplicação, o tipo de protocolo e o número da porta que o fluxo de dados pode ocorrer, permitir ou restringir também o fluxo de dados entre as camadas, máquinas virtuais, pertencentes à aplicação, através da especificação do protocolo e o número da porta, realizar também o mesmo procedimento para conexões de saída das camadas da aplicação, também através da especificação de protocolo e número de porta.

6.1.15.3.9. Deve permitir integração com softwares de terceiros para que seja possível o redirecionamento do tráfego das VMs para ferramentas de detecção e prevenção de intrusos (IDS/IPS), monitoração de performance de aplicações (APM), balanceadores de carga.

6.1.16. Visibilidade da conformidade com a segurança: fornecer um mapa de calor relacionado à segurança provendo visibilidade completa da postura de segurança do ambiente da **CONTRATANTE**. Identificar vulnerabilidades de segurança usando verificações de auditoria automatizadas.

6.1.17. Controle sobre conformidade de segurança: permitir a definição de políticas que detectam continuamente vulnerabilidades de segurança em tempo real e automatizam as ações necessárias para corrigi-las. Permitir criar verificações de auditoria personalizadas para atender às necessidades de conformidade de segurança específicas do **CONTRANTE**.

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03.929.049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS
JRR

6.1.18. Com relação a estrutura de nuvem privada do **CONTRATANTE**, a solução deverá prover auditorias de segurança com detalhes de quaisquer configurações incorretas ou inadequadas dos recursos instalados, classificados no mínimo pelas seguintes categorias:

6.1.18.1. Auditorias de rede, como exemplo as portas TCP/UDP publicamente acessíveis.

6.1.18.2. Auditorias de máquinas virtuais, como exemplo as VMs sem proteção de acesso.

6.1.18.3. Auditorias de dados, como exemplo dados não criptografados

6.1.18.4. Auditorias de acesso.

6.1.19. Além de detectar estes recursos que falhem durante as auditorias, a solução deverá prover ações de remediação necessárias para melhorar a segurança da infraestrutura.

6.1.20. Caso a licitante oferte sua solução com hipervisor ESXi, o fabricante também deverá configurar a solução conforme estabelecido no guia STIG de modo a:

6.1.20.1. Limitar o número de sessões concorrentes para o máximo de dez contas e/ou tipos de contas habilitando modo de bloqueio.

6.1.20.2. 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.

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

6.1.20.4. 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.

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

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

6.1.20.7. Empregar todos os patches e atualizações de segurança conforme descrito nos alertas do CTIR Gov não sendo aceitas soluções paliativas ou de contorno no momento da implantação.

6.2. REQUISITOS DE DISPONIBILIDADE E PROTEÇÃO DOS DADOS

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03.929.049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS JRR

6.2.1. A **CONTRATANTE** estabeleceu a quantidade de clusters em número par para que seja possível a instalação em sites separados geograficamente e assim estabelecer a replicação síncrona e assíncrona entre eles, nativamente, atendendo a diferentes requisitos de disponibilidade para as aplicações e serviços em execução nestes clusters. Os modos de replicação deverão ser configuráveis através da mesma console de gerenciamento e deverá estar licenciados para toda a capacidade do cluster.

6.2.2. Em situação de falência de um cluster, a solução deverá orquestrar o processo de recuperação e restabelecimento das máquinas virtuais no cluster funcional. A solução deverá permitir níveis de proteção por máquinas virtuais individualmente ou para o cluster em sua totalidade, sendo possível estabelecer sequências de inicialização, reconfiguração de redes, execução de *scripts* e também permitir a definição de intervalos necessários para funcionamento dos serviços.

6.2.3. A solução também deverá possuir a capacidade de proteção e recuperação dos dados armazenados no cluster local, além de permitir a replicação para outro cluster distante geograficamente.

6.2.4. A solução deverá permitir, através da interface gráfica de gestão do cluster, a conexão com provedores de nuvens públicas, tais como Amazon AWS e Microsoft Azure, para que seja possível utilizar serviços de armazenamento em nuvem para proteção dos dados.

6.2.5. Tanto para máquinas virtuais Windows como Linux, a solução deve permitir criar grupos de consistência compostos por máquinas virtuais dependentes entre si, tais como aplicação e banco de dados, de modo que elas possam ser protegidas e recuperadas em um estado consistente (*crash-consistent*). Ainda referente a proteção e recuperação de máquinas virtuais Windows e Linux, a solução deve permitir realizar snapshots com consistência dos dados para aplicação (*application consistent*), através de integração com VSS e semelhantes. A solução deve permitir que os usuários das máquinas virtuais possam recuperar arquivos de maneira granular sem envolvimento do administrador do cluster.

6.2.6. Permitir estabelecer pontos de recuperação para máquinas virtuais Windows e Linux com consistência dos dados para a aplicação (*application consistent*) de modo que seja possível restaurar estas máquinas virtuais para um estado sadio na linha do tempo, de modo que o administrador possa escolher através da mesma interface, qual o ponto de recuperação será utilizado.

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03.929.049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS JRR

6.2.7. Caso a solução para atender ao requisito do item anterior não seja nativa da solução de armazenamento definida por software, será necessário considerar 20% (vinte por cento) de capacidade adicional para área de *journal* em cada cluster.

6.2.8. O licenciamento para o recurso de snapshots das máquinas virtuais no nível da solução de armazenamento definida por software, independentemente do hipervisor, não poderá restringir o número de snapshots e suas retenções, beneficiando-se de um algoritmo que redireciona a escrita para o snapshot, oferecendo mais velocidade e eficiência, sem sacrificar a performance do cluster.

6.2.9. Caso a solução dependa de componentes de hardware e software específicos para atender aos requisitos de proteção e recuperação dos dados, estes deverão ser fornecidos em conjunto com a solução respeitando a quantidade de clusters e respectivas capacidades especificadas neste Contrato.

6.2.10. No que tange a capacidade de tierização, para configurações compostas por mais de uma camada de armazenamento (*tiers*), a solução deve ser capaz de mover, em tempo real, dados entre as camadas, para obter maior desempenho dos dados mais acessados. Toda gravação deverá ocorrer primeiramente na camada de armazenamento mais rápido (*tier* 0).

6.3. REQUISITOS FUNCIONAIS DO CLUSTER

6.3.1. A solução deverá prover uma estrutura de alta disponibilidade em configuração de cluster para ambiente de virtualização composta de unidades computacionais ou servidores físicos ou *appliances* ou nós, cada qual com sua respectiva capacidade de processamento, armazenamento e comunicação de rede. Neste cenário, a solução deverá ser capaz de:

6.3.1.1. Permitir escalabilidade horizontal, isso é, a adição de novos chassis e novos servidores (nós) ao cluster 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 hipervisor, além de crescer de forma linear o desempenho/performance do ambiente;

6.3.1.1.1. O procedimento para expansão do cluster deverá ocorrer na mesma interface com assistente que permita tratar as configurações de endereços de rede e garanta que as versões já empregadas no cluster existente sejam transferidas para os novos equipamentos.

DS
JRR

6.3.1.2. Permitir adição de um nó por vez.

6.3.1.3. Permitir adição de nós que incrementem apenas o armazenamento do cluster de forma independente do processamento e memória.

6.3.1.4. Permitir adição de novos equipamentos com geração mais recente no mesmo cluster.

6.3.1.5. Permitir remover equipamento do cluster sem parada no ambiente.

6.3.1.6. Criar um cluster lógico, agregando todos os discos físicos dos servidores contidos na solução, apresentando um único sistema de arquivos ao hipervisor.

6.3.1.7. A solução ofertada deve possuir funcionalidade para expor camada de armazenamento para aplicações físicas (*bare metal*) através do protocolo iSCSI ou NFS ou SMB.

6.3.1.8. A solução ofertada deverá suportar pelo menos dois Hipervisores. A solução ofertada deve oferecer capacidade de conversão de clusters e de cargas de trabalho de um hipervisor para outro a fim de permitir adequação de custos durante renovações de suporte das licenças fornecidas ou aquisição de novas tecnologias de virtualização, preservando o investimento realizado.

6.3.1.9. Deverão ser fornecidas licenças necessárias para utilização de técnicas de otimização de armazenamento, como por exemplo, compressão e desduplicação.

6.3.1.10. A solução deverá garantir replicação síncrona de todos os dados gravados localmente para outros servidores que compõem o cluster para redundância dos dados, cada qual com seu respectivo sistema de armazenamento local com garantia de que a promoção e a demoção dos dados ocorram simultaneamente nos servidores do cluster.

6.3.1.11. A falha ou remoção de um disco não deve interromper o funcionamento de outros discos no mesmo equipamento. Caso a solução não atenda este requisito, deverá ser dimensionada prevendo tolerância a falha simultânea de dois equipamentos no mesmo cluster.

6.3.1.12. Todos os nós do cluster devem participar das operações de reconstrução de disco (*rebuild*), deixando-os mais eficientes à medida que o cluster cresce em número de nós. Caso a solução não atenda a este requisito, deverá ser ofertada com discos de até 3TB (três terabytes) a fim de minimizar o impacto e o tempo de reconstrução.

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS
JRR

6.4. REQUISITOS DE VIRTUALIZAÇÃO E GERENCIAMENTO

6.4.1. A solução deverá ser compatível com o Hipervisor VMware ESXi, na versão 6.5 ou superior, atualmente instalado na **CONTRATANTE**.

6.4.2. A **CONTRATADA** deverá fornecer o licenciamento, suporte e subscrição, durante a vigência da garantia da solução, para o hipervisor nativo da solução, com a respectiva solução de gerenciamento centralizado, ambos em sua edição mais completa, de modo a permitir o uso de todas as suas funcionalidades para configuração e gerenciamento de um ambiente altamente disponível, sendo minimamente capaz de:

6.4.2.1. Permitir operações de *live migration* (migração da máquina virtual para outro host com a máquina virtual em operação);

6.4.2.2. Disponibilizar gerenciador de imagens através de um repositório centralizado e permitir o uso de discos ou imagens nos formatos qcow, qcow2, vmdk, VHD, VHDx, raw, ISO para que seja possível a utilização destes discos e imagens com as máquinas virtuais do cluster;

6.4.2.3. A solução deve ser capaz de distribuir os servidores virtuais entre os nós do cluster de modo que ocorra distribuição da carga.

6.4.2.4. O hipervisor deverá possuir um planejador (*scheduler*) com acesso a telemetria do host para tomar decisões de posicionamento das máquinas virtuais:

6.4.2.4.1. Posicionamento inicial: a melhor posição em um cluster para inicialização da máquina virtual ou carga de trabalho;

6.4.2.4.2. Otimização de tempo de execução: movimento de cargas de trabalho com base em métricas durante tempo de execução.

6.4.2.5. O posicionamento das VMs deverá seguir pelo menos os seguintes fatores:

6.4.2.5.1. Computação (CPU/MEM):

6.4.2.5.1.1. Utilização da CPU;

6.4.2.5.1.2. Utilização de memória;

6.4.2.5.1.3. Contenção de recursos;

6.4.2.5.1.4. Limiares e/ou marcas d'água para métricas de computação.

6.4.2.5.2. Desempenho de armazenamento:

DS JRR

6.4.2.5.2.1. Utilização do processo de gestão das operações de I/O;

6.4.2.5.2.2. Propriedade do disco virtual;

6.4.2.5.2.3. Localização dos volumes.

6.4.2.5.3. Regras de afinidade e anti-afinidade:

6.4.2.5.3.1. Políticas definidas pelo usuário para o local (*host*) onde será executada a VM

6.4.2.5.3.2. Agrupamento de VMs;

6.4.2.5.3.3. Separação de VMs.

6.4.2.6. Com intuito de simplificar as configurações de rede, a solução deverá dispor de switch virtual distribuído baseado em, ou compatível com, *Open Virtual Switch* (OVS), de modo que a gestão seja centralizada e todas as configurações sejam igualmente aplicadas e mantidas entre todos os hosts do cluster.

