## TERMO DE REFERÊNCIA - SERVIÇO

### 1. OBJETO:

**1.1.** Contratação de serviço de infraestrutura de TI baseada em arquitetura hiperconvergente, proteção de dados e proteção de rede, operação, sustentação, suporte técnico, instalação, configuração, licenciamento e equipamentos para a Prefeitura Municipal de Três Lagoas/MS.

(**X**) Natureza Comum
( ) Natureza Especial

| ITEM | CÓD. INTERNO | DESCRIÇÃO | UNIDADE DE MEDIDA | QUANTIDADE |
|---|---|---|---|---|
| 01 | 314.001.101 | Serviço de Infraestrutura de Data Center | MÊS | 12 |

**1.2.** O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto n.º 10.818, de 27 de setembro de 2021.

**1.3.** Os serviços objeto desta contratação são caracterizados como comuns, conforme elementos constantes no Estudo Técnico Preliminar.

### 1.4. VIGÊNCIA DO CONTRATO

**1.4.1.** A contratação será por **12 (doze) meses**, com possibilidade de prorrogações sucessivas, caracterizando-se como **serviço contínuo**, conforme previsto nos arts. 106 e 107 da Lei nº 14.133/2021, respeitada a vigência máxima decenal.

**1.4.1.1.** A prestação do serviço é enquadrada como **continuada** em razão da natureza do objeto, que envolve operação, sustentação, monitoramento, suporte técnico e segurança ininterrupta da infraestrutura de TI do Município.

**1.4.1.2.** Tais serviços são essenciais para garantir o funcionamento adequado dos sistemas municipais, assegurando a continuidade administrativa e a prestação eficiente dos serviços públicos à população.

**1.4.1.3.** A adoção de vigência plurianual revela-se **mais vantajosa** sob o ponto de vista técnico e econômico, em razão:

**1.4.1.3.1.** Da necessidade de continuidade operacional sem interrupções decorrentes de processos licitatórios anuais.

**1.4.1.3.2.** Da mitigação de riscos relacionados à descontinuidade de serviços críticos de TI, considerando a dependência tecnológica das atividades administrativas essenciais.

**1.4.1.3.3.** Da **economicidade**, considerando a redução de despesas administrativas com repetição de procedimentos licitatórios e a manutenção de condições comerciais equilibradas ao longo do período.

**1.4.1.4.** A vigência continuada contribui para maior estabilidade contratual, planejamento orçamentário e alinhamento às estratégias tecnológicas da Administração Pública.

## 1.5. DO LOCAL E CONDIÇÕES DE ENTREGA

**1.5.1.** Os serviços deverão ser entregues conforme condições estabelecidas no **item 5** deste instrumento.

## 1.6. DA GARANTIA

**1.6.1.** Todos os serviços entregues pela CONTRATADA deverão ser cobertos por garantia durante o período do contrato;

**1.6.2.** Deverá fornecer garantia permanente para todos os serviços entregues sendo responsável por monitorar e atuar imediatamente em qualquer situação que envolve garantias;

**1.6.3.** A CONTRATADA será responsável por todas as despesas associadas à substituição e manutenção das unidades, incluindo custos de envio, instalação e configuração;

**1.6.4.** Durante a vigência contratual, a CONTRATADA deverá manter canal de comunicação por telefone, e-mail ou sistema informatizado;

**1.6.5.** A não observância do prazo para correção de defeito implica execução das penalidades cabíveis estabelecidas em contrato e descritas neste termo;

**1.6.6.** As condições de garantia permanecerão em vigor durante todo o período de vigência do contrato e qualquer renovação subsequente.

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

**1.6.8.** O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade da Contratada.

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

### 1.7. ESCOPO GERAL DA SOLUÇÃO:

**1.7.1.** Fornecimento em regime de serviço de infraestrutura por prazo mínimo de 12 (doze) meses;

**1.7.2.** Utilização de tecnologias modernas, robustas, seguras e com ferramentas que alinham e agilizam a infraestrutura;

**1.7.3.** Tecnologia de resiliência a ataques cibernéticos, garantindo sempre a rápida detecção e resposta a incidentes para os dados vitais da Prefeitura de Três Lagoas/MS;

**1.7.4.** Implementação de segundo ambiente estrutural, para além de backups, serviço de alta disponibilidade ativo-ativo;

**1.7.5.** Atuação de profissionais certificados e capacitados, provendo ambiente estável com alta disponibilidade, seguro, padronizado e atualizado com todas as diretrizes que tratam de infraestrutura de Data Center.

## 2. FUNDAMENTAÇÃO DA CONTRATAÇÃO:

**2.1.** A Prefeitura de Três Lagoas/MS é integrante da Administração Pública e tem como um de seus objetivos acompanhar a modernização e as necessidades do uso de tecnologia existentes no mercado para melhor fiscalizar os gastos

públicos. Com isso, deve prover uma adequada infraestrutura de Tecnologia da Informação e Comunicação – TIC.

**2.2.** A presente contratação justifica-se pela crescente necessidade de otimizar as infraestruturas de tecnologia da informação e comunicação. O objetivo é garantir não apenas a continuidade dos serviços prestados, mas também promover uma evolução.

**2.3.** Aprimorar através da inovação tecnológica, como em inteligência artificial, machine learning, Big Data, flexibilidade, escalabilidade, cópia de dados de segurança, aproveitamento de dados, entre outros campos relevantes para a garantia dos trabalhos. O volume crescente de dados exige um plano de ação que promova sua qualificação, visando à circulação eficiente dessas informações e à sua integração, de forma a viabilizar serviços e soluções mais complexos, em um movimento consistente de desenvolvimento capaz de atender à crescente necessidade de processamento e armazenamento.

**2.4.** A implementação de soluções que integram o processamento e armazenamento de dados requer uma abordagem que leve em consideração questões cruciais de segurança, privacidade, integridade e ética.

**2.5.** Uma questão de extrema importância é a implementação da Lei Geral de Proteção de Dados (LGPD) 13.709/2018, que estabelece uma relação direta com o tema em questão. As exigências dessa lei impõem condições específicas para o armazenamento dos dados e estabelecem responsabilidades jurídicas claras. Para atender integralmente às disposições da LGPD, é imprescindível contar com um ambiente seguro e condições adequadas que garantam a conformidade com a legislação e assegurem a proteção dos dados em sua totalidade.

**2.6.** As soluções dos serviços são responsáveis por toda estrutura, sendo ela, equipamentos e mão de obra especializada, disponibilizando infraestrutura completa com todos os requisitos necessários para os diversos sistemas utilizados por esta Prefeitura, mantendo ambiente de Data Center, seguro, com alta disponibilidade e dando subsídios tecnológicos para tarefas desenvolvidas internamente e serviços prestados externamente.

**2.7.** A contratação em questão possui uma importância crucial para assegurar a continuidade dos serviços existentes, permitindo a incorporação contínua das evoluções tecnológicas.

**2.8.** A estimativa das quantidades/especificações técnicas foi baseada no levantamento pela Secretaria demandante, através dos elementos dispostos no Estudo Técnico Preliminar.

## 3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO:

**3.1.** Ambiente Técnico e Topologia Desejada.

**3.1.1.** A solução deve apresentar, obrigatoriamente, os seguintes requisitos técnicos:

**3.1.1.1. Escalabilidade:** A arquitetura tecnológica deve ser capaz de escalar de acordo com as demandas crescentes do sistema, seja em termos de tráfego, dados ou usuários.

**3.1.1.2. Disponibilidade:** Garantir que os serviços e sistemas estejam disponíveis 24x7 (vinte quatro horas por dia, 7 dias por semana), minimizando tempos de inatividade e interrupções.

**3.1.1.3. Desempenho:** Os sistemas devem ser capazes de lidar com cargas de trabalho esperadas e fornecer tempos de resposta aceitáveis.

**3.1.1.4. Segurança:** Proteger os dados, sistemas e comunicações contra acessos não autorizados, ataques cibernéticos e vazamentos de informações.

**3.1.1.5. Interoperabilidade:** Capacidade de integrar-se a outros sistemas, plataformas ou serviços de forma eficiente e sem problemas.

**3.1.1.6. Flexibilidade:** A arquitetura deve ser capaz de se adaptar a mudanças nos requisitos de negócios, tecnológicos e regulatórios.

**3.1.1.7. Manutenibilidade:** Facilidade de manter, atualizar e modificar os sistemas ao longo do tempo, garantindo sua longevidade e relevância.

**3.1.1.8. Padrões e Conformidade:** Seguir padrões de desenvolvimento, boas práticas e regulamentações relevantes para o setor.

**3.1.1.9. Custo-efetividade:** O uso de recursos deve ser otimizado para maximizar o retorno do investimento.

**3.1.1.10. Resiliência:** Capacidade de se recuperar de falhas de forma rápida e eficiente, garantindo a continuidade das operações.

**3.1.1.11. Monitoramento e Gerenciamento:** Implementar ferramentas e processos para monitorar o desempenho, detectar problemas e gerenciar recursos de forma eficaz.

**3.1.1.12. Escalabilidade horizontal e vertical:** Capacidade de aumentar a capacidade do sistema adicionando mais instâncias (escalabilidade horizontal) ou aumentando os recursos das instâncias existentes (escalabilidade vertical).

## 4. REQUISITOS DA CONTRATAÇÃO:

### 4.1. REQUISITOS DE NEGÓCIO:

**4.1.1.** A presente contratação orienta-se pelos seguintes requisitos de negócio, alinhados com a conclusão do Estudo Técnico Preliminar (ETP) para um modelo de Infraestrutura como Serviço (IaaS) adaptado à necessidade de controle e soberania de dados local:

**4.1.1.1.** A empresa responsável pelo serviço deverá atuar em ambiente *on-premises*, com toda infraestrutura alocada e operada nas dependências desta Prefeitura, garantindo a soberania e o controle físico dos dados e equipamentos.

**4.1.1.2.** A sala principal abrigará os equipamentos, fornecidos integralmente pela empresa vencedora do certame, incluindo racks e energia estável, que serão de propriedade da Contratada durante a vigência contratual e parte integrante do serviço.

**4.1.1.3.** O monitoramento deverá ser implementado de forma a acompanhar os serviços remotamente 24x7, prevendo qualquer intercorrência e auxiliando na rápida atuação para solução de problemas.

**4.1.2. Fazendo parte dos serviços:**

**4.1.2.1.** O suporte técnico para esclarecimento de dúvidas e resolução de problemas relacionados à configuração;

**4.1.2.2.** Atualizações, com entrega da infraestrutura que incorporem correções de erros ou de problemas registrados;

**4.1.2.3.** Manutenção corretiva, evolutiva e atualização tecnológica à eficiência, segurança e desempenho da Infraestrutura.

**4.1.3. Tipos de Manutenção:**

**4.1.3.1.** A manutenção do sistema deverá ser dividida em quatro especificações com tratamentos diferentes:

**4.1.3.1.1. Manutenção corretiva:** se refere ao diagnóstico e correção de erros;

**4.1.3.1.2. Manutenção preventiva:** quando da iniciativa desta Prefeitura de Três Lagoas, nos casos em que houver necessidade de modificar para melhorar a confiabilidade ou para oferecer uma base melhor para futuras ampliações;

**4.1.3.1.3. Manutenção legal:** configurações possíveis na infraestrutura para atender às mudanças na legislação e regras definidas pelo governo, órgãos reguladores e pela própria Prefeitura de Três Lagoas;

**4.1.3.1.4. Manutenção evolutiva:** adaptação do ambiente como todo às mudanças e ampliações gerais, estruturais ou não, para atender recomendações de novas atividades e necessidades dos usuários, que surjam com as constantes mutações ao longo do tempo ou em decorrência das necessidades da Prefeitura de Três Lagoas.

**4.1.4. Requisitos de Capacitação:**

**4.1.4.1.** A CONTRATADA será responsável pelos custos de elaboração, produção, impressão e fornecimento do material necessário;

**4.1.4.2.** As datas para a realização das atividades de treinamento e capacitação serão definidas previamente pela Contratante, respeitados os prazos de vigência do Contrato;

**4.1.4.3.** Abranger todo o conteúdo do treinamento da solução e as funcionalidades especificadas neste Estudo Técnico Preliminar, que capacite conhecimento suficiente para instalação, configuração e administração da solução contratada;

**4.1.4.4.** Poderá ser ministrado por empresa parceira ou terceirizada;

**4.1.4.5.** Ser ministrado individual ou em 01 (uma) turma de no máximo 05 (cinco) participantes;

**4.1.4.6.** Disponibilizar, para cada participante, material impresso ou em meio digital, atualizado e de primeiro uso, em idioma português ou inglês, bem como acesso a laboratório próprio da CONTRATADA ou sua representante para a realização das atividades práticas;

**4.1.4.7.** Caso o treinamento seja presencial, são requisitos do local do treinamento: instalações adequadas e disponibilizadas pela CONTRATADA;

**4.1.4.8.** A critério do CONTRATANTE, mediante apresentação detalhada de proposta da CONTRATADA, a capacitação poderá ser realizada presencialmente ou remotamente por videoconferência;

**4.1.4.9.** Caso o CONTRATANTE opte por capacitação remota ele deverá manter todas as características e qualidades ofertadas da modalidade presencial, tendo a carga horária compatível.

**4.1.5. Requisitos de Manutenção:**

**4.1.5.1.** Devido às características da solução, há necessidade de acompanhamento preciso realizando manutenções corretivas, preventivas e evolutiva pela Contratada, com objetivo de mantermos a infraestrutura atualizada, seguindo as boas práticas de segurança da informação, mantendo alta disponibilidade da solução e ao aperfeiçoamento de suas funcionalidades.

**4.1.6. Requisitos Temporais:**

**4.1.6.1.** O prazo para início da mobilização, para a execução dos serviços, deverá ocorrer e ser devidamente comprovada em até **5 (cinco) dias úteis** após o recebimento da Autorização de Fornecimento/Ordem de Serviço;

**4.1.6.2.** Mobilização refere-se ao processo de preparar e organizar todos os recursos necessários para iniciar as atividades referidas neste termo. Isso inclui a coordenação de equipes, a disponibilidade de equipamentos e materiais, a definição de cronogramas e a comunicação clara entre todas as partes envolvidas;

**4.1.6.3.** Garantindo assim que os recursos estejam prontos e que todos os envolvidos estejam cientes de suas responsabilidades e prazos;

**4.1.6.4.** A imprescindibilidade dos serviços levará à rescisão imediata caso o prazo não seja atendido, acarretando a convocação do segundo colocado no certame;

**4.1.6.5.** Toda a infraestrutura necessária para a prestação do serviço deverá ser instalada, configurada e estar disponível para utilização no prazo máximo de **30 (trinta) dias corridos**, contados a partir do recebimento da Autorização de Fornecimento/Ordem de Serviço.

**4.1.6.5.1.** Este prazo poderá ser reavaliado e ajustado em comum acordo entre as partes, mediante justificativa técnica, caso a complexidade da solução proposta ou a logística de fornecimento de equipamentos assim o exija, sem prejuízo da aplicação de penalidades por atrasos injustificados.

**4.1.7. Requisitos de Segurança e Privacidade:**

**4.1.7.1.** A solução deverá ser provida de requisitos de segurança, como criptografia, protocolos, atualizações contínuas, monitoramento 24x7, criação de fluxo de trabalho, implementação de boas práticas de segurança da informação, softwares oficiais e mão de obra especializada com certificações adequadas;

**4.1.7.2.** A contratada não poderá se utilizar da presente contratação para obter qualquer acesso não autorizado às informações da PREFEITURA DE TRÊS LAGOAS/MS;

**4.1.7.3.** A contratada não poderá veicular publicidade acerca do fornecimento a ser contratado, sem prévia autorização, por escrito, da PREFEITURA DE TRÊS LAGOAS/MS;

**4.1.7.4.** A contratada é responsável civil, penal e administrativa quanto à divulgação indevida ou não autorizada de informações, realizada por ela ou por seus empregados;

**4.1.7.5.** É de responsabilidade da contratada garantir que as informações por ela obtidas em decorrência da execução desta contratação sejam mantidas em sigilo, não podendo ser divulgadas, exceto se previamente acordado, por escrito, entre as partes contratantes;

**4.1.7.6.** É de responsabilidade da contratada garantir o tratamento de dados pessoais de acordo com a Lei Geral de Proteção de Dados

Pessoais (LGPD) com objetivo específico de assegurar a proteção, privacidade e transparência de dados de pessoas físicas;

**4.1.7.7.** O Termo de Confidencialidade deverá ser assinado pelo representante legal da Contratada e o Termo de Ciência pelos funcionários.

**4.1.8. Requisitos Sociais, Ambientais e Culturais:**

**4.1.8.1.** Durante a execução das atividades no ambiente da PREFEITURA DE TRÊS LAGOAS/MS, os funcionários da empresa fornecedora deverão observar, no trato com os servidores e o público em geral, a urbanidade e os bons costumes de comportamento, tais como: asseio, pontualidade, cooperação, respeito mútuo, discrição e zelo com o patrimônio público. Deverão ainda portar identificação pessoal, de acordo com as normas internas das instituições.

**4.1.9. Requisitos de Atestados e Certificados:**

**4.1.9.1.** Documentos que deverão ser apresentados, juntamente com a proposta (Fase classificatória):

**4.1.9.2.** Deverá apresentar comprovação para todos os itens e subitens, apontando a página e parágrafo da documentação o atendimento destes itens e subitens através de catálogos, folders e/ou outros comprovantes, desde que sejam do próprio fabricante do equipamento podendo ser certificação, catálogo técnico do fabricante ou declaração do fabricante;

**4.1.9.3.** Quando o licitante não for o próprio fabricante dos equipamentos ofertados, deverá apresentar declaração do fabricante específica para o edital, autorizando a empresa licitante a ofertar os equipamentos.

**4.1.10. Requisitos de Implantação:**

**4.1.10.1.** Compreende o serviço de implantação todos os serviços necessários à correta configuração da solução dentre eles:

**4.1.10.1.1. Ambiente de Implantação:** Definição clara dos requisitos, ferramentas necessárias para execução das tarefas, profissionais engajados e capacitados tecnicamente estando estes

certificados quanto aos equipamentos e softwares que compõe a solução.

**4.1.10.1.2. Infraestrutura de Hardware:** Especificações e configurações de hardware necessárias para executar o ambiente de forma eficiente, incluindo servidores, rede e armazenamento.

**4.1.10.1.3. Infraestrutura de Software:** Lista de software necessário como sistemas operacionais, servidores de aplicativos, bancos de dados e outras dependências.

**4.1.10.1.4. Configuração do Ambiente:** Procedimentos para configurar e preparar os ambientes de implantação, incluindo instalação de software, configuração de rede e segurança.

**4.1.10.1.5. Implantação Automatizada:** Implementação de processos automatizados para implementar de maneira consistente e confiável em diferentes ambientes, usando ferramentas como scripts de implantação ou ferramentas de automação.

**4.1.10.1.6. Monitoramento e Gerenciamento:** Implementação de ferramentas e processos para monitorar toda infraestrutura, coletar métricas de desempenho e gerenciar recursos de forma eficaz.

**4.1.10.1.7. Backup e Recuperação:** Estratégias e procedimentos para realizar backups regulares, seguindo política de backup, esta imposta pela contratante e garantir a recuperação rápida em caso de falha ou perda de dados.

**4.1.10.1.8. Testes de Implantação:** Realização de testes completos de implantação no ambiente, abrangendo site primário e secundário, para garantir que todos os requisitos necessários sejam implantados corretamente e que todas as funcionalidades estejam operacionais.

**4.1.10.1.9. Treinamento e Documentação:** Apresentar a documentação completa, compondo desde o projeto inicial, quanto especificidades de todos os equipamentos e sistemas que formam a solução. Treinamento presencial aos responsáveis pela área, contemplando especificações técnicas.

**4.1.10.1.10. Gestão de Configuração:** Implementação de um sistema de gestão de configuração para controlar e gerenciar mudanças na configuração do ambiente ao longo do tempo.

**4.1.10.1.11. Sede:** Manter sede, filial ou escritório na cidade de Três Lagoas/MS, onde serão prestados os serviços com capacidade operacional para receber e solucionar qualquer demanda da Administração, bem como realizar todos os procedimentos pertinentes à seleção, treinamento, admissão e demissão dos empregados. A exigência de sede local é necessária para garantir agilidade e eficiência na resolução de problemas, facilidade de comunicação e coordenação da solução a ser prestada.

**4.1.10.2.** A CONTRATADA deverá comprovar, no prazo de 60 (sessenta) dias a contar do início da prestação dos serviços, o cumprimento do item SEDE.

**4.1.11. Requisitos de Garantia e Manutenção:**

**4.1.11.1.** Requisitos de Experiência Profissional:

**4.1.11.1.1.** A empresa vencedora do certame deverá apresentar, juntamente com as documentações obrigatórias, atestados técnicos que comprovem experiência mínima de 36 meses, referente ao objeto deste termo, conforme parágrafo 5º do art. 67 da Lei 14.133/2021;

**4.1.11.1.2.** A apresentação de atestados técnicos que comprovem experiência mínima de 36 meses é essencial para assegurar que a empresa vencedora do certame tenha a capacidade técnica necessária para executar o contrato de forma eficiente e satisfatória;

**4.1.11.1.3.** Esta exigência visa proteger os interesses da administração pública, garantindo a qualidade e a continuidade dos serviços contratados, visto a complexidade do objeto aqui exposto, sendo este serviço essencial para as atividades da Prefeitura;

**4.1.11.1.4.** Todos os serviços deverão ser prestados por profissionais devidamente capacitados na solução técnica em questão, bem

como com todos os recursos ferramentais necessários para a prestação dos serviços.

**4.1.11.1.5.** O corpo técnico envolvido no contrato deve demonstrar experiência em funções similares ou relacionadas à posição em questão, evidenciando habilidades e conhecimentos relevantes. Essas qualificações devem ser formalmente comprovadas, sob pena de rescisão contratual.

**4.1.11.1.6.** A empresa contratada deve possuir um corpo técnico qualificado e certificado, com nível mínimo de escolaridade de ensino superior completo. Além disso, é necessário apresentar certificações oficiais tanto da solução oferecida em software quanto em hardware.

**4.1.11.1.7.** Todos os profissionais envolvidos na execução dos serviços devem possuir vínculo empregatício comprovado por meio da Carteira de Trabalho e Previdência Social (CTPS). Essa documentação deve ser apresentada inicialmente e continuamente nos relatórios mensais.

**4.1.11.1.8.** Qualquer equipamento, software ou tecnologia aplicada ao ambiente durante a vigência do contrato deve ser operado por profissionais habilitados, sem possibilidade de subcontratação. O descumprimento desta cláusula resultará em sanções contratuais.

**4.1.11.1.9.** Todas as provas documentais apresentadas, incluindo declarações, certificados ou atestados, são de total responsabilidade da contratada. Qualquer divergência identificada acarretará a perda do contrato.

**4.1.12. Requisitos de Segurança da Informação e Privacidade**

**4.1.12.1.** Garantir que apenas colaboradores da CONTRATADA autorizados tenham acesso aos dados relevantes, mediante a utilização de autenticação multifatorial, políticas de acesso baseadas em função e revisões regulares de privilégios de acesso.

**4.1.12.2.** Manter os hardwares, softwares e sistemas operacionais fornecidos atualizados com as últimas correções de segurança para mitigar vulnerabilidades conhecidas e garantir a integridade do ambiente.

**4.1.13. Requisitos de Vistoria Técnica**

**4.1.13.1.** Os interessados em participar desta licitação devem obrigatoriamente realizar uma vistoria no local de entrega e instalação dos equipamentos, bem como no local onde os serviços serão executados.

**4.1.13.2.** O Representante legal da licitante ou seu responsável técnico designado para este fim, deverá apresentar:

**4.1.13.3.** No caso de diretor, sócio ou proprietário da empresa licitante que comparecer ao local, deverá comprovar a representatividade por meio da apresentação de ato constitutivo, estatuto ou contrato social, do documento de eleição de seus administradores, devidamente registrados na Junta Comercial ou no cartório de pessoas jurídicas.

**4.1.13.4.** Tratando-se de procurador deverá apresentar instrumento público ou particular de procuração, com firma reconhecida em cartório, com poderes expressos, acompanhado do correspondente documento, dentre os indicados no subitem acima, que comprove os poderes do mandante para a outorga.