6.4.2.7. A solução de rede virtual deverá permitir *IP address management* (IPAM) para a configuração de *pools* de endereços IP para atribuição às máquinas virtuais automaticamente sem a necessidade de um serviço de DHCP.

6.4.2.8. A solução deverá permitir a visualização de informações dos switches topo de rack na console Web de administração do cluster. Através do protocolo *Link Layer Discovery Protocol* (LLDP) ou *Cisco Discovery Protocol* (CDP) a solução deverá prover visualização gráfica das portas dos switches que estão conectadas às respectivas portas de redes das unidades computacionais. Adicionalmente, deverá ser possível a configuração dos protocolos SNMP v3 ou SNMP v2c nos switches topo de rack, para visualizar na mesma interface gráfica de gestão do cluster, as informações estatísticas das interfaces dos switches tais como:

6.4.2.8.1. Número de pacotes *unicast* transmitidos e recebidos;

6.4.2.8.2. Número de pacotes transmitidos e recebidos com um erro;

6.4.2.8.3. Número de pacotes transmitidos e recebidos que foram descartados.

6.4.2.9. Permitir operações de alta disponibilidade automatizada, onde em caso de falha de um nó, as máquinas virtuais que dependam desse recurso, sejam automaticamente iniciadas em outro nó.

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS
JRR

6.4.2.10. Ter uma ferramenta de planejamento de capacidade disponível, de forma a permitir a análise dos recursos e indicar máquinas virtuais subdimensionadas, superdimensionadas e inativas, para que seja possível identificação e remediação/otimização através da própria interface de gerenciamento centralizado. A ferramenta de planejamento de capacidade deve permitir simulações de provisionamento de novas aplicações com recomendações de otimização e eventuais capacidades ou equipamentos a serem adicionados ao cluster para que seja possível suportar estas novas aplicações. As simulações poderão ser executadas em múltiplos clusters com seus respectivos Hipervisores.

6.4.2.11. Permitir o monitoramento e análise dos elementos de hardware, storage e máquinas virtuais do cluster de modo que a detecção de anomalias no ambiente possam gerar alertas que permitam a solução de gerenciamento disparar ações automatizadas que possibilitem adequação dos recursos computacionais das máquinas virtuais tais como aumento e redução de processamento e memória, reinicialização de máquinas virtuais, envio de notificações para usuários e sistemas de mensageria, realização de snapshots, chamadas via APIs do tipo REST sem necessidade de intervenção do administrador.

6.4.2.12. A solução deverá ser capaz de automatizar o processo de criação de clusters Kubernetes:

6.4.2.12.1. A solução deverá otimizar a implantação e o gerenciamento de clusters Kubernetes com uma interface gráfica simples e integrada ao gerenciamento centralizado dos clusters hiperconvergentes.

6.4.2.12.2. Todo cluster Kubernetes deverá ser instalado com as ferramentas Prometheus, ElasticSearch, Fluent Bit e Kibana (pilha EFK) para monitoração, registro (*logging*), e alertas. Caso não sejam instaladas com estas ferramentas, deverá ser fornecido com ferramentas semelhantes para exercer as mesmas funções.

6.4.2.12.3. Monitoramento contínuo com alertas exibidos na interface de gestão gráfica.

6.4.2.12.4. Permitir a configuração de clusters com alta-disponibilidade para os *master nodes*, com ou sem balanceador de carga.

6.4.2.12.5. Deverá permitir a gestão do ciclo de vida com atualizações da versão kubernetes de maneira simples e sem interrupções.

6.4.2.12.6. Prover armazenamento persistente através de integração com Container Storage Interface (CSI) conectados ao SDS para armazenamento de blocos e arquivos. Também deverá ser possível configurar armazenamento de objetos compatível com S3;

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS
JRR

6.4.2.12.7. Deverá suportar os modos de acesso ao armazenamento persistente:

6.4.2.12.7.1. Read-Write-Once;

6.4.2.12.7.2. Read-Write-Many.

6.4.2.12.8. Permitir filtrar e analisar logs de sistemas, pods e nós.

6.4.2.12.9. Fornecer um mecanismo de monitoramento que aciona alertas no cluster Kubernetes.

6.4.2.12.10. Deverá usar o sistema de monitoramento de saúde para interagir com o Suporte do fabricante objetivando agilizar a resolução de problemas dos cluster Kubernetes.

6.4.2.12.11. Permitir escalabilidade (*scale out* e *scale in*) dos nodes pela mesma interface gráfica e por linha de comando (CLI).

6.4.2.12.12. Deverá preservar a experiência nativa dos usuários Kubernetes com APIs abertas.

6.4.2.12.13. Permitir desativar autenticação baseada em senha em todos os nodes Kubernetes de forma que seja possível estabelecer o uso de chaves SSH com validade de até 24h (vinte e quatro horas).

6.4.2.13. A solução deve possuir console de administração WEB sem necessidade de instalação de qualquer componente adicional para essa finalidade;

6.4.2.14. A solução de gerenciamento WEB deve ser capaz de gerenciar qualquer hipervisor especificado neste Contrato;

6.4.2.15. A console WEB deve ser acessível por browsers que suportam a tecnologia HTML5.

6.4.2.16. A console WEB deve fornecer acesso à um *Dashboard* principal personalizável com informações da saúde do Sistema (cluster) tanto no site local como em sites remotos, sumário dos equipamentos e das Máquinas Virtuais, visão geral da utilização dos recursos computacionais do cluster (processamento, memória, armazenamento), bem como visualização de alertas e eventos, visualização das informações de desempenho da solução (utilização de banda do cluster, IOPS do cluster e latência do cluster).

6.4.2.17. A solução deve permitir, através de uma interface de gestão gráfica, a atualização do storage definido por software, Hipervisor, BIOS e *firmwares* dos

DS
JRR

dispositivos de todos os equipamentos do cluster de forma simples e automatizada, eliminando a intervenção manual do administrador e parada no ambiente;

6.4.2.18. Com a finalidade de automatizar os processos de implementação, manutenção e gerenciamento do cluster, o sistema operacional em execução na solução hiperconvergente deverá oferecer REST APIs;

6.4.2.19. O gerenciador do cluster deve enviar periodicamente informações e estatísticas, de maneira automática, para o suporte. Esta funcionalidade tem por objetivo aplicar análises avançadas para otimizar a implementação da solução ou atuar proativamente na identificação de problemas. Deverá ser permitido desabilitar este recurso a qualquer momento através da interface WEB;

6.4.2.20. A solução deverá possuir ferramenta de checagem interna integrada a console de gerenciamento, buscando por problemas de saúde no cluster proativamente;

6.4.2.21. Ferramenta de gerenciamento deve oferecer funcionalidade de planejamento de capacidade para crescimento baseado na carga de trabalho projetada;

6.4.2.22. A solução deve permitir que os usuários e administradores personalizem a visualização dos painéis de gerenciamento;

6.4.2.23. Ferramenta de gerenciamento deve possuir funcionalidade de busca (*search*) que suporte busca contextualizada;

6.4.2.24. A Ferramenta deve possuir a funcionalidade de criação de um portal de autosserviço, para que os usuários da infraestrutura disponibilizada pela solução conforme suas permissões, possam Criar, Deletar e Acessar a console de seus servidores virtuais, sem a necessidade da intervenção do administrador da solução;

6.4.2.25. O Portal de Autosserviço, deve ter a capacidade de definir permissões específicas para os usuários dependendo de sua função (*Role Based Access Control* – RBAC), definidas pelo usuário gestor da solução, ou um usuário gestor do portal de autosserviço;

6.4.2.26. A solução deve suportar o envio de alertas críticos automaticamente para o fabricante da solução;

6.4.2.27. Deve suportar envio de alertas e eventos via SNMP.

6.5. REQUISITOS PARA GESTÃO DA BASE DE DADOS - BACKEND METADADOS

6.5.1. A **CONTRATADA** deverá fornecer subscrição para gestão de base de dados Oracle com oito processadores virtuais (vCPUs) que atenderá ao *Backend Metadados* do projeto de *Big Data*.

6.5.2. Permitir automatizar as tarefas para provisionamento, emprego de correções de software (*patching*), gerenciamento do ciclo de vida, clonagem, atualização das bases (*refresh*), proteção contínua e recuperação de bases de dados.

6.5.3. Com objetivo de simplificar o provisionamento de bancos de dados, a solução deverá permitir a definição de perfis de:

6.5.3.1. Software: contendo as imagens de sistema operacional e banco de dados para provisionamento das máquinas virtuais de banco de dados.

6.5.3.2. Computação: parâmetros de configuração de processamento e memória das máquinas virtuais de banco de dados.

6.5.3.3. Rede: definição de rede virtual (VLAN) onde será provisionado o novo servidor de banco de dados.

6.5.3.4. Bancos de Dados: para especificar parâmetros customizados a serem aplicados no banco de dados.

6.5.4. Durante o provisionamento, a solução deverá permitir a escolha para o administrador utilizar um servidor de banco de dados registrado ou criar um servidor.

6.5.5. Também deverá permitir o uso de uma chave SSH pública para acesso ao servidor de banco de dados com opção através do upload de um arquivo e através da inserção direta da chave em campo de texto.

6.5.6. A solução deverá permitir registrar bancos de dados existentes para emprego de proteção contínua capturando e mantendo snapshots e logs transacionais da base de dados de origem conforme definições contidas no agendamento.

6.5.7. A mesma tecnologia deverá permitir a clonagem de bases de dados. Durante a clonagem, a solução deverá permitir a escolha para o administrador utilizar um servidor de banco de dados registrado ou criar um servidor. A ferramenta deverá permitir que o administrador realize o clone de uma base de dados dentro de uma política de proteção contínua, ou seja, recuperar uma base de dados em determinado dia, hora, minuto e segundo.

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS
JRR

6.5.8. Deverá ser possível definir as políticas de retenção dos snapshots diários, semanais, mensais e trimestrais.

6.6. REQUISITOS PARA ARMAZENAMENTO DE DADOS

6.6.1. Após a falha ou indisponibilidade de um equipamento (N+1), o cluster deverá dispor de pelo menos **113TiB (cento e treze tebibytes – base 2)** de capacidade efetiva de armazenamento sendo pelo menos **29TiB (vinte e nove tebibytes – base 2)** na camada de desempenho ou *Tier* 0 (SSD ou NVMe) sem prejuízo para oferta de toda a capacidade no Tier 0. A licitante poderá considerar ganhos com compressão e desduplicação de até 1.4:1. Não será aceita proposta dimensionada com *erasure-coding*.

6.6.2. Deverá ser comprovado o desempenho para banco de dados em cenário totalmente randômico com 70% de leitura, utilizando blocos de 8K, de pelo menos **30.000 IOPS (trinta mil operações de entrada e saída por segundo)** para o cluster. O desempenho de IOPS deverá ser comprovado com latência inferior a 2ms (dois milissegundos). A comprovação poderá ser apresentada através de ferramenta de dimensionamento original do fabricante ou testes realizados em laboratório. A **CONTRATANTE** se reserva ao direito de realizar teste de bancada com o número mínimo de equipamentos necessários para simulação e comprovação do desempenho proposto.

6.6.3. Todos os requisitos de capacidade líquida, desempenho e tolerância a falha são mínimos. A licitante poderá ofertar seus equipamentos com os tipos de dispositivos de armazenamento mais adequados ao cumprimento de todos os requisitos estabelecidos.

6.6.4. Dos 113TiB de capacidade de armazenamento, 10TiB serão destinados ao armazenamento de arquivos para usuários e aplicações (NFS e SMB) e 10TiB ao armazenamento de objetos compatível com protocolo S3.