**4.1.13.5.** O Representante legal da licitante ou seu responsável técnico, deverá realizar visita técnica, onde será emitido atestado declarando que a empresa tomou conhecimento das particularidades inerentes a prestação dos serviços e recebeu todas as informações necessárias para o cumprimento integral das obrigações objeto da licitação, não cabendo qualquer discordância futura, seja de ordem física ou técnica.

**4.1.13.6.** A empresa que não realizar a vistoria deverá apresentar, no momento da habilitação, declaração de que possui conhecimento pleno das condições e peculiaridades da contratação, responsabilizando-se por quaisquer ônus.

**4.1.13.7.** Agendar previamente as visitas no endereço abaixo, onde receberão o Atestado de Visita:

**4.1.13.7.1.** Órgão: PREFEITURA DE TRÊS LAGOAS/MS;

**4.1.13.7.2.** Setor: Diretoria de Tecnologia da Informação;

**4.1.13.7.3.** Fone: (67) 99122-7453;

**4.1.13.7.4.** Localidade: Prefeitura de Três Lagoas, Estado de Mato Grosso do Sul;

**4.1.13.7.5.** Endereço: Rua Dr. Oscar Guimarães, 541 – Centro – CEP: 79600-020 – Três Lagoas/MS.

**4.1.13.7.6.** OBS.: O local indicado para a visita deverá ser vistoriado até o 1º (primeiro) dia útil que antecede a data de abertura dos envelopes, para atendimento de Segunda a Sexta-feira, das 07:00 às 11:00 horas.

**4.1.13.8.** Subcontratação

**4.1.13.8.1.** É expressamente vedada qualquer que seja a subcontratação do objeto contratual.

**4.1.14. Requisitos de Confidencialidade das Informações**

**4.1.14.1.** A CONTRATADA deverá manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do contrato, respeitando todos os critérios estabelecidos aplicáveis aos dados, informações, regras de negócios, documentos, entre outros.

**4.1.14.2.** A CONTRATADA deverá manter sigilo absoluto sobre quaisquer dados, informações, códigos-fonte ou artefatos contidos em quaisquer documentos e em quaisquer mídias, incluindo meios de armazenamento e o que lhe for transferido por meio de canal de conectividade, de que venha a ter conhecimento durante a execução dos trabalhos de levantamento de requisitos, construção, implantação e execução dos serviços, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela CONTRATANTE a tais documentos.

**4.1.14.3.** Toda informação confidencial gerada e/ou manipulada em razão desta contratação, seja ela armazenada em meio físico, magnético ou eletrônico, deverá ser devolvida nas seguintes hipóteses, mediante formalização entre as partes:

**4.1.14.3.1.** Término ou rompimento do Contrato; ou

**4.1.14.3.2.** Solicitação da Prefeitura.

**4.1.15. Requisito de Garantia da Proposta**

**4.1.15.1.** Em concordância com o art. 58 da Lei n. 14.133/2021, será exigida a garantia da proposta de 1% em razão da complexidade e urgência desta contratação. Este instrumento legal visa proteger os interesses públicos envolvidos, uma vez que mitiga os riscos do retardamento ou fracasso do certame, ocasionado, geralmente, por empresas que se quer possuem capacidade técnica e financeira para participar de licitações deste nível, servindo como eficiente sinalização de condição prévia de aptidão.

**4.1.16.** Requisito da Garantia da Execução

**4.1.16.1.** Com base na complexidade técnica envolvida, estamos adotando um percentual de 10% como garantia, conforme estabelecido no artigo 98 da Lei 14.133/2021. Esta medida visa mitigar os riscos associados à execução da licitação, assegurando que o proponente tenha capacidade financeira e técnica para lidar com desafios técnicos complexos que possam surgir durante a implementação do contrato. Essa garantia não apenas protege os interesses da administração pública, garantindo a conclusão bem-sucedida da prestação dos serviços dentro dos parâmetros estabelecidos, mas também promove um ambiente competitivo mais robusto, incentivando propostas que reflitam um planejamento sólido e uma execução eficiente.

**4.1.17.** Papéis e Responsabilidades

**4.1.17.1.** São obrigações da CONTRATANTE:

**4.1.17.2.** Nomear Gestor e Fiscais Técnico e Administrativo do contrato para acompanhar e fiscalizar a execução dos contratos;

**4.1.17.3.** Encaminhar formalmente a demanda por meio de Ordem de Serviço com os critérios estabelecidos no Termo de Referência;

**4.1.17.4.** Receber a solução fornecida pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

**4.1.17.5.** Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, quando aplicável;

**4.1.17.6.** Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

**4.1.17.7.** Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução;

**4.1.17.8.** Exigir o afastamento e/ou substituição imediata de empregado que não mereça confiança no trato com os serviços prestados, que adote posturas inadequadas ou incompatíveis com o exercício das atribuições que lhe foram designadas;

**4.1.17.9.** Impedir que terceiros, que não seja a empresa CONTRATADA, efetuem os serviços prestados;

**4.1.17.10.** Rejeitar os serviços executados em desacordo com as obrigações assumidas pela empresa CONTRATADA, exigindo sua correção, no prazo máximo de 10(dez) dias, sob pena de suspensão do contrato, ressalvados os casos fortuitos ou de força maior desde que devidamente justificados e aceitos pela CONTRATANTE;

**4.1.17.11.** Prestar informações e esclarecimentos necessários e proporcionar condições – no que lhe couber – para que a contratada possa executar os serviços objeto do contrato;

**4.1.17.12.** Comunicar à contratada, com antecedência mínima de 30 dias, as eventuais alterações que realizar na solução e nas suas normas, padrões, processos e procedimentos;

**4.1.17.13.** Cumprir e fazer cumprir o disposto nas cláusulas do contrato, devendo aplicar as penalidades previstas em lei pelo não-cumprimento das obrigações contratuais ou execução insatisfatória dos serviços;

**4.1.17.14.** Solicitar à CONTRATADA todas as providências necessárias ao bom andamento dos serviços;

**4.1.17.15.** Zelar para que, durante a vigência do Contrato, sejam mantidas todas as obrigações assumidas pela CONTRATADA, inclusive quanto às condições de habilitação e qualificação exigidas na licitação;

**4.1.17.16.** Não praticar atos de ingerência na administração da empresa CONTRATADA, tais como:

**4.1.17.17.** exercer o poder de mando sobre os empregados desta, devendo reportar-se somente aos prepostos por ela indicados;

**4.1.17.18.** promover ou aceitar o desvio de funções dos empregados, utilizando-os em atividades distintas daquelas previstas no contrato e na função específica para a qual foram contratados;

**4.1.17.19.** considerar os trabalhadores da CONTRATADA como colaboradores permanentes e/ou pertencentes a estrutura da PREFEITURA DE TRÊS LAGOAS/MS; e

**4.1.17.20.** exercer qualquer relação com a CONTRATADA que caracterize pessoalidade e subordinação direta.

**4.1.17.21.** São obrigações do CONTRATADO

**4.1.17.22.** Indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato conforme requisitos temporais do item 4.5;

**4.1.17.23.** Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

**4.1.17.24.** Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;

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

**4.1.17.26.** Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

**4.1.17.27.** Manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução conforme item 4.13;

**4.1.17.28.** Manter sigilo sobre quaisquer informações do CONTRATANTE às quais, durante a vigência do contrato, venha a ter conhecimento ou acesso, devendo entregar a CONTRATANTE o Termo de

Confidencialidade, assinado por seu representante legal, e pelos profissionais designados para a prestação de serviços;

**4.1.17.29.** Assegurar a transferência à CONTRATANTE, de conhecimentos adquiridos ou produzidos pelos seus profissionais, relativamente a serviços em andamento, nos termos que venham a ser por estes definidos, a fim de garantir a continuidade dos serviços;

**4.1.17.30.** Garantir a execução dos serviços sem interrupção, substituindo, caso necessário, sem ônus para a CONTRATANTE, qualquer profissional que estiver em gozo de férias, auxílio-doença, auxílio maternidade ou qualquer outro benefício legal / regulamentar, por outro de mesma qualificação ou superior;

**4.1.17.31.** Arcar com todos os encargos sociais, trabalhistas, fiscais, comerciais e ambientais previstos na legislação vigente;

**4.1.17.32.** Prestar os esclarecimentos necessários ao CONTRATANTE, bem como informações concernentes à natureza e andamento dos serviços executados, ou em execução;

**4.1.17.33.** Garantir a integridade e disponibilidade dos documentos e informações que, em função do Contrato, estiverem sob a sua guarda, sob pena de responder por eventuais perdas e/ou danos;

**4.1.17.34.** Tratar todas as informações a que tenha acesso, em caráter de estrita confidencialidade, não podendo, sob qualquer pretexto, divulgar, revelar, reproduzir, ou deles dar conhecimento a terceiros estranhos a esta contratação, bem como utilizá-las para fins diferentes dos previstos na presente contratação;

**4.1.17.35.** Toda informação confidencial disponível em razão desta contratação, seja ela armazenada em meios físico, magnético ou eletrônico, deverá ser devolvida nas hipóteses de extinção ou rescisão do Contrato ou quando solicitado pela CONTRATANTE;

**4.1.17.36.** Manter o CONTRATANTE oficialmente informado sobre quaisquer necessidades de atualização ou mudança na configuração dos serviços prestados;

**4.1.17.37.** Em caso de conduta inadequada ou falta de habilidade técnica por parte de qualquer profissional designado, o CONTRATANTE reserva-

se o direito de exigir a substituição imediata. Referências objetivas de falta de habilidade técnica devem ser fornecidas para fundamentar essa decisão.

**4.1.17.38.** Prestar os serviços dentro dos parâmetros e rotinas estabelecidos neste Termo de Referência;

**4.1.17.39.** Responsabilizar-se pelos danos causados diretamente à Administração, equipamentos, ou a terceiros, decorrentes de sua culpa ou dolo na execução dos serviços, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo CONTRATANTE;

**4.1.17.40.** Manter endereço atualizado da sede da empresa ou escritório comercial e endereço eletrônico (e-mail), junto ao Fiscal do Contrato, durante a vigência da prestação do serviço, bem como indicar por escrito o nome e telefones do responsável para contato de forma a facilitar a comunicação da CONTRATANTE com a CONTRATADA.

## 5. MODELOS DE EXECUÇÃO DO OBJETO:

### 5.1. PRAZO E LOCAL DE EXECUÇÃO:

**5.1.1.** O prazo para término da implantação de todos os equipamentos e início da execução dos serviços previstos neste Termo de Referência será de até **30 (trinta) dias corridos**, contados **a partir do recebimento da Autorização de Fornecimento/Ordem de Serviço**, emitida pela Administração.

**5.1.1.1.** Caso não seja possível a entrega na data assinalada, a Contratada deverá comunicar formalmente as razões respectivas com antecedência mínima de **05 (cinco) dias úteis**, para que eventual pleito de **prorrogação de prazo** seja analisado pela Administração, ressalvadas as hipóteses de caso fortuito ou força maior, devidamente comprovadas.

**5.1.2.** A implantação, instalação e início efetivo das atividades deverão ocorrer no(s) local(is) designado(s) pela Administração, observando-se as condições técnicas necessárias para execução adequada do objeto.

**5.1.3.** Caso a Contratada identifique, previamente ao início dos serviços, alguma necessidade adicional para a instalação ou adequação do ambiente, deverá comunicar formalmente à Administração antes do início dos trabalhos, para avaliação e deliberação.