6.6.5. Caso a solução hiperconvergente ofertada não suporte nativamente o armazenamento de arquivos (NFS e SMB) e de objetos (S3), é facultado a **CONTRATADA** o fornecimento de unidade externa dedicada ao armazenamento de dados não estruturados. Neste caso, deverão ser entregues as mesmas capacidades líquidas e utilizáveis mínimas para o armazenamento de arquivos e para o armazenamento de objetos. O suporte para ambas as soluções (HCI e storage para dados não estruturados) deverá ser realizado pelo mesmo fabricante;

6.6.6. Em qualquer modelo de oferta, a solução deverá atender aos seguintes requisitos para armazenamento de arquivos:

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antonio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá-MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS
JRR

6.6.6.1. Compartilhamento através de protocolos NFSv3 e NFSv4 e SMBv2 e SMBv3. A solução deverá estar devidamente dimensionada para suportar o número de 1.500 (um mil e quinhentos) usuários conectados de forma simultânea;

6.6.6.2. A solução deverá possuir arquitetura na modalidade "*scale-out*", ou seja, ser possível adicionar nós ou máquinas virtuais de acordo com a necessidade de performance, números de usuários conectados de forma simultânea ou escalabilidade de volumetria;

6.6.6.3. A solução deverá suportar escalabilidade para pelo menos 5 (cinco) petabytes de volumetria útil;

6.6.6.4. A solução deverá ser composta de no mínimo 3 nós ou máquinas virtuais, e possuir sistema de Alta Disponibilidade Nativa para realizar o "*fail-over*" automático dos serviços para um nó ou máquina virtual remanescente em caso de falha;

6.6.6.5. Deverá possuir um assistente na própria solução para recomendações de "*scale in*", adição de recursos de CPU e/ou memória nos nós ou máquinas virtuais existentes ou "*scale out*", adição de novos nós ou máquinas virtuais com balanceamento de recursos baseado no nível de utilização da solução;

6.6.6.6. Deverá suportar as seguintes funcionalidades para compartilhamento de arquivos via Protocolo SMB:

6.6.6.6.1. Autenticação via *Active Directory*;

6.6.6.6.2. Filtro de pasta e arquivos para listar apenas aqueles que o usuário possui permissão via *Access-based enumeration* (ABE);

6.6.6.6.3. Habilitar assinatura digital para cada pacote enviado através da rede para assegurar a autenticidade e prevenir adulteração (*SMB Signing*);

6.6.6.6.4. Habilitar encriptação em nível de pasta (*SMB Encryption*);

6.6.6.7. Deverá suportar a organização de pastas compartilhadas entre diferentes servidores em um mesmo local ou geograficamente distantes através de um único "*Single namespace*", inserindo um diretório hierárquico unificado de modo a simplificar a integração com soluções existentes ou futuras através do protocolo DFS-N (*DFS Namespaces*);

6.6.6.8. Deverá suportar autenticação via "*Active Directory*", "*LDAP*" e acesso não gerenciado a compartilhamento via NFSv4 e autenticação via *LDAP* e acesso não gerenciado via protocolo NFSv3;

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS
JRR

6.6.6.9. Deverá suportar acesso multiprotocolo a uma ou mais pastas, ou seja, ser capaz de prover acesso tanto via SMB quanto via NFS a um mesmo compartilhamento utilizando de protocolos como Windos ACLs (*Access Control Lists*) e *Unix mode bits*;

6.6.6.10. Deverá suportar a configuração de acesso a *Home Share* por nível de diretório (*User Home Shares*);

6.6.6.11. Deverá suportar a otimização de um determinado compartilhamento de acordo com a natureza de tamanho do bloco, sendo possível personalizar entre:

6.6.6.11.1. Padrão: 64KB por bloco;

6.6.6.11.2. Randômico: 16KB por bloco;

6.6.6.11.3. Sequencial: 1MB por bloco.

6.6.6.12. A solução deverá possuir um painel de visualização de utilização que especifique as seguintes métricas em um intervalo mínimo de 7 dias:

6.6.6.12.1. Número de arquivos existentes;

6.6.6.12.2. Capacidade Utilizada;

6.6.6.12.3. Número de conexões abertas;

6.6.6.12.4. Espaço consumido por compartilhamento.

6.6.6.13. A solução deverá possuir um painel de visualização de performance que especifique as seguintes métricas em um intervalo mínimo de 7 dias:

6.6.6.13.1. Latência;

6.6.6.13.2. Banda (MB/s);

6.6.6.13.3. IOPs (I/O por segundo).

6.6.6.14. Deverá suportar a aplicação de cotas para controle de consumo do sistema de arquivos de forma granular a modo de avisar quando o usuário atingir consumo limite (*soft limit*) ou bloquear a escrita de novos arquivos (*Hard limit*). A cota deve ser possível de ser aplicada nos seguintes elementos:

6.6.6.14.1. Por usuário;

6.6.6.14.2. Por grupo;

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS
JRR

6.6.6.14.3. Nível da própria pasta no momento de sua criação (*Directory Level Quotas*).

6.6.6.15. Deverá suportar o bloqueio de gravação de arquivos baseado em sua extensão a nível de servidor ou pasta, para os protocolos SMB, NFS e compartilhamentos multiprotocolo;

6.6.6.16. Deverá suportar o envio de eventos de notificação em tempo real como, criação, deleção, leitura, escrita e mudança de permissão em qualquer arquivo armazenado na solução a fim de retenção e auditoria através de soluções como "*syslog servers*";

6.6.6.17. Deverá ser fornecido nativamente ou através de integração com software de terceiros, solução que seja capaz de capturar os eventos de notificação e seja capaz de prover de forma simplificada um *dashboard* de auditoria que forneça no mínimo as seguintes informações:

6.6.6.17.1. Tendência de capacidade, com foco no que foi consumido e como foi na linha do tempo;

6.6.6.17.2. Idade dos arquivos, demonstrando cálculo de quando o arquivo foi alterado pela última vez e a porcentagem dos dados baseado no intervalo de variação de sua idade;

6.6.6.17.3. Detecção de anomalias, demonstrando todas as operações que excedem uma determinada política pré-determina, como a deleção de múltiplos arquivos em um intervalo menor do que 1 (uma) hora;

6.6.6.17.4. Distribuição por tamanho e tipo de arquivo;

6.6.6.17.5. Ranking dos usuários mais ativos no sistema de armazenamento;

6.6.6.17.6. Ranking dos arquivos mais acessados no sistema de armazenamento;

6.6.6.17.7. Lista das operações mais frequentes (criação, escrita, leitura, deleção e alteração de permissionamento) seja pela média, tendência ou pico da operação.

6.6.6.18. A solução de auditoria deverá ser capaz de analisar e reter para consulta um tempo mínimo de 12 (doze) meses de dados capturados.

6.6.6.19. Deverá suportar a integração de software de antivírus de terceiros através do protocolo ICAP (*Internet Content Adaptation Protocol*) para compartilhamento via SMB e permitir a varredura de arquivos em tempo real quando o arquivo é aberto, fechado ou modificado.

DS
JRR

6.6.6.20. A interface de gerenciamento da solução de armazenamento deverá mostrar o estado do arquivo após varredura de arquivos, tal como modo de quarentena, além dos eventos ocorridos com os mesmos (limpo, quarentena, deletado).

6.6.6.21. A interface de gerenciamento da solução de armazenamento deverá mostrar a lista de arquivos escaneados, as ameaças detectadas e os arquivos colocados em modo quarentena;

6.6.6.22. A interface de gerenciamento da solução de armazenamento deverá realizar ações voltadas aos arquivos, tais como:

6.6.6.22.1. *Rescan*;

6.6.6.22.2. Mover os arquivos para fora da Quarentena;

6.6.6.22.3. Deletar arquivos na quarentena de forma permanente.

6.6.6.23. Deverá suportar a criação de domínios de proteção de forma automatizada a fim de proteger com cópias locais e remotas a solução de armazenamento, através de agendamentos periódicos de snapshots (horas, dias, semanas e meses)

6.6.6.24. Deverá suportar a possibilidade de recuperação a nível de arquivo pelo próprio usuário final (*self service restore*) baseado no agendamento de cópias locais (*snapshots*) previamente estabelecidos. Para o protocolo SMB a recuperação deverá ser realizada pela propriedade de Versões Prévias da pasta destino. Para o protocolo NFS, através da listagem do subdiretório escondido (snapshot)

6.6.6.25. Deverá suportar a replicação remota habilitando a recuperação de desastres com intervalo mínimo de um minuto entre cópias para um segundo sistema de armazenamento ou cluster;

6.6.7. Referente ao Serviço de Armazenamento de Objetos, deverá ser configurado de maneira altamente disponível e distribuído, projetado com uma interface de API REST compatível com o *Amazon Web Services Simple Storage Service* (AWS S3) para lidar com dados não estruturados e gerados por máquina para fins de armazenamento para backup, armazenamento e retenção de longo prazo e desenvolvimento de aplicativos nativos para nuvem usando APIs padrão S3.

6.6.7.1. Também deverá possuir arquitetura na modalidade "*scale-out*", ou seja, ser possível adicionar nós, clusters ou máquinas virtuais de acordo com a necessidade de performance, números de requisições ou escalabilidade de volumetria;

DS
JRR

6.6.7.2. A solução deverá estar devidamente dimensionada para suportar o número de 1.500 (mil e quinhentas) requisições por segundo;

6.6.7.3. A solução deverá possuir um assistente para criação de *Object Stores* capaz de dimensionar os recursos computacionais necessários com base no número de requisições por segundo e ainda permitir adequação destes recursos antes mesmo da criação do *Object Store* de acordo com a necessidade;

6.6.7.4. Permitir a criação de unidades organizacionais lógicas (*buckets*) para armazenamento dos objetos. Os objetos consistem em dados e metadados que descrevem os dados;

6.6.7.5. Deverá permitir a configuração de serviços de diretórios, compatível com *Microsoft Active Directory* e *OpenLDAP*, para adicionar facilmente pessoas que devem ter acesso a objetos;

6.6.7.6. Deverá permitir a geração e o controle de chaves de acesso para garantia de segurança;

6.6.7.7. A solução deverá permitir o compartilhamento dos "*buckets*" com os usuários que possuem as chaves de acesso, assim como, permitir a delegação de permissões como escrita e leitura de acordo com o nível de acesso

6.6.7.8. Deverá permitir a listagem dos *buckets* compartilhados, identificando quais usuários possuem acesso a cada um deles;

6.6.7.9. Deve ser possível gerenciar os *buckets* e seus respectivos objetos usando APIs REST compatíveis com a solução de gerenciamento central do cluster ou S3 depois que um administrador autorizar os aplicativos e usuários a acessarem os *buckets* adequadamente;

6.6.7.10. A solução deverá permitir o versionamento de múltiplas versões de um objeto dentro de um mesmo *bucket*. Opção deverá ser possível de ser habilitada na criação ou edição de um *bucket* existente;

6.6.7.11. A solução deverá permitir a criação de um conjunto de regras para definir ações do ciclo de vida de um objeto, como permitir que um objeto se apague automaticamente depois de um determinado número de dias, meses ou anos, assim como, apagar determinada versão de um objeto após um determinado período;

DS JRR

6.6.7.12. A solução deverá permitir a prevenção da deleção ou alteração de um objeto existente de acordo com um determinado período de retenção, utilizando de algoritmos de WORM (*Write-Once-Rean-Many*);

6.6.7.13. A solução deverá 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);

6.6.7.14. Deverá suportar a atribuição de políticas de cotas de utilização notificando os respectivos usuários de acordo com nível de consumo de espaço ou número de *buckets* criados;

6.6.7.15. Deverá suportar o envio de eventos de notificação em tempo real como, criação, deleção, leitura, escrita e mudança de permissão em qualquer objeto armazenado na solução a fim de retenção e auditoria através de soluções como "*syslog servers*";

6.7. REQUISITOS SUPORTE TÉCNICO

6.7.1. Durante a vigência do contrato, os softwares deverão contar com suporte 24x7 e atendimento a chamados em até uma hora.

6.7.2. O portal de suporte do fabricante deverá permitir o registro de pelo menos seis administradores da **CONTRATANTE** responsáveis por realizar gestão de licenças e abertura de chamados.