**5.1.1.** O local da execução dos serviços será:

**5.1.1.1.** **Site Primário:** Rua João Carrato, nº 33 – Centro – Três Lagoas/MS;

**5.1.1.2.** **Site Secundário:** Avenida Antônio Trajano, nº 30 – Centro – Três Lagoas/MS.

**5.1.2.** O objeto desse termo deve ser prestado 24x7x365 dias, durante todo prazo em que o contrato esteja vigente.

**5.2. ESPECIFICAÇÕES TÉCNICAS DOS EQUIPAMENTOS:**

**5.2.1.** *Appliances Hiperconvergentes* - 06 unidades, sendo no mínimo 04 (QUATRO) do tipo I e 02 (DOIS) do tipo II

**5.2.1.1.** A solução *hiperconvergente* deverá prover infraestruturas integradas de alta disponibilidade, entregues em configuração de *clusteres*, compostos de nós de computação e armazenamento físicos (*appliances*), voltados a execução de ambiente de virtualização;

**5.2.1.2.** A quantidade de *appliances* da solução deverá ser de no mínimo 06 (seis) nós;

**5.2.1.3.** O cluster da solução deverá ser fornecido com todos os componentes, incluindo *appliances*, licenças e subscrições, módulos, acessórios, conectores, cabos e adaptadores, bem como qualquer outro elemento de hardware ou software adicionais, de forma a atender plenamente os seguintes requisitos:

**5.2.1.3.1.** Capacidade de processamento, memória RAM e conectividade de rede;

**5.2.1.3.2.** Sistema de armazenamento definido por software (SDS);

**5.2.1.3.3.** Funcionalidades de *hypervisor* para virtualização de computação;

**5.2.1.3.4.** Funcionalidades de gerenciamento da solução;

**5.2.1.3.5.** Funcionalidades de replicação de dados;

**5.2.1.3.6.** Switches TOR (topo de rack) para conexão dos componentes da solução;

**5.2.1.3.7.** Serão aceitas apenas soluções de *appliances* de *hiperconvergência* do tipo "*turnkey*", ou seja, com recursos de computação, armazenamento e rede totalmente integrados fim a fim, com gerenciamento de operações e sistema de gerenciamento unificado desenvolvido pelo fabricante, testado, pré-configurado, e desenvolvido em conjunto com o fabricante da solução de Software *Defined Storage*, comprovado através de documentação oficial do fabricante da solução de Software *Defined Storage* e aderente às seguintes definições:

**5.2.1.4.** Como referência, segue a definição de appliance do SNIA (https://www.snia.org/education/online-dictionary/term/appliance):

**5.2.1.4.1.** "*An intelligent device programmed to perform a single well-defined function, such as providing file, web, network or print services. Appliances differ from general purpose computers in that their software is normally customized for the function they perform, pre-loaded by the vendor, and not alterable by the user.*"

**5.2.1.4.2.** Em tradução livre: "Um dispositivo inteligente programado para realizar uma única função bem definida, como fornecer arquivos, web, rede ou serviços de impressão.

**5.2.1.4.3.** Os "appliances" diferem dos computadores de uso geral na medida em que seu software é normalmente personalizado para a função que desempenham, pré-carregado pelo fornecedor, e não alterável pelo usuário;

**5.2.1.5.** Não serão aceitas como *appliances* de HCI as soluções baseadas em servidores certificados ou VSAN *Ready* Nodes, listados no VMware *vSAN Compatibility Guide* https://compatibilityguide.broadcom.com/search?program=server&persona=live&column=partnerName&order=asc

**5.2.1.6.** A solução de *hiperconvergência* integrada ("turnkey") deverá ter ferramenta unificada para instalação mais rápida, simplificada e que

garanta uma configuração idêntica de todos os nós aplicando as melhores práticas;

**5.2.1.7.** Deve ter ferramenta unificada de monitoração e atualização de todo hardware e software da solução, que gerencie no mínimo os seguintes itens: atualização da BIOS dos nós, atualização de firmware dos drives e da controladora de discos, atualização dos drivers das placas de rede, atualização do *vSphere*, do armazenamento definido por software (software *defined storage*-SDS) e atualização do próprio software de governança. Todas as atualizações devem estar homologadas pelo fabricante da solução. Esta ferramenta deve ser gráfica, com suporte a apresentação de visões do hardware físico dos nós, suporte a troca de drives, com controle do inventário, com ferramenta de diagnóstico e com módulo para a adição de novos nós.

**5.2.1.8.** A solução deve empregar recursos de alta disponibilidade para garantir a continuidade dos serviços, mesmo em caso de falha parcial dos equipamentos, e deve prever recursos de recuperação contra desastres em caso de falha;

**5.2.1.9.** A solução deve implementar escalabilidade horizontal (*scale*-out), ou seja, permitir aumentar a capacidade de armazenamento, processamento e memória do ambiente virtual de forma linear, através da adição de novos nós (appliances) ao cluster, além de crescer de forma linear o desempenho do ambiente, sem a parada do ambiente de produção;

**5.2.1.10.** A solução deverá implementar a migração de máquinas virtuais entre *appliances* de um mesmo cluster, independentemente da quantidade de *appliances*, sem que isto gere qualquer problema de performance às aplicações (*vMotion*);

**5.2.1.11.** A solução deve possuir ferramenta unificada (interface única) para upgrades de todos os componentes de hardware e software, o que inclui BIOS, firmwares, drivers, *vSphere*, armazenamento definido por *sotware* (SDS) e da ferramenta de gerenciamento da solução de HCI;

**5.2.1.12.** Deve permitir a atualização de todos os componentes da solução (BIOS, *firmware*, *softwares* de gerenciamento e *softwares VMware*),

através de um único pacote de instalação integrado, disponibilizado pelo fabricante;

**5.2.1.13.** Caso a solução não possua a funcionalidade de atualização de todos os componentes através de um único pacote de instalação integrado, a CONTRATADA deverá realizar, durante todo o período de vigência e sem custos para a CONTRATANTE, serviços que contemplem a atualização de cada componente da solução, sempre que uma versão importante (*major release*) for disponibilizada ou sempre que o cliente demandar, limitado a seis acionamentos por ano.

## 5.3. CARACTERÍSTICAS GERAIS DOS SERVIDORES FÍSICOS (APPLIANCES) DA SOLUÇÃO

**5.3.1.** A marca e o modelo do appliance ofertado deverá estar certificado para o sistema operacional *VMware vSphere ESXi* na versão 7 ou superior na família do processador sendo ofertado. Esse item deverá ser comprovado através da matriz de compatibilidade da VMware no link https://compatibilityguide.broadcom.com/search?program=server&persona=live&column=partnerName&order=asc , ou através de documentos técnicos como *Release* Notes e *Specsheets* públicos, demonstrando compatibilidade e suporte oficial do fabricante do *appliance* com o *hypervisor* proposto;

**5.3.2.** Serão aceitos os certificados para os servidores que são base do *appliance* HCI;

**5.3.3.** A solução deverá ser pré integrada logicamente, com seus componentes interligados sem ponto único de falha e de acordo com as melhores práticas do fabricante permitindo o acesso ao portal de configuração da solução como um todo imediatamente após a energização e conexão física e lógica do sistema;

**5.3.4.** Os *appliances* fornecidos deverão atender, integralmente, à especificação funcional da solução hiperconvergente acima e acompanhar todos os componentes de hardware, software e licenças necessários para a devida operabilidade deles.

## 5.4. GABINETE E FONTES

**5.4.1.** Os *appliances* deverão possuir chassi em formato rack padrão 19" polegadas, com altura máxima de 2U por nó;

**5.4.2.** Os *appliances* deverão possuir kit de trilhos deslizante e braço organizador de cabos, ambos do mesmo fabricante dos equipamentos, para fixação dos equipamentos em rack 19 polegadas padrão EIA-310D;

**5.4.3.** Possuir baias de drives frontal hot-*pluggable*, com pelo menos 24 unidades do total de discos dispostos na baia frontal disponíveis para armazenamento de discos de dados e cache;

**5.4.4.** Possuir *display* frontal ou LEDs, embutido no gabinete, para monitoramento das condições de funcionamento dos principais componentes do servidor por meio de exibição de alertas de falha;

**5.4.5.** Cada nó que compõe a solução deverá possuir fontes de alimentação elétrica (PSU) hot-*pluggable* com redundância mínima 1+1, com potência suficiente para suportar a configuração ofertada, não sendo aceitos equipamentos com transformadores ou adaptadores;

**5.4.6.** As fontes devem possuir tensão de entrada de 100~240 VAC automaticamente ou operar em 220 VAC;

**5.4.7.** As fontes devem possuir eficiência energética padrão *Platinum*;

**5.4.8.** Cada fonte deve acompanhar 1 (um) cabo de energia elétrica padrão IEC C13/C14 de no mínimo 1.5 metro, e amperagem compatível com a potência da fonte;

**5.4.9.** Os *appliances* devem possuir ventilação adequada para a refrigeração de seu sistema interno dentro dos limites de temperatura adequados para operação. Os ventiladores devem ser redundantes, ou seja, o sistema poderá continuar em operação normalmente no caso de falha de parte dos ventiladores, e os defeituosos deverão poder ser substituídos sem a parada do equipamento;

**5.4.10.** Os componentes internos ao gabinete dos *appliances* deverão ser integrados, homologados e testados pelo fabricante do *appliance* ou pelo fabricante da solução hiperconvergente como um todo, garantindo a compatibilidade e o desempenho otimizado.;

**5.4.11.** Não serão aceitas componentes/placas de livre comercialização no mercado, soluções baseadas em *vSAN Ready* Nodes ou configurações montadas exclusivamente para atendimento destas especificações;

**5.4.12.** A falha isolada de um componente da solução não pode impactar a disponibilidade da infraestrutura de armazenamento para as máquinas virtuais;

**5.4.13.** Deverá possuir no mínimo 1 (uma) porta de vídeo VGA padrão DB-15;

**5.4.14.** Deverá possuir no mínimo 2 portas USB externas sendo uma dedicada para gerência do *hardware*;

**5.4.15.** Com a finalidade de automatizar os processos de implementação, manutenção e gerenciamento do *CLUSTER* e permitir a integração com aplicações externas, a solução hiperconvergente deverá oferecer API (*Application Program Interface*) para REST (*Representation State Transfer*);

**5.4.16.** A solução de hiperconvergência deve incorporar segurança em conformidade com padrões governamentais e internacionais de segurança, NIST SP800, FIPS 140-2, CNSA, *Common Criteria* EAL2+, além de permitir o emprego de configurações baseadas no *Security Technical Implementation Guide* (STIG);

**5.4.17.** É de responsabilidade da CONTRATADA fornecer atualização de todos os componentes (firmware, drivers, softwares de virtualização de armazenamento, gerenciamento, e demais softwares que fazem parte da solução).

### 5.5. VOLUMETRIA LIQUIDA

**5.5.1.** A solução, após instalado e configurado, deverá fornecer pelo menos 170 (cento e setenta) TiB em discos SSD para capacidade em área útil total para armazenamento do ambiente virtual considerando a perda de 1 (um) nó por completo por site e um site inteiro, sendo 03 (três) nós em cada site, sem que haja perda de dados, sem considerar qualquer ganho com desduplicação ou compressão, em sua configuração inicial.

### 5.6. CARACTERÍSTICAS TÉCNICAS DA SOLUÇÃO DE INFRAESTRUTURA COMPUTACIONAL (HIPERCONVERGENTE)

**5.6.1.** *APPLIANCE* – tipo I (04 unidades)

**5.6.1.1.** Cada nó hiperconvergente deverá possuir 2 (dois) processadores simétricos, cada um com, no mínimo, 24 (vinte e quatro) núcleos físicos;

**5.6.1.2.** O processador deve possuir frequência de *clock* base de, no mínimo, 3.0GHz;

**5.6.1.3.** O processador deve possuir memória cache L3 de, no mínimo, 30MB;

**5.6.1.4.** Memória *Ram* De Cada Nó;

**5.6.1.5.** Cada nó deve possuir 1 TB (um *terabyte*) de Memória RAM;

**5.6.1.6.** Drives De Cada Nó;

**5.6.1.7.** Deverão ser fornecidos drives, conforme a recomendação do fabricante do software de armazenamento proposto, desenvolvido exclusivamente para servidores;

**5.6.1.8.** O fator mínimo do número de falhas toleráveis será de 1 (um) – *Failures to Tolerate* (FTT)=1, *Replication* Factor (RF=2) ou equivalente. Isto é, a solução, deverá suportar, pelo menos, a perda de um nó por completo, sem que haja perda ou indisponibilidade de dados em cada site;

**5.6.1.9.** Em todo e qualquer caso, será obrigação da CONTRATADA durante o período de contrato, substituir os discos, tempestivamente, sem qualquer ônus, em caso de falhas, mesmo que a falha se deva ao uso do disco ter excedido a carga de trabalho nominal (DWDP) do disco.