6.7.3. O fabricante deverá disponibilizar em seu portal de suporte, recomendações específicas para os clusters da **CONTRATANTE** a fim de facilitar e agilizar a implantação de atualizações e correções necessárias para o ambiente.

6.7.4. Deverá prover suporte proativo com abertura automática de chamados a partir de alertas críticos gerados pelo sistema.

6.7.5. Durante o primeiro ano de operação da solução, o fabricante deverá nomear um Gerente Técnico remoto, responsável por:

6.7.5.1. Atuar como ponto focal principal e proativo no fabricante para tratar de questões comerciais, técnicas e de suporte.

6.7.5.2. Coordenar reuniões com especialistas em produtos, engenharia, suporte e serviços

6.7.5.3. Coordenar questões técnicas e críticas aos negócios da **CONTRATANTE** com a equipe técnica do fabricante.

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03.929.049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS
JRR

6.7.5.4. Priorizar novos recursos solicitados pela **CONTRATANTE**.

6.7.5.5. Coordenar escalonamentos de suporte com todos os produtos de software envolvidos na solução quando ocorrerem problemas.

6.7.5.6. Realizar verificações de saúde abrangentes e apresentar recomendações para alcançar os resultados.

6.7.5.7. Conduzir e coordenar o gerenciamento, escalonamento e resolução de problemas.

6.7.5.8. Melhorar a utilização da capacidade recomendando análises e otimizações no ambiente.

6.7.5.9. Otimizar o gerenciamento de serviços e o uso de licenças.

6.7.5.10. Revisar versões de software e fornecer recomendações para padronização e economia.

6.7.5.11. Serviço personalizado para análises e relatórios de disponibilidade, confiabilidade e utilização da solução.

6.7.5.12. Análise de capacidade e utilização da solução.

6.7.5.13. Gerar relatórios de com auditorias de desempenho e saúde.

6.7.5.14. Análise de eventos e relatórios sobre casos críticos, incluindo a causa raiz do problema.

6.7.5.15. Desenvolver um plano e recomendar estratégia para escalonamento, maximizando o retorno sobre o investimento.

6.7.5.16. Definir métricas de sucesso para o negócio da **CONTRATANTE**.

6.7.5.17. Auxiliar com o planejamento e preparação para eventos significativos ou lançamentos de grandes projetos.

6.7.5.18. Rever o ciclo de vida da solução.

6.7.5.19. Avaliação de aprendizagem da equipe técnica da **CONTRATANTE**.

6.7.5.20. Facilitar a capacitação de produtos e tecnologia.

6.7.5.21. Compartilhar as melhores práticas e documentações específicas para o ambiente da **CONTRATANTE**.

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS
JRR

6.7.5.22. Facilitar apresentações de roteiro de produtos com especialistas do fabricante.

CLÁUSULA SÉTIMA – DO HARDWARE PARA INFRAESTRUTURA EM CLUSTER

7.1. REQUISITOS PARA DIMENSIONAMENTO DO CLUSTER

7.1.1. Todos os equipamentos e seus componentes deverão ser compatíveis e constar na matriz de compatibilidade do conjunto de softwares para nuvem privada especificados no item 1.

7.1.2. Será aceita oferta de clusters configurados com equipamentos do tipo *appliances* ou nós certificados desde que a solução contemple ferramenta de gestão e *upgrades* de versões dos firmwares, drivers e softwares relacionados de maneira centralizada, automatizada e com capacidade de orquestração para evacuação de máquinas virtuais e reinicialização de equipamentos sempre que necessário.

7.1.3. Todos os equipamentos deverão ser fornecidos com todos os acessórios necessários para sua instalação, incluindo, mas não se limitando a, trilhos para montagem em rack, cabos de alimentação elétrica, além de todas as licenças de softwares necessárias para o funcionamento da solução conforme requisitos mínimos deste Contrato.

7.1.4. Todos os recursos computacionais (processamento, memória e armazenamento) deverão ser úteis para as aplicações da **CONTRATANTE**, ou seja, deverão estar disponíveis para as aplicações após serem descontadas todas as perdas da solução de armazenamento definida por software (SDS). Caso ocorra necessidade de manter uma infraestrutura separada para gerenciamento dos clusters, esta deverá ser fornecida pela **CONTRATADA** (hardware, softwares e serviços de instalação, configuração e treinamento).

7.1.5. A **CONTRATADA** deverá então comprovar através de relatório extraído da ferramenta de dimensionamento ou manuais originais do respectivo fabricante, as perdas / overhead considerados na proposta. A **CONTRATANTE** também poderá exigir teste de bancada para comprovação dos requisitos editalícios.

7.1.6. Com o intuito de anular a exposição à vulnerabilidades conhecidas e ao mesmo tempo não haver perda de desempenho decorrente da correção não estrutural para estas vulnerabilidades, os processadores ofertados deverão ser da última geração disponível pelo fabricante da pastilha.

DS JRR

7.1.7. Objetivando atender aos requisitos de projetos de aprendizagem profunda (*deep learning*), os processadores deverão possuir instruções para redes neurais vetoriais (VNNI) compatíveis com AVX-512.

7.1.8. A configuração de memória dos equipamentos deverá ser constituída de maneira simétrica ocupando todos os canais de memória dos processadores com módulos idênticos em padrão e capacidade para garantia de melhor desempenho. Não serão aceitas configurações com módulos diferentes entre si.

7.1.9. Quanto a capacidade de armazenamento de dados, deverão ser calculadas e descontadas todas as perdas com formatação, configuração de RAID (quando aplicável) em nível para prover o melhor desempenho para o SDS, fator de replicação (dado original e uma réplica em equipamentos distintos no mesmo cluster e no mesmo site), alta-disponibilidade (HA), área de manobra (*slack space*) máxima e, também quando aplicável, grupos de discos em número máximo conforme estabelecido nos manuais do fabricante da solução de armazenamento definida por software, para reduzir impacto durante operações de reconstrução e re-sincronização. Além disso, deverá considerar as perdas relativas à soma de verificação (*checksum*) para garantia de integridade dos dados e quaisquer outras perdas / overhead da solução de armazenamento definida por software, inclusive perdas decorrentes do emprego de tecnologias para ganhos de eficiência como desduplicação e compressão.

7.1.10. A **CONTRATADA** poderá considerar ganhos com técnicas de desduplicação e compressão desde que estes ganhos sejam factíveis e não impossibilitem o atendimento aos demais requisitos deste Contrato e do Termo de Referência. A solução deverá estar licenciada para o uso destas funcionalidades. Caso a solução requeira evacuação dos dados e/ou reformatação dos discos para ativar ou desativar estas funcionalidades, a área de manobra (*slack space*) para esta evacuação deverá ser considerada com pelo menos 30% (trinta por cento) da capacidade do cluster, conforme recomendação expressa no manual do fabricante da solução de armazenamento definida por software. Se a solução não for capaz de otimizar os dados no nível do cluster (global), a **CONTRATADA** deverá considerar 30% (trinta por cento) de capacidade de armazenamento útil adicional para o cluster a fim de compensar a ineficiência da solução em manter cópias redundantes no cluster.

7.1.11. Para redução dos riscos de perda ou corrupção de dados em caso de falha de disco durante processos de atualização de firmwares e softwares que requeiram reinicialização de equipamentos, a falha de um disco de cache ou de capacidade não deve impactar ou interromper o funcionamento de outros discos na solução. Caso a solução não atenda este requisito, a capacidade de armazenamento útil do cluster deverá considerar a existência

DS
JRR

de três cópias dos dados (original e duas réplicas). Neste cenário a **CONTRATADA** também deverá considerar tempo de reposição de discos em no máximo 4h (quatro horas), a fim de reduzir o tempo e o impacto de reconstrução (*rebuild*) no cluster. O fabricante deverá garantir a troca de quaisquer discos mesmo quando as aplicações excederem seus limites de gravação (DWPD).

7.1.12. Para soluções que dependam da configuração de RAID, a **CONTRATADA** deverá considerar, no dimensionamento da capacidade útil, a quantidade de grupos de discos e o nível de RAID que garantam o melhor desempenho da solução ofertada conforme estabelecido nos manuais do respectivo fabricante da solução de armazenamento definida por software.

7.1.13. A solução deverá possuir suporte com número de discagem gratuita e portal web para abertura de chamados;

7.1.14. A solução visará o emprego de configurações para um ambiente altamente disponível, com garantia e suporte técnico do fabricante durante 60 (sessenta) meses, na modalidade 24x7 com atendimento para chamados em até 1 (uma) hora e reposição de peças defeituosas até o próximo dia útil.

7.1.15. Cada cluster deverá prover os seguintes recursos computacionais úteis para processamento das aplicações:

7.1.15.1. Processamento:

7.1.15.1.1. SPECrate2017_int_base 582 ou superior.

7.1.15.1.2. Os processadores deverão operar a uma frequência mínima de 2.9GHz, inclusive na velocidade de comunicação com a memória.

7.1.15.1.3. A definição de NUMA para execução das máquinas virtuais com o devido desempenho, cada CPU deverá prover pelo menos dezesseis núcleos de processamento.

7.1.15.2. Memória:

7.1.15.2.1. Pelo menos **1843GB (hum mil, oitocentos e quarenta e três gigabytes) de memória RAM** ou superior.

7.1.15.3. Armazenamento:

7.1.15.3.1. A configuração de discos e agrupamentos necessária para atender a capacidade de **113TiB (cento e treze tebibytes – base 2)** e o desempenho do cluster com **30.000**

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03.929.049/0001-11
Avenida Andre Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá-MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS
JRR

IOPS (trinta mil operações de entrada e saída por segundo) conforme estabelecido no item 1.6 deste edital.

7.1.15.4. Comunicação:

7.1.15.4.1. Referente a capacidade de comunicação, cada equipamento que compõe o cluster deverá ser configurado com pelo menos 4 (quatro) portas de rede 10/25GbE com conectores SFP28 em placas idênticas entre si. Para cada porta de rede deverá ser fornecido um cabo de conexão direta tipo DAC ou Twinax de 3m (três metros) de comprimento para conexão com os switches MoR especificados neste edital.

7.1.15.5. Instalação Física e Cabeamento:

7.1.15.5.1. Poderá ser realizada por técnico capacitado da **CONTRATADA** seguindo orientações do fabricante para emprego das melhores práticas.

7.1.15.5.2. Em caso de restrições de viagem devido a pandemia, será aceita coordenação e colaboração dos esforços para instalação física em conjunto com a equipe técnica da **CONTRATANTE** até que seja disponibilizado acesso remoto para que o técnico responsável do fabricante da solução conduza as atividades de configuração do ambiente.

CLÁUSULA OITAVA – DO COMUTADORES DE REDE

8.1. REQUISITOS PARA COMUTADORES DE REDE

8.1.1. Cada unidade deverá contemplar pelo menos dois comutadores de rede para garantia de redundância. O conjunto deve prover o número de portas necessárias para conexão de todas as interfaces de rede do cluster, sendo o mínimo estabelecido em ao menos 36 (trinta e seis) portas 25Gbps e pelo menos 8 (oito) portas 100Gbps, todas licenciadas e prontas para uso. Deverão ser fornecidos todos os acessórios para instalação em rack padrão 19" e o fluxo de ventilação com ingestão de ar frio pelas fontes e exaustão de ar ente pelas portas de comunicação, para que todas as conexões de rede fiquem concentradas na parte traseira do rack.