**5.6.1.10.** Drives Para O Sistema Operacional

**5.6.1.10.1.** Cada nó deve possuir 2 (dois) drives padrão SSD de no mínimo 240GB em RAID 1 para o sistema operacional. Podem ser utilizados SD Card, *microSD*, SSD, m.2, BOSS, SSD SAS ou SSD SATA;

**5.6.1.10.2.** Os drives do sistema operacional não podem compartilhar a mesma controladora de disco do armazenamento e do cache/Tier 0;

**5.6.1.11.** Armazenamento;

**5.6.1.11.1.** Cada nó deve possuir pelo menos 24 (vinte e quatro) slots para discos SSD (*Solid State Disks*);

**5.6.1.11.2.** Cada nó deve possuir pelo menos 3 (três) discos SSD de 800GB SAS brutos dedicados para cache;

**5.6.1.11.3.** Caso a solução não possua discos SSDs dedicados para cache deverá prover adicionalmente 800GB de memória RAM brutos por *appliance*;

**5.6.1.11.4.** Possuir, no mínimo, 15 (quinze) discos SSD (*Solid State Disk*) SATA *Read Intensive* com capacidade bruta de 3.84TB cada, totalizando 57TB por nó;

**5.6.1.11.5.** Entende-se por área útil total aquela disponível após descontar overhead de proteção de dados e formatação. Deve-se considerar base 10 (1 *Terabyte* igual a 1000 *Gigabytes*) para referência de cálculo;

**5.6.1.12.** Conectividade De Cada Nó

**5.6.1.12.1.** Cada nó deverá ser fornecido com, no mínimo, 4 (quatro) interfaces 25Gbps, podendo as interfaces estarem distribuídas em uma ou mais placas;

**5.6.1.12.2.** Deverão as interfaces de rede de 25Gbps dos *appliances* possuir suporte às seguintes tecnologias:

**5.6.1.12.3.** MSI-X;

**5.6.1.12.4.** SR-IOV;

**5.6.1.12.5.** VLAN;

**5.6.1.12.6.** NIC *Teaming*;

**5.6.1.12.7.** *Link Aggregation*;

**5.6.1.12.8.** *Multi Queueing* (*VMware NETQueue* ou similar);

**5.6.1.12.9.** UDP *checksum offload*;

**5.6.1.12.10.** *Large Send Offload* (LSO);

**5.6.1.12.11.** *Large Receive Offload*;

**5.6.1.12.12.** *Receive Side Scaling* (RSS);

**5.6.1.12.13.** Virtual *Network Fabrics* (NVGRE & VXLAN);

**5.6.1.12.14.** Suportar jumbo *frame*, IPv4 e IPv6 TCP.

**5.6.1.13.** Possuir no mínimo 1 (uma) porta 1Gbps RJ45 para ser utilizada como interface de gerenciamento *out-of-band*.

**5.6.2.** APPLIANCES – TIPO II (02 UNIDADES)

**5.6.2.1.** Cada nó hiperconvergente deverá possuir 2 (dois) processadores simétricos, cada um com, no mínimo, 28 (vinte e oito) núcleos físicos;

**5.6.2.2.** O processador deve possuir frequência de *clock* base de, no mínimo, 2GHz;

**5.6.2.3.** O processador deve possuir memória cache L3 de, no mínimo, 30MB;

**5.6.2.4.** Memória *Ram* De Cada Nó

**5.6.2.5.** Cada nó deve possuir 1TB (um *terabyte*) de Memória RAM;

**5.6.2.6.** Drives De Cada Nó;

**5.6.2.7.** Deverão ser fornecidos drives, conforme a recomendação do fabricante do software de armazenamento proposto, desenvolvido exclusivamente para servidores;

**5.6.2.8.** O fator mínimo do número de falhas toleráveis será de 1 (um) – *Failures to Tolerate* (FTT)=1, *Replication* Factor (RF=2) ou equivalente. Isto é, a solução, deverá suportar, pelo menos, a perda de um nó por completo, sem que haja perda ou indisponibilidade de dados em cada site;

**5.6.2.9.** Em todo e qualquer caso, será obrigação da CONTRATADA durante o período de contrato, substituir os discos, tempestivamente, sem qualquer ônus, em caso de falhas, mesmo que a falha se deva ao uso do disco ter excedido a carga de trabalho nominal (DWDP) do disco.

**5.6.2.10.** Drives Para O Sistema Operacional

**5.6.2.10.1.** Cada nó deve possuir 2 (dois) drives padrão SSD de no mínimo 480GB em RAID 1 para o sistema operacional. Podem ser utilizados SD *Card*, microSD, SSD, m.2, BOSS, SSD SAS ou SSD SATA;

**5.6.2.10.2.** Os drives do sistema operacional não podem compartilhar a mesma controladora de disco do armazenamento e do cache/*Tier* 0;

**5.6.2.10.3.** Armazenamento

**5.6.2.10.4.** Cada nó deve possuir pelo menos 24 (vinte e quatro) slots para discos SSD (*Solid State Disks*);

**5.6.2.10.5.** Cada nó deve possuir pelo menos 2 (dois) discos SSD de 800GB SAS brutos dedicados para cache;

**5.6.2.10.6.** Caso a solução não possua discos SSDs dedicados para cache deverá prover adicionalmente 800GB de memória RAM brutos por appliance;

**5.6.2.10.7.** Possuir, no mínimo, 8 (oito) discos SSD (*Solid State Disk*) SATA *Read Intensive* com capacidade bruta de 3.84TB cada, totalizando 30TB por nó;

**5.6.2.10.8.** Entende-se por área útil total aquela disponível após descontar overhead de proteção de dados e formatação. Deve-se considerar base 10 (1 *Terabyte* igual a 1000 *Gigabytes*) para referência de cálculo;

**5.6.2.11.** Conectividade De Cada Nó

**5.6.2.11.1.** Cada nó deverá ser fornecido com, no mínimo, 4 (quatro) interfaces 25Gbps, podendo as interfaces estarem distribuídas em uma ou mais placas;

**5.6.2.11.2.** Deverão as interfaces de rede de 25Gbps dos *appliances* possuir suporte às seguintes tecnologias:

**5.6.2.11.3.** MSI-X;

**5.6.2.11.4.** SR-IOV;

**5.6.2.11.5.** VLAN;

**5.6.2.11.6.** NIC *Teaming*;

**5.6.2.11.7.** Link *Aggregation*;

**5.6.2.11.8.** *Multi Queueing* (*VMware NETQueue* ou similar);

**5.6.2.11.9.** UDP *checksum offload*;

**5.6.2.11.10.** *Large Send Offload* (LSO);

**5.6.2.11.11.** *Large Receive Offload*;

**5.6.2.11.12.** *Receive Side Scaling* (RSS);

**5.6.2.11.13.** Virtual *Network Fabrics* (NVGRE & VXLAN);

**5.6.2.11.14.** Suportar jumbo frame, IPv4 e IPv6 TCP.

**5.6.2.12.** Possuir no mínimo 1 (uma) porta 1Gbps RJ45 para ser utilizada como interface de gerenciamento *out-of-band*.

**5.7. SOFTWARE DE VIRTUALIZAÇÃO:**

**5.7.1.** Cada nó da solução hiperconvergente, composto por servidores físicos (appliances), deverá estar totalmente licenciado para toda a capacidade computacional do cluster;

**5.7.2.** Deverá suportar a escalabilidade de nós com configurações de processamento, memória e discos diferentes da fornecida inicialmente no mesmo cluster, ou seja, suportando configurações heterogêneas no cluster;

**5.7.3.** Caso não seja possível, cada appliance deverá ser fornecido com 20% a mais de processamento, memória e armazenamento;

**5.7.4.** O conjunto de *softwares* (*stack*) de cada *CLUSTER* da solução hiperconvergente deverá ser composto de, pelo menos, softwares de virtualização (computação, redes e armazenamento) e gerenciamento conforme relação a seguir:

**5.7.5.** Licenças do software de virtualização *VMWARE VSPHERE*, versão *ENTERPRISE PLUS* 8, com suporte 24x7, na versão "*PRODUCTION*" ou equivalente;

**5.7.6.** Licença do software de gerenciamento *VMWARE VCENTER SERVER*, versão *STANDARD*, com suporte 24x7 na versão "*PRODUCTION*" ou equivalente;

**5.7.7.** Licenças dos softwares de virtualização de armazenamento (SDS), compatível com as soluções do fabricante *VMWARE*, com suporte 24x7 na versão "*PRODUCTION*" ou equivalente;

**5.7.8.** Todos os softwares da solução deverão ser fornecidos na modalidade *OPEN* ou OEM (*Original Equipment Manufacturer*);

**5.7.9.** Os *softwares* de virtualização (computação, redes e armazenamento) e gerenciamento que compõe a solução deverão ser licenciados, com direito a atualizações e upgrades durante o período de vigência do contrato, e com todos os recursos necessários para o pleno funcionamento da solução com todos os itens especificados neste Termo de Referência;

**5.7.10.** É de responsabilidade da CONTRATADA fornecer atualização de todos os componentes (*firmware*, *softwares* de virtualização - computação, redes e armazenamento - gerenciamento, automação e orquestração, e demais *softwares* que fazem parte da solução), em forma de pacote com instalação assistida.

## 5.8. CARACTERÍSTICAS DO SISTEMA DE ARMAZENAMENTO DEFINIDO POR SOFTWARE – SDS

**5.8.1.** A solução deve possuir SISTEMA DE ARMAZENAMENTO DEFINIDO POR *SOFTWARE* - SDS, composto dos drives locais, controladoras virtuais e interfaces de I/O de cada nó que compõe o *CLUSTER*, apresentado como um único sistema de armazenamento (STORAGE) ao ambiente virtual;

**5.8.2.** O sistema de armazenamento definido por software da solução deverá possuir mecanismos de monitoramento proativo dos dados armazenados quanto à consistência e integridade, capaz de recuperar ou isolar dados corrompidos;

**5.8.3.** Cada nó deve possuir seu subsistema de armazenamento local definido por software, composto de unidades SSD (*solid-state drive*), interfaces de I/O e controladora física ou virtual, que agregados em CLUSTER formam um único sistema de armazenamento distribuído e definido por software;

**5.8.4.** Deverá possuir funcionalidades de dês duplicação e compressão de dados *inline* ou *near-line*, isto é, durante a gravação dos dados para a camada persistência;

**5.8.5.** A solução de SDS deverá ser totalmente integrada com o *VMware vSphere* sem necessidade de controladora adicional. Caso a solução de SDS necessite de um controlador virtual específico para controlar o armazenamento, deverá ser fornecido 20% a mais de recursos de memória e processamento por nó para esta finalidade.

**5.8.6.** Deverá suportar funcionalidade de criptografia do armazenamento por *software* ou ser entregue com discos SED (*Self-Encrypting Drives*);

**5.8.7.** O sistema de armazenamento definido por software da solução deverá ser capaz de garantir o melhor desempenho de acesso aos dados mesmo com possíveis movimentações de VMs entre diferentes tipos de *appliances* computacionais;

**5.8.8.** A solução deverá suportar sistema de arquivos nativo, com suporte ao protocolo NFS;

**5.8.9.** Deverá ser permitida a troca de discos avariados, sem interrupção das operações de I/O das aplicações que estão acessando os dados;

**5.8.10.** Deverá suportar as funções nativas do VMware *vSphere* como: *vMotion*, *High Availability*, e *Dynamic Resource Scheduler*;

**5.8.11.** Deverá suportar as ferramentas nativas de proteção de dados, tais como: *Snapshots* e *Linked Clone*;

**5.8.12.** Garantir que os dados e réplicas nunca sejam provisionados no mesmo nó, a fim de garantir que em caso de falha de nó, os dados continuem acessíveis;

**5.8.13.** Permitir upgrades de *software* e *firmware* não disruptivos, ou seja, que não necessitem de parada nas máquinas virtuais ou aplicações;

**5.8.14.** Permitir o upgrade de nós de forma transparente e não disruptiva, ou seja, ao inserir o nó no *cluster*, o *Software Defined Storage* deverá integrar o appliance ao cluster, aumentando imediatamente os recursos de processamento, memória e armazenamento;

**5.8.15.** A falha isolada de um componente do sistema de armazenamento definido por *software* da solução não pode impactar a disponibilidade da infraestrutura de armazenamento para as máquinas virtuais;

**5.8.16.** Permitir a replicação de máquinas virtuais mesmo estas estando em equipamentos de diferentes fabricantes utilizando o mesmo *hypervisor*;

**5.8.17.** Caso a solução não suporte tal possibilidade, será aceito o fornecimento de software de replicação adicional, com todos os recursos adicionais (processamento, armazenamento e conectividade) para a sua instalação e funcionamento, em unidades equivalentes aos requisitos dos *appliances* especificados no edital.

## 5.9. REQUISITOS DE GERENCIAMENTO DA SOLUÇÃO

**5.9.1.** Deverá se integrar ao *VMware vCenter* para criação de uma console única de gerenciamento, ou seja, deverá ser capaz de realizar as tarefas de gerenciamento através da console do *VMware vCenter*;

**5.9.2.** A ferramenta de gerenciamento deve detectar automaticamente a inclusão de novos *appliances* no *CLUSTER*;

**5.9.3.** Deverá fornecer um conjunto de hardware e software de gerência, do mesmo fabricante do servidor, compatível com o padrão IPMI 2.0 que possibilite o gerenciamento remoto através de controladora de gerenciamento integrada, com porta RJ-45 dedicada, não sendo essa

nenhuma das interfaces de controladora de rede, e software de gerenciamento, que ofereça as seguintes funções para a solução ofertada;

**5.9.4.** Permitir associação de políticas de armazenamento em tempo real para cada VM ou conjunto de VMs, que reflitam a necessidade atual da aplicação ou serviço sem necessidade de parada para manutenção ou ajustes físicos nos nós do cluster;

**5.9.5.** Trabalhar com console remota que ofereça controle pleno do servidor, isto é, com funcionalidades de uma console local independente do funcionamento do sistema operacional;

**5.9.6.** Ligar e desligar servidor remotamente;

**5.9.7.** Receber alertas de pré-falhas e defeitos de discos e memórias;

**5.9.8.** Emitir alertas sempre que os principais componentes (processador, memória, disco) atinjam valores preestabelecidos;

**5.9.9.** Possibilidade de emissão de inventário de hardware;

**5.9.10.** Deve possuir interface ethernet dedicada, suportando alocação fixa de endereço IP e que suporte nativamente a atribuição de endereçamento IP dinâmico;

**5.9.11.** Permitir detecção e recuperação automática do servidor quando houver falhas;

**5.9.12.** Permitir redirecionamento de mídia (mídia virtual);

**5.9.13.** Controle dos servidores via KVM *Virtual* (Teclado, Vídeo e Mouse) dispensando o uso de *switches* KVM;

**5.9.14.** Permitir acesso a BIOS remotamente;

**5.9.15.** Suportar os protocolos de criptografia SSL para acesso *Web* e SSH para acesso CLI;

**5.9.16.** Integração com o AD (*Microsoft Active Directory*);

**5.9.17.** Permitir acesso através de navegador web (sem necessidade de cliente específico);

**5.9.18.** Operar independentemente da CPU do servidor e do sistema operacional, mesmo se a CPU ou o sistema operacional estiverem travados ou inacessíveis de alguma forma;

**5.9.19.** Permitir a criação de grupos de usuários;

**5.9.20.** Suportar controle de firmware instalados nas máquinas, após download da versão atualizada do site do fabricante deve identificar o(s) nó(des) que não estejam com as suas versões mais recentes e orquestrar as atualizações;

**5.9.21.** Deve o *software* de gerência ser do mesmo fabricante do servidor de rede;

**5.9.22.** Deve ser capaz de monitorar e controlar o consumo de energia do servidor;

**5.9.23.** Possuir gestão automática de chamados ao suporte;

**5.9.24.** Realizar abertura automática de chamados proativamente "*Call Home*" com o fabricante;

**5.9.25.** Deverá possuir integração com *VMware vCenter*;

**5.9.26.** Emitir alertas de anormalidade de hardware através do *software* de gerência e suportar o encaminhamento via e-mail e *trap* SNMP;

**5.9.27.** A solução de gerenciamento do hardware dos servidores deve suportar o gerenciamento através de aplicação de gerenciamento via dispositivos moveis (*smartphones* e *tablets*) compatível com sistemas IOS e *Android*. O APP deverá estar disponível para *download* na *Google Play Store* e *Apple APP Store*;

**5.9.28.** Suporte a capacidade de gerenciamento remoto de um único equipamento (1:1) e vários equipamentos (1:N) da mesma marca;

**5.9.29.** Deverá suportar QoS (*Quality of Service*) na camada de armazenamento a fim de limitar a quantidade de I/Os que uma determinada máquina virtual, ou conjunto de máquinas virtuais podem executar na infraestrutura.

## 5.10. BIOS E SEGURANÇA

**5.10.1.** BIOS ou EUFI desenvolvida pelo mesmo fabricante do equipamento não sendo aceitas soluções em regime de OEM ou customizadas;

**5.10.2.** A BIOS ou EUFI deve possuir o número de série do equipamento e campo editável que permita inserir identificação customizada podendo ser consultada por software de gerenciamento, como número de propriedade e de serviço;

**5.10.3.** Deve possuir funcionalidade de recuperação de estado da BIOS/UEFI a uma versão anterior gravada em área de memória exclusiva e destinada a

este fim, de modo a garantir recuperação em caso de eventuais falhas em atualizações ou incidentes de segurança;

**5.10.4.** As atualizações de BIOS/UEFI devem possuir (assinatura) autenticação criptográfica segundo as especificações NIST SP800-147B ou NIST SP800131A ou FIPS 140-2.

## 5.11. FUNCIONALIDADES DE REPLICAÇÃO DE DADOS E DISASTER RECOVERY DA SOLUÇÃO

**5.11.1.** A solução deverá possuir módulo capaz de realizar a replicação de máquinas virtuais VMWARE localmente e remotamente para outro *CLUSTER*, realizando clones e *snapshots* com proteção contínua dos dados por máquina virtual;

**5.11.2.** O *software* de replicação deverá estar licenciado para no mínimo cinco máquinas virtuais por nó;

**5.11.3.** A funcionalidade de replicação remota deve permitir replicar os dados das máquinas virtuais entre *appliances* da solução de hiperconvergência entre localidades distintas;

**5.11.4.** A solução deverá ser capaz de realizar a proteção local em nível de VM ou bloco entre os *appliances* para garantir o RPO próximo ou igual a zero para as aplicações críticas utilizadas pela CONTRATANTE;

**5.11.5.** Deverá permitir a replicação de máquinas virtuais VMWARE utilizando recursos de otimização de tráfego através de dês duplicação e compressão dos dados para *clusteres* instalados em outra localidade, através de rede IP;

**5.11.6.** Permitir a replicação das máquinas virtuais em modo assíncrono.

**5.11.7.** Permitir que a replicação seja executada por máquina virtual (VM) de maneira individual, selecionando uma ou mais VMs;

**5.11.8.** Deve permitir a orquestração e execução de rotinas configuráveis (*scripts*) de pré e pós processo durante o *failover* das máquinas virtuais;

**5.11.9.** Deve suportar replicar máquinas virtuais que façam uso de discos VMDK;

**5.11.10.** Deverá permitir testes não disruptivos de desastre utilizando a imagem da VM de replica sem impacto e indisponibilidade no ambiente produtivo.

## 5.12. FUNCIONALIDADE DE ANALYTICS EM CLOUD

**5.12.1.** A solução deverá possuir ferramenta de análise preditiva para auxiliar os administradores a tomarem decisões de como otimizar o desempenho e melhorar a disponibilidade dos sistemas através de técnicas de "*machine learning*" aplicadas aos dados disponíveis no portal, que pode ser baseado em nuvem.

## 5.13. QUALIFICAÇÃO DO FABRICANTE

**5.13.1.** O fabricante deve ser registrado na "*Membership List*" do *Unified Extensible Firmware Interface* Fórum, acessível pelo website www.uefi.org/members , em categoria que ateste a conformidade de seus equipamentos com a especificação UEFI 2.x ou superior, ou apresentar certificação equivalente que comprove a conformidade com padrões de firmware modernos e seguros.

## 5.14. LICENCIAMENTO DE SISTEMAS OPERACIONAIS:

**5.14.1.** Possuir licença do sistema operacional *Microsoft Windows Server* 2022 Data Center (ou versão superior/equivalente que atenda aos requisitos funcionais) com número ilimitado de máquinas virtuais contemplando todos os nós de processamento e armazenamento dos *clusteres* hiperconvergente;

**5.14.1.1.** Deverá incluir CALs de Acesso para serviços Microsoft alocados neste ambiente contemplando todos os usuários da PREFEITURA DE TRÊS LAGOAS/MS durante a vigência do contrato;

**5.14.1.2.** Possuir licença do sistema operacional *Red Hat Enterprise Linux* ou *Suse Enterprise Linux* (ou distribuição Linux de nível empresarial equivalente que atenda aos requisitos funcionais) em sua última versão com número ilimitado de máquinas virtuais contemplando todos os nós de processamento e armazenamento do *clusteres* hiperconvergentes.

## 5.15. SWITCHES PARA SOLUÇÃO HIPERCONVERGENTE 24 PORTAS SFP28 25GB E 4 PORTAS 100G L3 COM FONTE REDUNDANTE (06 UNIDADES)

**5.15.1.** O equipamento deve possuir no mínimo 24 (vinte quatro) portas 10/25 *Gigabit Ethernet* SFP28;

**5.15.1.1.** Deve ocupar no máximo 1 (uma) unidade de *rack* (1 RU);

**5.15.1.2.** Deve ser instalável em *rack* padrão de 19", sendo que deverão ser fornecidos os respectivos kit's de fixação;

**5.15.1.3.** As portas SFP28 devem suportar *transceivers* dos padrões SFP+ 10GBase-SR, 10GBase-LR, 10GBase-ER, SFP 1000Base-SX, 1000Base-LX e 1000Base-T e cabos *Direct Attach Cable* (DAC);

**5.15.1.4.** Possuir 04 (quatro) portas 100 *Gigabit Ethernet* QSFP28 com suporte a velocidades de 40 e 100 *Gigabit Ethernet*.

**5.15.1.5.** Deve suportar *transceivers* padrões 40GBase-SR4, 40GBase-LR4;

**5.15.1.6.** Deve suportar *transceivers* padrão 100GBase-SR4 e 100GBase-LR4

**5.15.1.7.** Deve possuir matriz de comutação com capacidade de pelo menos 1.08 Tbps;

**5.15.1.8.** Deve possuir capacidade mínima de encaminhamento de pacotes de 720 Mpps;

**5.15.1.9.** Deve possuir *buffer* mínimo de 32 MB;

**5.15.1.10.** Deve possuir latência menor ou igual a 1µs (microsegundo);

**5.15.1.11.** Deve possuir capacidade para no mínimo 98.000 endereços MAC;

**5.15.1.12.** Deve suportar a Jumbo *frames* de no mínimo 9000 *bytes*;

**5.15.1.13.** Deve possuir no mínimo 1 (uma) porta de console com conector RJ-45;

**5.15.1.14.** Deve possuir no mínimo 1 (uma) porta *Ethernet* RJ-45 para administração fora de banda (*out-of-band management*);

**5.15.1.15.** Deve ser fornecido com configuração de CPU e memória (RAM e Flash) suficiente para implementação de todas as funcionalidades descritas nesta especificação.

**5.15.1.16.** Deve possuir fontes de alimentação redundantes internas ao equipamento com ajuste automático de tensão 110 ou 220 volts;

**5.15.1.17.** O equipamento deverá ter ventiladores redundantes com opção de fluxo de ar frente para trás ou trás para frente (*front-to-back* ou *back-to-front*). Os equipamentos devem vir equipados preferencialmente, com ventiladores de fluxo de ar frente para trás;

**5.15.1.18.** As fontes e ventiladores devem ser capazes de serem trocados com o equipamento em pleno funcionamento, sem nenhum impacto na performance (*hot-swappable*) e devem ser redundantes;

**5.15.1.19.** O equipamento deve ser específico para o ambiente de Data Center com comutação de pacotes de alto desempenho;

**5.15.1.20.** Deve ser um equipamento homologado pela Agência Nacional de Telecomunicações (Anatel);

**5.15.1.21.** Deve possuir LEDs, por porta, que indiquem a integridade e atividade do *link*;

**5.15.1.22.** A solução deve implementar e prover arquitetura de rede de Data Center utilizando a arquitetura "*spine - leaf*", tendo o VxLAN como plano de dados ("*data-plane*") e BGP EVPN para o plano de controle ("*control-plane*").