8.1.2. O equipamento deverá vir acompanhado com todo hardware e licenciamento de portas e softwares necessários para o perfeito funcionamento do equipamento e comunicação com os equipamentos do cluster;

8.1.3. Deverá suportar latência inferior a 400ns (quatrocentos nanossegundos).

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS JRR

8.1.4. Cada switch ofertado, deve possuir altura máxima 1U, com dimensões apropriadas para montagem em rack de 19''

8.1.5. Cada switch ofertado, assim como seus acessórios, módulos, cabos e componentes, devem ser do mesmo fabricante.

8.1.6. Deve ser compatível com Ansible e Puppet a fim de automatizar tarefas no ambiente.

8.1.7. Deve ser gerenciável via SNMP versões 1, 2 e 3.

8.1.8. Deve permitir a configuração de Link Layer Discovery Protocol (LLDP), ou semelhante, a fim de permitir a descoberta de dispositivos conectados à rede que divulgam detalhes sobre sua própria configuração, identificação e capacidades.

8.1.9. Deve ser gerenciável via Telnet.

8.1.10. Deve implementar SSH versão 2.

8.1.11. Deve implementar o protocolo Syslog para funções de "logging" de eventos.

8.1.12. Deve implementar o protocolo NTP (Network Time Protocol).

8.1.13. Deve implementar o espelhamento de tráfego de uma porta para uma outra porta específica.

8.1.14. Deverá ser fornecido 01 (um) cabo console.

8.1.15. Cada switch deverá ser fornecido com um cabo para conexão direta entre os switches com pelo menos 0.5m (meio metro) de comprimento. Além disso, deverá ser fornecido um cabo para conexão direta entre os switches com pelo menos 5m (cinco metros) de comprimento.

8.1.16. A infraestrutura de rede deve suportar funções Zero Touch Provisioning (ZTP) promovendo a escalabilidade dos elementos de rede de maneira simples e com o menor envolvimento operacional. Será permitido o uso de pen drives para executar esta função de maneira mais efetiva possível.

8.1.17. Os switches deverão contar com 5 anos de garantia e suporte 24x7 com atendimento em até duas horas e reposição de peças no próximo dia útil.

DS
JRR

8.1.18. A **CONTRATADA** deverá prover o licenciamento necessário para o perfeito funcionamento da solução prevendo a utilização de todas as portas, bem como suas respectivas conectorizações.

8.1.19. A **CONTRATADA** deverá realizar a instalação posicionando pelo menos dois equipamentos em altura proporcional a metade do rack (MoR) com as portas posicionadas para a traseira do rack para facilitar a conexão dos cabos e desta forma, o fluxo de ar dos equipamentos deverá liberar ar quente pelas portas de conexão de rede. Os racks padrão 19" (dezenove polegadas) serão fornecidos pela **CONTRATANTE**.

8.1.20. A **CONTRATADA** deverá realizar a configuração dos equipamentos garantindo a integração com a solução hiperconvergente de modo a permitir visibilidade das interfaces de rede conectadas através da interface de gestão da solução hiperconvergente, seguindo as melhores práticas do(s) fabricante(s).

8.2. ACESSÓRIOS

8.2.1. Deverá contemplar 2 (dois) transceivers QSFP28 SR4 para 100G e respectivos cabos de fibra óptica OM3, ou superior, com 15m (quinze metros) de comprimento.

8.2.2. Deverá contemplar 2 (dois) cabos de conexão direta, tipo DAC ou twinax, de 100G QSFP+ 1m (um metro).

8.2.3. Deverá contemplar 2 (dois) cabo de conexão direta, tipo DAC ou twinax, de 100G QSFP+ 5m (cinco metros).

8.2.4. Os acessórios especificados deverão ser do mesmo fabricante do switch ou oferta OEM compatível que não afete o atendimento de garantia e suporte.

CLÁUSULA NONA – DA IMPLANTAÇÃO DA SOLUÇÃO

9.1. REQUISITOS PARA IMPLANTAÇÃO DA SOLUÇÃO

9.1.1. A **CONTRATADA** deve garantir que todos os equipamentos, componentes, acessórios e cabos de conexão para interligar fisicamente todos os componentes da solução sejam entregues;

9.1.2. Todas as configurações relacionadas a solução serão realizadas por profissional do fabricante em conjunto com os requisitos fornecidos pelo **CONTRATANTE** para o ambiente em questão;

DS
JRR

9.1.3. A **CONTRATADA** deverá prover serviços profissionais do fabricante para efetuar, no mínimo, os seguintes serviços relacionados para cada cluster:

9.1.3.1. Planejamento do projeto;

9.1.3.2. Configuração do cluster inicial conforme recomendação do fabricante;

9.1.3.3. Configurar os equipamentos para funcionamento em alta disponibilidade, com múltiplos caminhos redundantes aos switches;

9.1.3.4. Ativação e configuração do hipervisor em cada servidor que compõe o cluster da solução de hiperconvergência;

9.1.3.5. Configuração da solução de abertura automática de chamados junto ao fabricante;

9.1.3.6. Configuração do ambiente, seguindo as melhores práticas do fabricante, contemplando no mínimo as atividades relacionadas a criação do cluster, unidades de armazenamento, rede virtual, balanceamento de carga, desduplicação e compressão, hipervisor, datacenter virtual bem como demais funcionalidades relacionadas a segurança;

9.1.3.7. Configuração da estrutura de rede virtual do hipervisor (pelo menos dois Switches Virtuais e cinco grupos de portas ou VLANs);

9.1.3.8. Instalação, configuração e integração da solução de gerenciamento centralizado da solução de armazenamento de dados definida por software e do ambiente de virtualização;

9.1.3.9. Para migração do ambiente existente a **CONTRATADA** deverá confeccionar um Plano de Migração para 50 (cinquenta) servidores virtuais, a ser aprovado pela **CONTRATANTE** constando os procedimentos que serão realizados, dados que serão migrados, cronograma, testes, homologação e contingenciamento;

9.1.3.10. Será de responsabilidade da **CONTRATADA** quaisquer custos relacionados ao licenciamento de softwares ou ferramentas adicionais para migração;

9.1.3.11. O processo de migração deverá ser iniciado imediatamente após a conclusão da implantação do novo ambiente;

9.1.3.12. A validação dos dados existentes a serem migrados será de responsabilidade da **CONTRATANTE**. A **CONTRATADA** deverá prover o modelo de dados do novo sistema para que as informações sejam disponibilizadas neste formato e verificar a consistência desses dados após a migração;

DS
JRR

9.1.3.13. Desenho e implantação da solução de armazenamento de arquivos e de objetos:

9.1.3.13.1. Desenho e dimensionamento da solução de armazenamento de objetos, armazenamento de arquivos, compartilhamentos e exportações.

9.1.3.13.2. Planejamento do projeto com status de progresso.

9.1.3.13.3. Implantação da solução de armazenamento de arquivos e objetos.

9.1.3.13.4. Criação de alvos de montagem.

9.1.3.13.5. Realização de workshop para levantamento detalhado dos requisitos e revisão do desenho da solução.

9.1.3.13.6. Teste e validação da implementação da solução.

9.1.3.13.7. Documentação *as-built* de toda a implantação da solução.

9.1.3.13.8. Transferência de conhecimento.

9.1.3.13.9. Este serviço tem um escopo de dois dias e deverá incluir 10 (dez) participantes.

9.1.3.14. Workshop para orientar a migração do serviço de arquivos (NAS) atualmente instalado em sistemas distribuídos, para a solução de armazenamento de arquivos especificada neste Contrato:

9.1.3.14.1. Planejamento do projeto.

9.1.3.14.2. Realização de workshop para levantamento detalhado dos requisitos e revisão do desenho da solução.

9.1.3.14.3. Migração de até 20 (vinte) compartilhamentos ou 5TB (cinco terabytes) de dados.

9.1.3.14.4. Teste e validação da migração.

9.1.3.14.5. Transferência de conhecimento de pelo menos 2h (duas horas).

9.1.3.14.6. Documentação dos procedimentos.

9.1.3.14.7. Limpeza de compartilhamento de arquivos obsoletos.

9.1.3.14.8. Calibração básica de desempenho.

9.1.3.14.9. Implementação de permissão no nível de compartilhamento.

DS JRR

9.1.3.15. Reunião para levantamento dos requisitos detalhados e revisão de projeto para definir o plano de proteção de dados para diferentes aplicações;

9.1.3.15.1. Implementação das opções integradas para Proteção de Dados, incluindo solução de recuperação de desastre com replicação síncrona e assíncrona com base nos requisitos de RPO e RTO das aplicações;

9.1.3.15.2. Criação de pelo menos uma política de proteção para 5 (cinco) VMs de teste para recuperação em site secundário, estabelecendo sequência de inicialização, reconfiguração de rede, execução de *script* para configurar de DNS no site secundário;

9.1.3.15.3. Teste e validação de failover e restauração de até 5 (cinco) VMs de teste;

9.1.3.15.4. A **CONTRATANTE** será responsável por prover a largura de banda e latência de rede adequadas entre os sites para dar suporte às suas necessidades de RPO / RTO;

9.1.3.15.5. Transferência de conhecimento com pelo menos 24 horas comerciais para a equipe da **CONTRATANTE**;

9.1.3.16. Deverá prover workshop para o desenho do projeto para implantação da ferramenta de gestão da base de dados.

9.1.3.16.1. Alinhamento sobre os objetivos;

9.1.3.16.2. Levantamento dos requisitos de negócio, técnicos, restrições, riscos e premissas;

9.1.3.16.3. Reuniões específicas com os responsáveis pela infraestrutura e bases dados Oracle;

9.1.3.16.4. Revisão e validação dos requisitos para a nova infraestrutura;

9.1.3.16.5. Endereçar requisitos identificados

9.1.3.16.5.1. Revisão do dimensionamento do cluster HCI, VM e base de dados;

9.1.3.16.5.2. Requisitos de rede;

9.1.3.16.5.3. Desenho da base de dados em cluster (se aplicável);

9.1.3.16.5.4. Segurança;

9.1.3.16.5.5. Proteção de dados;

DS
JRR

9.1.3.16.5.6. Disponibilidade;

9.1.3.16.5.7. Recuperabilidade.

9.1.3.16.6. O desenho contemplara melhores práticas tanto para infraestrutura quanto para engine de base de dados.

9.1.3.17. Workshop para migração da base de dados

9.1.3.17.1. Análise dos dados previamente descobertos através do trabalho em conjunto com as equipes de administração de infraestrutura e base de dados;

9.1.3.17.2. Discutir objetivos de migração tais como requisitos de disponibilidade de aplicação, janelas de manutenção indisponibilidade permitida para cada base de dados;

9.1.3.17.3. Revisar requisitos de dimensionamento e desempenho da base de dados;

9.1.3.17.4. Discutir opções de migração e restrições para cada método de migração com base nas versões de suas bases de dados e disponibilidade de sistemas operacionais e aplicações;

9.1.3.17.5. Prover um plano de migração;

9.1.3.17.6. Conduzir a migração de uma base de testes com até 200GB na mesma versão, para o cluster HCI.

9.1.3.18. Implantação da ferramenta de Gestão de Base de Dados:

9.1.3.18.1. Sessão de visão geral e introdução da tecnologia:

9.1.3.18.2. Visão geral da arquitetura e dos componentes da solução de armazenamento definida por software, hipervisor e as ferramentas de gestão;

9.1.3.18.3. Revisão das características e funções da ferramenta incluindo provisionamento, clonagem e gestão de patches juntamente com casos de uso comuns;

9.1.3.18.4. Sessão de imersão nos conceitos e construções da ferramenta, tais como Perfis, funcionalidades de proteção de dados e acesso programático via CLI e interfaces API;

9.1.3.18.5. Demonstração do uso perfis de Software, Compute, Network e parâmetros de bancos de dados para realização de operações com simplicidade através da interface gráfica;

DS
JRR

9.1.3.18.6. Demonstrar como um servidor de banco de dados virtualizado pode ser registrado e protegido pela ferramenta para facilitar a proteção e a clonagem da base de dados;

9.1.3.18.7. Demonstrar em um ambiente não produtivo como simplificar o gerenciamento de patches para bases de dados Oracle;