**5.15.2.** Deve possuir porta de console para gerenciamento e configuração via linha de comando. O conector deve ser RJ-45 ou padrão RS-232 (os cabos e eventuais adaptadores necessários para acesso à porta de console devem ser fornecidos);

**5.15.2.1.** Deve ser gerenciável via SSHv2;

**5.15.2.2.** O switch suportar o padrão X.509v3 para certificados digitais;

**5.15.2.3.** Deve permitir o espelhamento de uma porta e de um grupo de portas para uma porta especificada;

**5.15.2.4.** Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em um switch remoto no mesmo domínio L2 ou em outro domínio L2 através de tunelamento;

**5.15.2.5.** Deve implementar *Netflow*, *sFlow* ou similar;

**5.15.2.6.** Deve ser gerenciável via SNMPv3;

**5.15.2.7.** Deve implementar o protocolo *Syslog* para funções de "*logging*" de eventos;

**5.15.2.8.** Deve implementar o protocolo NTP ou SNTP;

**5.15.2.9.** Deve suportar autenticação *RADIUS*;

**5.15.2.10.** Deve suportar autenticação TACACS+;

**5.15.2.11.** Deve implementar controle de acesso por porta (IEEE 802.1x);

**5.15.2.12.** Deve implementar listas de controle de acesso (ACLs) baseadas em endereço IPv4 ou IPv6 de origem e destino, portas TCP e UDP de origem e destino e endereços MAC de origem e destino;

**5.15.2.13.** Deve possuir controle de *broadcast*, *multicast* e *unicast* por porta;

**5.15.2.14.** Deve implementar pelo menos uma fila de saída com prioridade estrita (SP *Strict Priority*) por porta e divisão ponderada (WRED, WRR ou similar) de banda entre as demais filas de saída;

**5.15.2.15.** Deve implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do *frame ethernet* (IEEE 802.1p CoS);

**5.15.2.16.** Deve implementar classificação, marcação e priorização de tráfego baseada nos valores do campo "*Differentiated Services Code Point*" (DSCP) do cabeçalho IP, conforme definições do IETF;

**5.15.2.17.** Deve implementar classificação de tráfego baseada em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino;

**5.15.2.18.** Deve formar um virtual switch, de forma que os dois possam ser vistos como uma entidade única, logicamente.

**5.15.3.** Suporte à funcionalidade de agregação de portas *multi-chassi*, através da criação de redundância ativa/ativa livre de loop e sem utilização de protocolo *Spanning Tree*, conforme as tecnologias MLAG, MC-LAG, M-LAG, Virtual *Link Trunking, Multi-Chassis EtherChannel* ou tecnologia semelhante que possibilite funcionalidade idêntica;

**5.15.3.1.** Deverão ser fornecidos todos os componentes necessários para garantia da alta disponibilidade, incluindo todos os módulos e/ou cabos/*transceivers* para interconexão dos equipamentos, bem como as licenças necessárias, caso aplicável;

**5.15.3.2.** Deve implementar no mínimo 3967 VLANs Ids conforme definições do padrão IEEE 802.1Q;

**5.15.3.3.** Deve implementar "VLAN *Trunking*" conforme padrão IEEE 802.1Q nas portas Ethernet. Deve ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos 802.1Q configurados.

**5.15.3.4.** Deve implementar a funcionalidade de "*Link Aggregation* (LAGs)" conforme padrão IEEE 802.3ad;

**5.15.3.5.** Deve suportar no mínimo 54 grupos por switch com até 8 portas por LAG (IEEE 802.3ad);

**5.15.3.6.** Deve implementar o padrão IEEE 802.1d, IEEE 802.1s e IEEE 802.1w;

**5.15.3.7.** Deve implementar mecanismo de proteção da "root bridge" do algoritmo *Spanning-Tree*;

**5.15.3.8.** Deve permitir a suspensão de recebimento de BPDUs (*Bridge Protocol Data Units*) caso a porta esteja colocada no modo "*fast forwarding*" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

**5.15.3.9.** Deve implementar o protocolo IEEE 802.1AB *Link Layer Discovery Protocol* (LLDP) e sua extensão LLDP-MED, permitindo a descoberta dos elementos de rede vizinhos;

**5.15.4.** O equipamento deve suportar funcionalidade de virtualização em camada 2 de modo a suportar diversidade de caminhos em camada 2 e agregação de *links* entre 2 *switches* distintos (*Layer* 2 *Multipathing*);

**5.15.4.1.** Deve possuir roteamento nível 3 entre VLANs;

**5.15.4.2.** Deve implementar protocolos de roteamento dinâmico OSPFv3;

**5.15.4.3.** Deve implementar protocolos de roteamento dinâmico BGPv4 e BGPv6 ou através de MP-BGP com suporte a IPV6;

**5.15.4.4.** Deve ter suporte a 120.000 (cento e vinte mil) rotas IPv4;

**5.15.4.5.** Deve ter suporte a 30.000 (trinta mil) rotas IPv6;

**5.15.4.6.** Deve trabalhar simultaneamente com protocolos IPv4 e IPv6;

**5.15.4.7.** Deve implementar VRF ou VRF-*Light* com suporte a no mínimo 32 instâncias;

**5.15.4.8.** Deve implementar *Policy Based Routing*;

**5.15.4.9.** Deve implementar o protocolo VRRP (Virtual *Router Redundancy Protocol*) v3.

## 5.16. CABOS E TRANSCEVEIRS

**5.16.1.** Devem ser fornecidos com pelo menos 08 (oito) cabos DAC passivo (100GB) padrão QSFP28 de no mínimo 1 (um) metro. Os cabos fornecidos deverão ser do mesmo fabricante do switch;

**5.16.2.** Devem ser fornecidos com pelo menos 24 (vinte a quatro) cabos DAC passivo (25Gb) padrão SFP28 de no mínimo 5 (cinco) metros. Os cabos fornecidos deverão ser do mesmo fabricante do switch;

**5.16.3.** Devem ser fornecidos com pelo menos 08 (oito) *transceivers* SFP28 25GBase-LR. Os *transceivers* fornecidos deverão ser do mesmo fabricante do switch;

**5.16.4.** Devem ser fornecidos com pelo menos 04 (quatro) *transceivers* SFP+ 10GBase-SR. Os *transceivers* fornecidos deverão ser do mesmo fabricante do switch;

**5.16.5.** Devem ser fornecidos com pelo menos 08 (oito) *transceivers* 1GBaseT. Os *transceivers* fornecidos deverão ser do mesmo fabricante do switch;

**5.16.6.** Devem ser fornecidos com pelos menos 04 (quatro) fibras óticas LC-LC multimodo OM4 com no mínimo 5metros;

**5.16.7.** Devem ser fornecidos com pelos menos 04 (quatro) fibras óticas LC-LC monomodo com no mínimo 5 metros;

**5.16.8.** Devem ser fornecidos com pelos menos 08 (oito) cabos par trançado RJ45 CAT5 5 metros.

## 5.17. SOFTWARE DE PROTEÇÃO E RECUPERAÇÃO (01 UNIDADE)

**5.17.1.** Poderão ser fornecidos mais de um produto afim de que todas as funcionalidades sejam atendidas desde que tais softwares sejam do mesmo fabricante e estejam contidos no mesmo pacote de licenciamento.

**5.17.1.1.** Devem ser propostos de forma a atender um mesmo ambiente de servidores e repositórios de dados de forma individual conforme descrito nesta especificação;

**5.17.1.2.** Deve ser ofertada a versão mais atual do(s) *software*(s), liberada oficialmente pelo fabricante. Caso haja necessidade, por razões de compatibilidade com os demais componentes de hardware e software do ambiente de backup, a Contratante se reserva o direito de utilizar a versão do software imediatamente anterior à versão mais atual, sem nenhum ônus adicional para a CONTRATANTE;

**5.17.2.** Todas as funcionalidades descritas poderão ser implementadas de maneira isolada pelo *software* de *backup* ou pela integração com *appliance* de dês duplicação, desde que devidamente homologadas pelo fabricante do *appliance*;

**5.17.3.** Deve implementar política de gerenciamento centralizada para múltiplos servidores de *backup*, mesmo que em diferentes plataformas, através de console única com interface gráfica;

**5.17.4.** O licenciamento do software deve ser por capacidade (*terabytes*) ou por processador (*socket*), permitindo utilizar em quantidade ilimitada os agentes e módulos do software de backup, enquanto mantendo-se o limite da quantidade contratada;

**5.17.5.** O licenciamento de software no modelo de capacidade (*terabytes*) deve considerar o volume máximo de dados medidos na origem que deve ser de no mínimo 100 (cem) TiB.

**5.17.6.** O licenciamento de software no modelo de licenciamento por processador (*socket*) deve ser considerado a quantidade de processadores físicos (*socket*) da solução hiperconvergente no total de no mínimo 12 (doze) *sockets*.

**5.17.7.** O servidor de *backup*, deverá ser disponibilizado no formato de "*vApp*", ou seja, uma Imagem de *appliance* virtual composto de sistema operacional otimizado e camada de software para *deploy* em *Hypervisor*;

**5.17.8.** Caso não disponha desta funcionalidade, deverá ser fornecido sistema operacional compatível com o servidor de backup;

**5.17.9.** Só serão aceitos sistemas operacionais que possuam o mesmo nível de serviços solicitado para a solução de backup;

**5.17.10.** O licenciamento deve permitir em quantidade ilimitada, integrações com uma ampla variedade de aplicações, permitindo desta forma o backup consistente, atendendo a lista abaixo:

**5.17.10.1.** Linux, Windows;

**5.17.10.2.** Ambientes Virtuais;

**5.17.10.3.** Banco de Dados;

**5.17.10.4.** Aplicações Microsoft;

**5.17.10.5.** SAP HANA;

**5.17.10.6.** Kubernetes.

**5.17.11.** Deve executar o *backup* de arquivos abertos (*open files*);

**5.17.12.** Deve possuir interface gráfica baseada em HTML5 sem necessidade de plug-in Flash ou Java;

**5.17.13.** Deve possuir em sua interface gráfica a funcionalidade de agendamento de processos de *backup* segundo políticas a serem definidas (periodicidade, período de retenção, agendamento, tipo de *backup*);

**5.17.14.** Deve possuir um banco de dados ou catálogo interno, contendo informações sobre todos os arquivos e mídias onde os backups foram armazenados. Caso o *software* não utilize bancos de dados proprietário, a licença do mesmo deve ser fornecida pela Contratada, com os mesmos níveis de suporte exigidos neste termo;

**5.17.15.** Possibilitar a reconstrução parcial ou total do catálogo ou banco de dados no caso de perda do mesmo;

**5.17.16.** Deve gerar automaticamente cópia de segurança da própria base de catálogos e configuração;

**5.17.17.** Possuir ambiente de gerenciamento de *backup* e *restore* via interface gráfica e linha de comando;

**5.17.18.** Deve suportar *backup* via LAN e WAN;

**5.17.19.** Deve suportar múltiplas operações de *backup* e *restore* simultâneas;

**5.17.20.** Deve permitir priorizar regras de proteção;

**5.17.21.** Deve permitir o estabelecimento de níveis de serviços (SLA) para as políticas de proteção baseados nos objetivos de nível de serviços (SLO);

**5.17.22.** Deve possuir funcionalidade de gerenciamento dos prazos de retenção por políticas definidas centralmente;

**5.17.23.** Deve possuir a funcionalidade de recuperar dados para servidores diferentes do equipamento de origem;

**5.17.24.** Deve permitir criar cópias de dados de diversas plataformas em um mesmo repositório simultaneamente;

**5.17.25.** Deve fazer uso do serviço de VSS (Volume *Shadow Copy*) para toda plataforma *Microsoft* que possua o serviço;

**5.17.26.** O *software* de *backup* deve possuir recurso que permita que o servidor cliente de *backup* envie os dados diretamente para um *appliance* de *backup* em disco, sem necessidade de que este dado seja transferido para o servidor de mídia de backup;

**5.17.27.** Deve implementar diferentes perfis de usuários, ao menos administradores e usuários simples;

**5.17.28.** Aos diferentes perfis de usuários, deve ser permitido atribuir ou revogar diferentes níveis de privilégios, tais como:

**5.17.28.1.** Acesso a logs de auditoria, configuração de assets, gerenciamento de segurança, gerenciamento de armazenamento, para usuários com perfil de administradores;

**5.17.28.2.** Acesso a monitoração do ambiente, acesso a visualização de logs, acesso a execução de atividades de *backup* e *restore*, para o perfil de usuário simples.