9.1.3.18.8. Discutir diferentes abordagens para migrar bases legadas (físicas ou virtuais) para a plataforma contratada.

9.1.3.19. Desenho e configuração da ferramenta para qualquer cenário a seguir:

9.1.3.19.1. Habilitar o provisionamento de novas bases e servidores de bancos de dados (até dois perfis de SLAs, Software, Compute, Network e parâmetros de banco de dados Oracle);

9.1.3.19.2. Clonar uma base de dados a partir da Proteção em um servidor de banco novo ou existente rodando no cluster HCI, incluindo *refresh* agendado dos dados (validar até dois clones de banco);

9.1.3.19.3. Atribuir redes através da interface de gestão e criar perfis de rede que serão utilizados para provisionamento de bases de dados (até dois Perfis de Rede);

9.1.3.19.4. Exibir e demonstrar os fluxos para gestão de *patches* de bases de dados para um servidor Oracle;

9.1.3.19.5. Demonstrar e configurar RBAC e Notificações para duas contas de usuários;

9.1.3.19.6. Transferência de conhecimento incluindo uma sessão de revisão/coaching durante o deployment.

9.1.3.20. Arquitetura de Backup e Gestão de Cópias das bases de dados (CDM):

9.1.3.20.1. Visão geral da arquitetura e do conceito de CDM;

9.1.3.20.2. Revisão das características e funções ferramenta para CDM, incluindo recuperação de base, clonagem com snapshot e *Point in Time Recovery* (PITR);

9.1.3.20.3. Demonstrar no ambiente instalado como um servidor de banco de dados executando no cluster HCI pode ser registrado na funcionalidade de Proteção para aplicar níveis de serviço (SLAs);

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03.929.049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS
JRR

9.1.3.20.4 Discutir e demonstrar opções de CDM para criação de clones:

9.1.3.20.4.1. Agendamento;

9.1.3.20.4.2. *Refresh*;

9.1.3.20.4.3. Execução de comandos pré / pós clonagem.

9.1.3.20.5. Sessão de imersão técnica descrevendo arquitetura de backup de qualquer base de dados e como as construções de níveis de serviço são baseadas em políticas de backup;

9.1.3.20.6. Explanar o significado e a importância da funcionalidade de proteção de dados na definição das políticas de backup;

9.1.3.20.7. Explicar como configurar níveis de serviço (SLAs) em termos de backup e retenção;

9.1.3.20.8. Compreender os requisitos de nível de serviço da **CONTRATANTE** e demonstrar a criação de políticas de backup;

9.1.3.20.9. Gestão de backup de bases de dados utilizando SLAs:

9.1.3.20.10. Frequência de *snapshot* baseada nas definições de RPO e RTO;

9.1.3.20.11. Requisitos de *log catchup*.

9.1.3.20.12. Demonstrar a recuperação de base de dados a partir da funcionalidade de proteção no ambiente instalado;

9.1.3.20.13. Transferência de conhecimento incluindo uma sessão de revisão/*coaching* durante o *deployment*.

9.1.3.21. Após concluídos os serviços relacionados a instalação, deverão ser realizados testes completos visando a garantia de alta-disponibilidade.

9.1.3.22. Documentação *As-built* com diagramas da arquitetura e resultados dos testes;

9.1.4. Toda e qualquer despesa relacionada ao transporte, alimentação e hospedagem se necessários para os profissionais responsáveis pela execução dos serviços, deverá ocorrer por conta da **CONTRATADA** ou do próprio fabricante, sem quaisquer ônus para o **CONTRATANTE.**

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03.929.049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS
JRR

CLÁUSULA DÉCIMA – DA MIGRAÇÃO

10.1. REQUISITOS PARA MIGRAÇÃO

10.1.1. A **CONTRATADA** deverá elaborar um Plano de Migração a ser aprovado pela **CONTRATANTE** constando os procedimentos que serão realizados, dados que serão migrados, cronograma, testes, homologação e contingenciamento.

10.1.2. O processo de migração deverá ser iniciado imediatamente após a conclusão da implantação do novo ambiente.

10.1.3. A validação dos dados existentes a serem migrados será de responsabilidade da **CONTRATANTE**. A **CONTRATADA** deverá prover o modelo de dados do novo sistema para que as informações sejam disponibilizadas neste formato e verificar a consistência desses dados após a migração.

10.1.4. A **CONTRATANTE** possui diversas aplicações virtualizadas e não virtualizadas, o acesso a relação das aplicações assim como todas as informações dos servidores existentes poderão ser disponibilizadas na vistoria.

10.1.5. Serviço de migração de conteúdo e soluções para o novo ambiente, baseado em quantidade de terabytes (TB).

10.1.6. Elaboração de projeto e configuração de ambiente para proporcionar redundância e alta disponibilidade.

10.1.7. A redundância deve ser avaliada para a instalação e configuração de ambiente idêntico ao principal em outra localidade para replicação da solução.

CLÁUSULA DÉCIMA PRIMEIRA – DOS SERVIÇOS DE CUSTOMIZAÇÃO DE SEGURANÇA E PREVENÇÃO RANSONWARE

11.1. REQUISITOS PARA CUSTOMIZAÇÃO DE SEGURANÇA E PREVENÇÃO RANSONWARE

11.1.1. Configuração da solução de armazenamento definida por software com as características de eficiência e segurança, tais como compressão, desduplicação, criptografia de dados data-at-rest com gerenciador de chaves (KMS), autenticação de usuários com RBAC (*Role-based Access Control)*. Salientamos que é de responsabilidade da **CONTRATADA** o fornecimento e configuração do KMS em alta-disponibilidade

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá-MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS JRR

para cada cluster, compatível com a funcionalidade de criptografia de dados das soluções de armazenamento de dados ofertadas (definidas por software ou por hardware);

11.1.2. A solução deverá ser configurada de modo que o hipervisor e as soluções de armazenamento de dados tenham conformidade com as recomendações do Guia de Implementações Técnicas de Segurança (STIG) da Agência de Sistemas de Informação do Departamento de Defesa dos EUA (DISA). As configurações deverão ser minimamente capazes de proteger o carregador de inicialização (boot loader), pacotes, sistema de arquivos, controle de serviço e inicialização, propriedades de arquivos, autenticação, kernel e log.

11.1.3. Tanto para o hipervisor ofertado como para o sistema de armazenamento (definido por software ou por hardware), deverá ser configurado um modelo padrão com todas as configurações empregadas no cluster de modo que a solução possa corrigir automaticamente qualquer desvio da configuração de segurança do sistema operacional e do hipervisor para permanecer em conformidade. Se algum componente for considerado não compatível, o componente deverá ser restaurado às configurações de segurança suportadas sem nenhuma intervenção do administrador.

11.1.4. O fabricante também deverá configurar a solução conforme estabelecido no STIG de modo a limitar o número de sessões concorrentes para o máximo de dez contas e/ou tipos de contas habilitando modo de bloqueio.

11.1.5. Para soluções baseadas em tecnologia VMware, o técnico do fabricante deverá:

11.1.5.1. 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.

11.1.5.2. Os hosts ESXi devem proteger a confidencialidade e integridade das informações transmitidas, protegendo o tráfego de gerenciamento do ESXi.

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

11.1.5.4. O firewall dos hosts ESXi devem restringir o acesso aos serviços em execução no host.

11.1.5.5. O firewall dos hosts ESXi devem bloquear o tráfego de rede por padrão.

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS
JRR

11.1.6. Implementar todas as recomendações dos alertas publicados pelo CTIR Gov e garantia que não sejam utilizadas soluções de contorno durante o processo de implantação sendo necessário o emprego de soluções e correções legítimas do fabricante.

11.1.7. Empregar todos os patches e atualizações de segurança instalados.

11.1.8. O fabricante também deverá configurar regras de autenticação, tais como:

11.1.8.1. Proibir o login direto como usuário rootç

11.1.8.2. Bloquear contas do sistema que não sejam root;

11.1.8.3. Impor detalhes de manutenção de senha;

11.1.8.4. Configurar cautelosamente o acesso via SSH;

11.1.8.5. Ativar o bloqueio de tela.

11.1.9. Para implantação da solução de microssegmentação, a **CONTRATADA** deverá:

11.1.9.1. Apresentar a visão geral da arquitetura e revisão dos componentes envolvidos.

11.1.9.2. Revisar os recursos e funções da solução, incluindo microssegmentação, inserção de serviços de rede e automação de rede junto com casos de uso comuns.

11.1.9.3. Realizar sessão de aprofundamento técnico descrevendo as construções, tais como tipos de política, quarentena e categorias usando a instância de gerenciamento de **CONTRATANTE**.

11.1.9.4. Demonstrar em um ambiente de teste a criação de uma política de microssegmentação que restringe / permite o tráfego de rede entre duas máquinas virtuais.

11.1.9.5. Demonstrar em um ambiente de teste como uma a política de microssegmentação pode ser herdada por meio de marcação por uma máquina virtual recém-provisionada.

11.1.9.6. Demonstrar em um ambiente de teste como gerenciar e usar a quarentena de VM nos modos completo e forense.

11.1.10. Projetar e configurar políticas e categorias de segurança para um dos cenários abaixo:

DS JRR

11.1.10.1. Segmentação de uma aplicação em dois ou três níveis e controle do acesso entre os níveis com base nas conexões que devem ser permitidas, com até 5 VMs por camada.

11.1.10.2. Aplicar políticas de segurança para restringir/permitir o acesso entre camadas da aplicação.

11.1.10.3. Desenvolver políticas que isolam ambientes de desenvolvimento e produção para que não haja comunicação cruzada entre as cargas de trabalho de teste/desenvolvimento e de produção, aplicando políticas para pelo menos 10 VMs (dez máquinas virtuais) em cada ambiente.

11.1.10.4. Desenvolver política para quarentena forense manual e programática de VMs.

11.1.11. Transferência de conhecimento, incluindo revisão / sessão de coaching sobre a implantação.

11.1.12. Este serviço tem um escopo mínimo de dois dias e deverá incluir 10 (dez) participantes.

CLÁUSULA DÉCIMA SEGUNDA – DA SUBCONTRATAÇÃO

12.1. É expressamente vedada a subcontratação total ou parcial do objeto.

12.2. A comercialização de licenças e suporte técnico do fabricante não caracterizam subcontratação.

CLÁUSULA DÉCIMA TERCEIRA – DAS OBRIGAÇÕES DA CONTRATADA

13.1. São obrigações da **CONTRATADA**, além de outras previstas neste Contrato ou decorrentes da natureza do ajuste:

a) Cumprir fielmente as obrigações contratuais, de acordo com as especificações (cor, formato e tamanho) solicitadas, de forma que os serviços sejam realizados com esmero e perfeição;

b) Assumir, com exclusividade, todos os impostos e taxas que forem devidos em decorrência do objeto contratado, bem como, as contribuições devidas à Previdência

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03.929.049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br | FaceALMT | (65) 3313-6411

DS
JRR

Social, encargos trabalhistas e quaisquer outras despesas que se fizerem necessárias à perfeita execução do objeto deste Contrato, do Termo de Referência e seus Apêndices.

c) Abster-se de transferir direitos ou obrigações decorrentes do contrato sem a expressa concordância da **CONTRATANTE**.

d) Não subcontratar o objeto do presente Contrato, sem o consentimento prévio da **CONTRATANTE**, o qual, caso haja, será dado por escrito:

e) Credenciar junto à **CONTRATANTE** funcionário(s) que atenderá(ão) às solicitações dos serviços objeto deste Contrato;

f) Substituir, no prazo máximo de 10 (dez) dias a contar do recebimento da notificação formal, os objetos que durante o prazo de garantia, venham apresentar defeitos de fabricação ou quaisquer outros que venham a dificultar ou impossibilitar a sua utilização, desde que, para a sua ocorrência, não tenha contribuído, por ação ou omissão, a **CONTRATANTE**.

g) Responder, perante a **CONTRATANTE** e terceiros, por eventuais prejuízos e danos decorrentes de sua demora ou de sua omissão, na condução do objeto deste Instrumento sob a sua responsabilidade ou por erros relativos à execução do objeto deste Contrato;

h) Responsabilizar-se pelo bom comportamento de seus prepostos, podendo a **CONTRATANTE** solicitar a substituição de qualquer indivíduo, cuja permanência seja, a critério da **CONTRATANTE**, considerada inadequada na área de trabalho;

i) Zelar para que seus prepostos envolvidos na entrega dos materiais contratados se apresentem convenientemente trajados e devidamente identificados;

j) Responsabilizar-se pela estrita observância das normas de segurança interna e aquelas determinadas pelo Ministério do Trabalho;

k) Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados no desempenho dos serviços ou em conexão com eles, ainda que acontecido nas dependências da **CONTRATANTE**;

l) Entregar os objetos em perfeito estado de uso e funcionamento, de acordo com as especificações exigidas neste Contrato, no Termo de Referência e seus Apêndices;

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS
JRR

m) Promover por sua conta, através de seguros, a cobertura dos riscos a que se julgar exposta em vista das responsabilidades que lhe cabem na execução do objeto deste instrumento.

CLÁUSULA DÉCIMA QUARTA - DAS OBRIGAÇÕES DA CONTRATANTE

14.1. São obrigações da Assembleia Legislativa do Estado de Mato Grosso:

a) Gerenciar, fiscalizar, prestar, por meio de seu representante, as informações necessárias, bem como atestar as Notas Fiscais oriundas das obrigações contraídas;

b) Emitir pareceres sobre atos relativos à execução do objeto deste, em especial, quanto ao acompanhamento e fiscalização das entregas, à exigência de condições estabelecidas neste Contrato, no Termo de Referência e à proposta de aplicação de sanções;

c) Assegurar-se do fiel cumprimento das condições estabelecidas neste Contrato, no Termo de Referência, no instrumento convocatório e seus anexos;

d) Assegurar-se de que os preços contratados são os mais vantajosos para a Administração, por meio de estudo comparativo dos preços praticados pelo mercado;

e) Proporcionar todas as facilidades para que a **CONTRATADA** possa desempenhar seus serviços dentro das normas deste Contrato;

f) Comunicar a **CONTRATADA** as irregularidades observadas na execução dos serviços.

CLÁUSULA DÉCIMA QUINTA – DAS CONDIÇÕES DE SUSTENTABILIDADE

15.1. Todo documento deverá ser entregue pela **CONTRATADA**, quer seja pelo processo de cópia ou impresso, deverão ser feitos, preferencialmente, através de papel A4 ou papel ofício oriundos de processo de reciclagem, inclusive, os envelopes que forem entregues ao Pregoeiro, preferencialmente deverão ser todos em material reciclado.

DS
JRR

CLÁUSULA DÉCIMA SEXTA - DO PAGAMENTO

16.1. O pagamento será em até 10 (dez) dias da entrada da Nota Fiscal/Fatura na Secretaria de Planejamento, Orçamento e Finanças, de acordo com a Nota de Empenho e a Nota de Autorização de Despesa - NAD, após o atesto pela fiscalização do recebimento pela **CONTRATANTE**.

16.2. A **CONTRATADA** deverá indicar no corpo da Nota Fiscal/Fatura, descrição do produto (com detalhes), o número e o nome do Banco, Agência e número da conta corrente onde deverá ser feito o pagamento, via ordem bancária e apresentação dos comprovantes atualizados de regularidade abaixo, sob pena de aplicação das penalidades específicas previstas na Clausula Décima Nona:

a) Prova de regularidade fiscal para com a Fazenda Federal, Estadual e Municipal do domicílio ou sede da **CONTRATADA**, consistindo em certidões ou documento equivalente, emitidos pelos órgãos competentes e dentro dos prazos de validade expresso nas próprias certidões ou documentos;

b) Prova de regularidade fiscal para com a Procuradoria da Fazenda Nacional e para com a Procuradoria Geral do Estado, nos casos em que não sejam emitidas em conjunto às regularidades fiscais;

c) Prova de regularidade perante o Fundo de Garantia por Tempo de Serviço – FGTS (art. 27 da Lei 8.036/90), em plena validade, relativa à **CONTRATADA**;

d) Prova de regularidade perante o Instituto Nacional de Seguridade Social - INSS (art. 195, § 3° da Constituição Federal), em plena validade, relativa à **CONTRATADA**;

e) Certidão Negativa de Débitos Trabalhista – TRT.

16.3. A **CONTRATADA** deverá apresentar **NOTA FISCAL ELETRÔNICA** correspondente produtos efetivamente entregues, nos termos previstos em contrato.

16.4. As Notas Fiscais deverão ser emitidas em nome da Assembleia Legislativa do Estado de Mato Grosso – com o seguinte endereço: Edifício Gov. Dante Martins De Oliveira, Avenida André Antônio Maggi, S/N - CPA - Cuiabá/MT, CNPJ nº 03.929.049/0001-11, e deverão ser entregues no local indicado pela **CONTRATANTE**.

16.5. O pagamento efetuado à adjudicatária não a isentará de suas responsabilidades vinculadas ao fornecimento, especialmente aquelas relacionadas com a qualidade e validade, nem implicará aceitação definitiva do fornecimento;

DS
JRR

16.6. Deverá apresentar a Nota Fiscal de fornecimento/entrada dos produtos/serviços no ato da liquidação, procedimento de conferência.

16.7. Não haverá, sob hipótese alguma, pagamento antecipado;

16.8. Havendo vício a reparar em relação à nota fiscal/fatura apresentada ou em caso de descumprimento pela **CONTRATADA** de obrigação contratual, o prazo constante no item 16.1, poderá ser suspenso até que haja reparação do vício ou adimplemento da obrigação;

16.9. Caso constatado alguma irregularidade nas Notas Fiscais/Faturas, estas serão devolvidas pela Secretaria de Planejamento, Orçamento e Finanças ao fornecedor, para as necessárias correções, com as informações que motivaram sua rejeição, contando-se o prazo para pagamento da data da sua reapresentação;

16.10. Nenhum pagamento será efetuado à empresa adjudicatária enquanto pendente de liquidação qualquer obrigação. Esse fato não será gerador de direito a reajustamento de preços ou a atualização monetária;

16.11. A **CONTRATANTE** não efetuará pagamento de título descontado, ou por meio de cobrança em banco, bem como, os que forem negociados com terceiros por intermédio de operação de *factoring*;

16.12. O pagamento somente será efetuado mediante apresentação da regularidade documental.

16.13. As eventuais despesas bancárias decorrentes de transferência de valores para outras praças ou agências são de responsabilidade da **CONTRATADA**;

16.14. Quando da ocorrência de eventuais atrasos de pagamento provocados exclusivamente pela Administração, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes fórmulas:

$$I=(TX/100)$$
$$365$$
$$EM = I \times N \times VP, \text{ onde:}$$

I = Índice de atualização financeira;
TX = Percentual da taxa de juros de mora anual;
EM = Encargos moratórios;

DS
JRR

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela em atraso.

16.14.1. Na hipótese de pagamento de juros de mora e demais encargos por atraso, os autos devem ser instruídos com as justificativas e motivos e submetidos à apreciação da autoridade competente, que adotará as providências para eventual apuração de responsabilidade, identificação dos envolvidos e imputação de ônus a quem deu causa à mora.

16.15. Caso haja aplicação de multa, o valor será descontado de qualquer fatura ou crédito existente na Assembleia Legislativa em favor da **CONTRATADA**, se esse valor for superior ao crédito eventualmente existente, a diferença será cobrada administrativamente ou judicialmente, se necessário.

16.15.1. Caso a **CONTRATADA** não tenha nenhum valor a receber da **CONTRATANTE**, ser-lhe-á concedido o prazo de 15 (quinze) dias úteis, contados de sua intimação, para efetuar o pagamento.

16.15.2. Após esse prazo, não sendo efetuado o pagamento, seus dados serão encaminhados ao Órgão competente para que seja inscrita na dívida ativa do Estado, podendo, ainda a Administração proceder a cobrança judicial do valor devido.

16.16. O pagamento da fatura não será considerado como aceitação definitiva do objeto contratado e não isentará a **CONTRATADA** das responsabilidades contratuais quaisquer que sejam.

CLÁUSULA DÉCIMA SÉTIMA – DO REAJUSTE

17.1. Os preços são fixos e irreajustáveis no prazo de 12 (doze) meses contados da assinatura do contrato.

17.2. Dentro do prazo de vigência do contrato e mediante solicitação da **CONTRATADA**, os preços contratados poderão sofrer reajuste após o interregno de 12 (doze) meses contados da data de assinatura do contrato, aplicando-se o IPCA – Índice Nacional de Preços ao Consumidor Amplo, ou outro índice oficial que vier a substituí-lo, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência do prazo acima mencionado.

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

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS
JRR

17.4. No caso de atraso ou não divulgação do índice de reajustamento, o **CONTRATANTE**, pagará à **CONTRATADA** a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.

17.5. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

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

17.7. 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.

17.8. O reajuste será realizado por apostilamento.

17.9. O reajuste somente será concedido após análise pelo setor competente e mediante motivação e comprovação, por parte da **CONTRATADA**.

17.10. De forma a explanar acerca do índice escolhido, se faz necessário ressaltar que ante a ausência de normativa própria desta Assembleia Legislativa, que disponha sobre as contratações na área de tecnologia da informação, utilizamos para subsidiar as contratações de serviços e produtos a Instrução Normativa n.º 01/2019 do Governo Federal, que trata das contratações relacionadas a Tecnologia da Informação e que vincula os órgãos da administração pública federal.

17.11. A referida normativa dispõe sobre a necessidade de a utilização do ICTI – Índice de Custos da Tecnologia da Informação, para serviços relacionados a TI, ocorre que em pesquisas realizadas em órgãos públicos da administração federal, tais como TCU e STF (Contrato SEI/STF 0746706, SEI/STF 0489055 Contrato n.º 063/2017, Pregão Eletrônico TCU n.º 080/2019, Pregão Eletrônico n.º 23/2020), observamos que os referidos órgãos utilizam o IPCA – Índice Nacional de Preços ao Consumidor, pois é o que mais se aproxima do efetivo índice inflacionário.

DS
JRR

CLÁUSULA DÉCIMA OITAVA – DA RESCISÃO

18.1. O presente Contrato poderá ser rescindido pelos motivos previstos nos artigos 77 e 78 e nas formas estabelecidas no art. 79, acarretando as consequências do art. 80, todos da Lei nº 8.666/93, nas seguintes hipóteses:

18.1.1. A inexecução total ou parcial do contrato enseja a sua rescisão, com as consequências contratuais e as previstas em lei ou regulamento;

18.1.2. O não cumprimento de cláusulas contratuais, especificações, projetos ou prazos;

18.1.3. O cumprimento irregular de cláusulas contratuais, especificações, projetos e prazos;

18.1.4. A lentidão do seu cumprimento, levando a Administração a comprovar a impossibilidade da conclusão da obra, do serviço ou do fornecimento, nos prazos estipulados;

18.1.5. O atraso injustificado no início da obra, serviço ou fornecimento;

18.1.6. A paralisação da obra, do serviço ou do fornecimento, sem justa causa e prévia comunicação à Administração;

18.1.7. A subcontratação total do seu objeto, a associação da **CONTRATADA** com outrem, a cessão ou transferência, total ou parcial, bem como a fusão, cisão ou incorporação, não admitidas no edital e no contrato;

18.1.8. Desatendimento das determinações regulares da autoridade designada para acompanhar e fiscalizar a sua execução, assim como as de seus superiores;

18.1.9. O cometimento reiterado de faltas na sua execução, anotadas na forma do § 1º do art. 67 desta Lei;

18.1.10. A decretação de falência ou a instauração de insolvência civil;

18.1.11. A dissolução da sociedade ou o falecimento da **CONTRATADA**;

18.1.12. A alteração social ou a modificação da finalidade ou da estrutura da empresa, que prejudique a execução do contrato;

18.1.13. Razões de interesse público, de alta relevância e amplo conhecimento, justificadas e determinadas pela máxima autoridade da esfera administrativa a que está

DS
JRR

subordinado a **CONTRATANTE** e exaradas no processo administrativo a que se refere o contrato;

18.1.14. A supressão, por parte da Administração, de obras, serviços ou compras, acarretando modificação do valor inicial do contrato além do limite permitido no § 1º do art. 65 da Lei 8666/93;

18.1.15. A suspensão de sua execução, por ordem escrita da Administração, por prazo superior a 120 (cento e vinte) dias, salvo em caso de calamidade pública, grave perturbação da ordem interna ou guerra, ou ainda por repetidas suspensões que totalizem o mesmo prazo, independentemente do pagamento obrigatório de indenizações pelas sucessivas e contratualmente imprevistas desmobilizações e mobilizações e outras previstas, assegurado a **CONTRATADA**, nesses casos, o direito de optar pela suspensão do cumprimento das obrigações assumidas até que seja normalizada a situação;

18.1.16. O atraso superior a 90 (noventa) dias dos pagamentos devidos pela Administração decorrentes de obras, serviços ou fornecimento, ou parcelas destes, já recebidos ou executados, salvo em caso de calamidade pública, grave perturbação da ordem interna ou guerra, assegurado ao contratado o direito de optar pela suspensão do cumprimento de suas obrigações até que seja normalizada a situação;

18.1.17. A não liberação, por parte da Administração, de área, local ou objeto para execução de obra, serviço ou fornecimento, nos prazos contratuais, bem como das fontes de materiais naturais especificadas no projeto;

18.1.18. A ocorrência de caso fortuito ou de força maior, regularmente comprovada, impeditiva da execução do contrato;

18.1.19. Descumprimento do disposto no inciso V, do art. 27 da Lei nº 8.666/93, sem prejuízo das sanções penais cabíveis.

18.2. A rescisão, por algum dos motivos previstos na Lei nº 8.666/93 e suas alterações, não dará à **CONTRATADA** direito a indenização a qualquer título, independentemente de interpelação judicial ou extrajudicial;

18.3. A rescisão acarretará, independentemente de qualquer procedimento judicial ou extrajudicial por parte da **CONTRATANTE**, a retenção dos créditos decorrentes deste Contrato, limitada ao valor dos prejuízos causados, além das sanções previstas neste ajuste até a completa indenização dos danos;

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03.929.049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS JRR

18.4. Fica expressamente acordado que, em caso de rescisão, nenhuma remuneração será cabível, a não ser o ressarcimento de despesas autorizadas pela **CONTRATANTE** e, previstas no presente Contrato e comprovadamente realizadas pela **CONTRATADA.**

18.5. Os casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa.

CLÁUSULA DÉCIMA NONA – DAS SANÇÕES ADMINISTRATIVAS

19.1. Se a **CONTRATADA** descumprir quaisquer das condições deste instrumento ficará sujeita às penalidades previstas na Lei n. 10.520/2002, bem como nos art. 86 e 87 da Lei 8.666/93, quais sejam:

19.1.1. Por atraso injustificado na entrega do produto;

19.1.2. Atraso de até 10 (dez) dias, multa diária de 0,25% (vinte e cinco centésimos por cento), do valor adjudicado;

19.1.3. Atraso superior a 10 (dez) dias, multa diária de 0,50% (cinquenta centésimos por cento), do valor adjudicado, sobre o total dos dias em atraso, sem prejuízo das demais cominações legais;

19.2. No caso de atraso no recolhimento da multa aplicada, incidirá nova multa sobre o valor devido, equivalente a 0,20% (vinte centésimos por cento) até 10 (dez) dias de atraso e 0,40% (quarenta centésimos por cento) do valor adjudicado, acima desse prazo, calculado sobre o total dos dias em atraso.

19.3. Pela inexecução parcial ou total das condições estabelecidas neste ato convocatório, a Assembleia Legislativa do Estado de Mato Grosso poderá, garantida a prévia defesa, aplicar, também, as seguintes sanções:

19.3.1. Advertência,

19.3.2. Multa de até 20% (vinte por cento) sobre o valor homologado, atualizado, recolhida no prazo de 15 (quinze) dias corridos, contados da comunicação oficial, sem embargo de indenização dos prejuízos porventura causados a Assembleia Legislativa do Estado de Mato Grosso;

19.3.3. Suspensão temporária de participação em licitação e impedimento de licitar e contratar com a Administração Pública, bem como o cancelamento de seu certificado de

registro cadastral no cadastro de fornecedores do Estado de Mato Grosso por prazo não superior a 02 (dois) anos.

19.4. As multas serão descontadas dos créditos da empresa detentora da ata ou cobradas administrativa ou judicialmente.

19.5. As penalidades previstas neste item têm caráter de sanção administrativa, consequentemente, a sua aplicação não exime a empresa detentora da ata, da reparação das eventuais perdas e danos que seu ato venha acarretar a **CONTRATANTE**.

19.6. As penalidades são independentes e a aplicação de uma não exclui a das demais, quando cabíveis.

19.7. Nas hipóteses de apresentação de documentação inverossímil, cometimento de fraude ou comportamento de modo inidôneo, a licitante poderá sofrer, além dos procedimentos cabíveis de atribuição desta instituição e do previsto no art. 7.º da Lei 10.520/02, quaisquer das sanções adiante previstas, que poderão ser aplicadas cumulativamente:

19.7.1. Desclassificação ou inabilitação, caso o procedimento se encontre em fase de julgamento;

19.7.2. Cancelamento do contrato, se esta já estiver assinada, procedendo-se a paralisação do fornecimento;

19.8. As penalidades serão obrigatoriamente registradas no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Cadastro de Fornecedores do Estado de Mato Grosso, e no caso de ficar impedida de licitar e contratar, a licitante deverá ser descredenciada por igual período, sem prejuízo das multas previstas neste Contrato, no Termo de Referência, Edital e das demais cominações legais.

CLÁUSULA VIGÉSIMA – DO ACOMPANHAMENTO E FISCALIZAÇÃO

20.1. Para o acompanhamento e a fiscalização da execução do contrato será designada a Comissão de Recebimento de Bens e Serviços, formada por servidores nomeados pela Secretaria de Tecnologia da Informação da Assembleia Legislativa do Estado de Mato Grosso, nos termos do art. 67, Lei nº 8.666, de 1993, que se responsabilizará pelo registro de todas as ocorrências relacionadas com a execução e determinará o que for necessário à regularização de falhas ou defeitos observados;

DS
JRR

20.2. A fiscalização de que trata o item anterior não exclui nem reduz a responsabilidade da **CONTRATADA**, 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 em corresponsabilidade da Assembleia Legislativa do Estado de Mato Grosso ou de seus agentes, em conformidade com o art. 70 da Lei nº 8.666, de 1993;

20.2.1. A **CONTRATADA**

20.2.1.1. Deverá possuir o seguinte ator agindo para a execução contratual:

a) Preposto – Funcionário representante da **CONTRATADA**, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto a **CONTRATANTE**, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual.

20.2.1.2. A **CONTRATADA** deverá aceitar, antecipadamente, todos os métodos de inspeção, verificação e controle a serem adotados pela fiscalização, obrigando-se a fornecer-lhe todos os dados, elementos, explicações, esclarecimentos, soluções e comunicações de que esta necessitar e que forem julgados necessários ao cumprimento do objeto deste Contrato.

20.2.1.3. A existência e a atuação da fiscalização em nada restringem a responsabilidade única, integral e exclusiva da **CONTRATADA**, no que concerne ao objeto da respectiva contratação, às implicações próximas e remotas perante a **CONTRATANTE** o ou perante terceiros, do mesmo modo que a ocorrência de irregularidade decorrentes da execução contratual não implica em corresponsabilidade da **CONTRATANTE** ou de seus prepostos, devendo, ainda, a contratada, sem prejuízo das penalidades previstas, proceder ao ressarcimento imediato dos prejuízos apurados e imputados às falhas em suas atividades.

CLÁUSULA VIGÉSIMA PRIMEIRA – DA GARANTIA

21.1. A **CONTRATADA** deverá apresentar a garantia de execução contratual de 5% (cinco por cento), sobre o valor global da contratação, em uma das modalidades previstas no §1º do art. 56 da Lei nº 8.666/93, no momento da assinatura do contrato.

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03.929.049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

DS
JRR

CLÁUSULA VIGÉSIMA SEGUNDA – DA CLÁUSULA ANTICORRUPÇÃO

22.1. Para execução deste contrato, nenhuma das partes poderá oferecer, dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de que quer que seja, tanto por conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação vantagens financeiras ou benefícios de qualquer espécie, seja de forma direta ou indireta quanto ao objeto deste contrato, ou de outra forma a ele relacionada, o que deve ser observado, ainda, pelos prepostos e colaboradores.

CLÁUSULA VIGÉSIMA TERCEIRA – DA SUJEIÇÃO ÀS NORMAS LEGAIS E CONTRATUAIS

23.1. A legislação aplicável a este Contrato será a Lei Estadual nº. 10.534 de 13 de abril de 2017, e, subsidiariamente pela Lei Federal nº 8.666, de 21 de junho de 1993 e suas alterações posteriores, Lei nº. 8.078/1990 (Código de Defesa do Consumidor), demais legislações pertinentes e as condições e especificações estabelecidas no Processo Licitatório Pregão Eletrônico Registro de Preços nº 02/2022/ALMT e no Termo de Referência nº 022/2021/STI, bem como as cláusulas deste Instrumento.

CLÁUSULA VIGÉSIMA QUARTA – DAS DISPOSIÇÕES GERAIS

24.1. Integram este Contrato, o Termo de Referência nº 022/2021/STI e seus anexos, e a proposta comercial apresentada pela **CONTRATADA**.

24.2. Os casos omissos serão resolvidos conforme dispõem as Leis Federais nº 8.078/1990 (Código de Defesa do Consumidor), nº 10.534/2017 e nº 8.666/1993, Código Civil e demais legislações vigentes e pertinentes à matéria;

24.3. A abstenção, por parte da **CONTRATANTE**, de quaisquer direitos e/ou faculdades que lhe assistem em razão deste contrato e/ou lei não importará renúncia a estes, não gerando, pois, precedente invocável.

CLÁUSULA VIGÉSIMA QUINTA – DO FORO

25.1 - Fica eleito o foro da cidade de Cuiabá, Estado de Mato Grosso, como competente para dirimir quaisquer dúvidas ou questões decorrentes da execução deste Contrato.

DS
JRR

E, por se acharem justas e contratadas, as partes assinam o presente instrumento na presença das testemunhas abaixo, em 3 (três) vias de igual teor e forma, para que produza todos os efeitos legais.

Cuiabá – MT 11 de abril de 2022.

CONTRATANTE	**DEPUTADOS – MESA DIRETORA**
ASSEMBLÉIA LEGISLATIVA DO ESTADO DE MATO GROSSO **CNPJ nº 03.929.049/0001-11**	Eduardo Botelho: _____ **Presidente** Max Russi: _____ **1º Secretário**
CONTRATADA	**REPRESENTANTE LEGAL**
ADISTEC BRASIL INFORMÁTICA LTDA **CNPJ n° 15.457.043/0001-78**	José Roberto Inforzato Rodrigues RG nº 10.969.824 SSP/SP e CPF nº 04.767.238-25 ASSINATURA: DocuSigned by: José Roberto Rodrigues 3B068C6B177A47A...
TESTEMUNHA	**TESTEMUNHA**
NOME: _____ RG Nº: Luzia S. Ribeiro CPF Nº: CPF nº 124.952.498-92 ASSINATURA: G nº 23392713-X SSP/SP	NOME: Jenifer Cristina RG Nº: JENIFER CRISTINA DA SILVA CPF : CPF: 013.172.711-73 ASSINATURA: RG: 1735117-0 SSP/MT