**5.17.29.** Deve suportar LDAP para autenticação de usuários;

**5.17.30.** Possuir interfaces de gerenciamento/monitoração por *Browser*;

**5.17.31.** Deve possibilitar a criação de diferentes usuários com diferentes perfis de acesso (preferencialmente através de integração com AD);

**5.17.32.** Deve possuir funcionalidade para envio de alertas através de e-mail, *Script* ou via *Windows Event Log*;

**5.17.33.** Deve possuir funcionalidade para informar *jobs* de *backup* completados ou não com sucesso;

**5.17.34.** Deve disponibilizar console *Web* para busca granular dos arquivos protegidos nos servidores.

**5.17.35.** A solução deverá controlar o envio de dados de *backup* para armazenamento em nuvem a partir do *appliance* de *backup*;

**5.17.36.** Monitoração e relatórios

**5.17.37.** Deve possuir serviço de monitoração e relatórios baseado em nuvem (SaaS), permitindo que qualquer usuário autorizado com acesso à *internet* possa, a partir de um portal, verificar as seguintes informações do ambiente via navegador suportado:

**5.17.38.** Status das políticas de *backup*;

**5.17.39.** Sumário da proteção dos ativos;

**5.17.40.** Lista das maiores violações de níveis de serviços estabelecidos para o *backup*;

**5.17.41.** Lista de conformidade de ativos de acordo com o os níveis de serviços estabelecidos;

**5.17.42.** Alertas críticos das últimas 24 horas;

**5.17.43.** Capacidade ocupada de sistemas de armazenamento do *backup*;

**5.17.44.** Reportes de ativos protegidos, podendo ser exportado pelo menos no formato CSV;

**5.17.45.** Reportes de conformidade da proteção dos ativos protegidos podendo ser exportado pelo menos no formato CSV;

**5.17.46.** Possibilidade de aplicar filtros, incluir e excluir campos no relatório;

**5.17.47.** Proteção de dados contínua e replicação.

**5.17.48.** Deve possuir mecanismo capaz de realizar a replicação de máquinas virtuais *VMWare* local e remota realizando clones e snapshots com proteção contínua dos dados por máquina virtual;

**5.17.49.** A solução deverá permitir o uso de recursos avançados de proteção baseado em CDP (*Continuos Data Protection* ou Proteção Contínua de Dados) para garantir o POR próximo ou igual a zero para as aplicações críticas utilizadas pela CONTRATANTE. Esta funcionalidade deverá ser capaz de realizar a proteção local em nível de VM ou bloco entre os volumes usando CDP que registra cada gravação para recuperação posterior em qualquer *point-in-time*.

**5.17.50.** Deverá permitir a replicação de máquinas virtuais *VMWare* utilizando recursos de otimização de tráfego através de dês duplicação e compressão dos dados para outra localidade através de rede IP;

**5.17.51.** A solução deve permitir configurar a priorização de VMs e reconfiguração de endereço IP das máquinas virtuais em caso de *failover* entre sites;

**5.17.52.** Deve permitir a orquestração e execução de rotinas customizáveis (scripts) de pré e pós-processo durante o *failover* das máquinas virtuais.

**5.17.53.** Deve suportar replicar máquinas virtuais que façam uso de discos RDM (*Raw Device Mapping*) e VMDK;

**5.17.54.** Deve permitir a replicação local e remota de máquinas virtuais que façam uso de discos RDM (Raw Device Mapping) para VMs com disco VMDK e vice-versa;

**5.17.55.** Deverá permitir testes não disruptivos de desastre utilizando a imagem da VM de replica sem impacto e indisponibilidade no ambiente produtivo;

**5.17.56.** Proteção de file systems de hosts

**5.17.57.** O agente deve implementar dês duplicação na origem dos dados;

**5.17.58.** Deve permitir o backup full, incremental;

**5.17.59.** Deve permitir execução de backups tipo full sintético, que permite a criação de uma única imagem de backup a partir de um backup full e qualquer quantidade de backup incrementais. O restore deverá ser efetuado a partir da nova imagem full sintética;

**5.17.60.** Deve suportar volumes tipo LVM e VxVM;

**5.17.61.** Deve permitir o backup e restore centralizado com datapath direto para o repositório de dados;

**5.17.62.** Deve permitir o backup e restore descentralizado a partir do host, também chamado de self service; mantendo a consistência de catálogo da aplicação de backup;

**5.17.63.** Deve permitir o restore no nível de arquivos para o host de origem ou hosts distintos;

**5.17.64.** Deve suportar filtros de exclusão de arquivos como data de criação, data de alteração, tamanho e caminho. Deve permitir o uso de operadores lógicos como "E" e "OU";

**5.17.65.** Deve permitir backups tipo FBB (file backup level) e BBB (Block Backup Level) em ambientes Linux e Windows;

**5.17.66.** Deve suportar pelo menos sistemas de arquivos tipo ext2, ext3, xfs, refs e ntfs;

**5.17.67.** Proteção de Ambientes Vmware

**5.17.68.** Suportar integração com Vmware através do vStorage API;

**5.17.69.** Realizar o backup e recuperação das máquinas virtuais Vmware utilizando a tecnologia de CBT (*Change Block Tracking*);

**5.17.70.** Suportar backup e restore de máquina virtual Vmware, suportando backup de guest e backup de imagem com restore individual de arquivos e diretórios em ambientes Windows e Linux;

**5.17.71.** Deve possuir a funcionalidade de utilização de filtros de backup, tanto para inclusão como para exclusão de determinados tipos e características de arquivos;

**5.17.72.** Possuir console Web que permita que o administrador das máquinas virtuais execute o restore granular de arquivos sem necessidade de recuperar a VM completa;

**5.17.73.** Os servidores de "proxy" necessários para backup das máquinas virtuais VMWare deverão ser no formato virtual ("Virtual Appliance"). O Sistema Operacional do servidor proxy deverá ser licenciado e nativo do produto;

**5.17.74.** Disponibilizar plug-in de integração com a interface do usuário vSphere Web Client, de forma a permitir que as funções de backup e recuperação possam ser gerenciadas diretamente pela console do VMWare;

**5.17.75.** Possuir plugin nativo para integração com vSphere e vRealize Automation;

**5.17.76.** Deve prover mecanismo capaz de indexar metadados de arquivos contidos em backups de máquinas virtuais permitindo operações de buscas baseadas em parâmetros configuráveis.

**5.17.77.** Deve permitir a descoberta e backup automático de máquinas virtuais adicionadas a um vCenter protegido;

**5.17.78.** Executar a inicialização de uma VM diretamente do repositório de backup sem a necessidade de restore.

**5.17.79.** Proteção em ambientes SQL Server

**5.17.80.** Deve fazer a descoberta automática das bases de dados contidas em um servidor;

**5.17.81.** O agente deve implementar desduplicação na origem dos dados;

**5.17.82.** Deve permitir o backup full e incremental;

**5.17.83.** Deve fazer uso de VDI;

**5.17.84.** Deve permitir a cópia consistente de bases de dados a partir do backup tipo Image da VM em ambientes Vmware;

**5.17.85.** Deve permitir o backup e restore centralizado consistente de bases de dados com datapath direto para o repositório de dados;

**5.17.86.** Deve permitir o backup e restore descentralizado a partir do host, também chamado de self service; mantendo a consistência de catálogo da aplicação de backup;

**5.17.87.** Deve permitir o restore no nível de database ou de tabelas;

**5.17.88.** Deve permitir o acesso instantâneo à base de dados à partir do repositório de backup, sem a necessidade de restore;

**5.17.89.** Proteção em ambientes Oracle

**5.17.90.** Deve fazer a descoberta automática das bases de dados contidas em um servidor;

**5.17.91.** O agente deve implementar desduplicação na origem dos dados;

**5.17.92.** Deve permitir o backup full, incremental e logs;

**5.17.93.** Deve fazer uso do RMAN;

**5.17.94.** Deve permitir o backup e restore centralizado consistente de bases de dados com datapath direto para o repositório de dados;

**5.17.95.** Deve permitir o backup e restore descentralizado a partir do host, também chamado de self service; mantendo a consistência de catálogo da aplicação de backup;

**5.17.96.** Deve permitir o restore no nível de database ou de tabelas;

**5.17.97.** Proteção em ambientes SAP HANA

**5.17.98.** O agente deve implementar desduplicação na origem dos dados;

**5.17.99.** Deve permitir o backup full e incremental;

**5.17.100.** Deve fazer uso do Backint;

**5.17.101.** Deve permitir o backup e restore centralizado consistente de bases de dados com datapath direto para o repositório de dados;

**5.17.102.** Deve permitir o backup e restore descentralizado a partir do host, também chamado de self service; mantendo a consistência de catálogo da aplicação de backup;

**5.17.103.** Deve suportar SDC, MDC, Standalone, Multi-host, Scale-Out, High-Isolation.

**5.17.104.** Proteção em ambientes Exchange

**5.17.105.** O agente deve implementar desduplicação na origem dos dados;

**5.17.106.** Deve fazer uso de BBB;

**5.17.107.** Deve permitir o backup e restore centralizado consistente com datapath direto para o repositório de dados;

**5.17.108.** Deve permitir o backup e restore descentralizado a partir do host, também chamado de self service; mantendo a consistência de catálogo da aplicação de backup;

**5.17.109.** Deve suportar implementações Standalone, DAG & IP-Less DAG;

**5.17.110.** Proteção de ambientes Kubernetes

**5.17.111.** Deve possuir integração nativa com Kubernetes no nível de namespaces e PVCs, não sendo aceitos scripts ou backups no nível de sistema de arquivos para atendimento a esse item;

**5.17.112.** Deve suportar volumes contidos em armazenamento tipo CSI-based;

**5.17.113.** Deve ser compatível com Container Storage Interface (CSI) driver;

**5.17.114.** Deve suportar o backup de volumes persistentes com modo de volume "Fileystem";

**5.17.115.** Utilizar recursos de desduplicação na origem, transferindo apenas os blocos únicos durante o processo de backup do Kubernetes.

**5.17.116.** Deve realizar o backup completo do Namespace e seus objetos como: Pods, Secrets, Services, Deployments, Replica set, Certificates, ConfigMaps e Persistent Volumes.

**5.17.117.** Deve ser possível a visualização dos diversos clusteres Kubernetes e seus componentes protegidos a partir da console de gerenciamento de backup;

**5.17.118.** Serão aceitas composições com softwares de terceiro para prover as funcionalidades solicitadas, desde que o nível de suporte atenda ao solicitado desde que centralizado;

**5.17.119.** Deve ser capaz de realizar a descoberta automática de namespaces dentro de um cluster;

**5.17.120.** Deve realizar a descoberta automática dos containers e seus volumes persistentes configurados.

**5.17.121.** Possuir políticas de backup dinâmicas onde através de filtros e regras um novo Namespace pode ser protegido em uma determinada política de maneira automática, sem intervenção do administrador.

**5.17.122.** Permitir o restore do Namespace nos seguintes formatos:

**5.17.122.1.** Restore para o Namespace original;

**5.17.122.2.** Restore para um Namespace existente;

**5.17.122.3.** Restore para um novo Namespace;

**5.17.122.4.** Restore do Namespace em um outro cluster Kubernetes diferente da origem;

**5.17.122.5.** Deve permitir o backup e restore centralizado consistente com datapath direto para o repositório de dados;

**5.17.122.6.** Permitir excluir determinados volumes persistentes (PV) durante a rotina de backup

**5.17.122.7.** Deve permitir o backup e restore descentralizado a partir do host, também chamado de self service; mantendo a consistência de catálogo da aplicação de backup;

**5.17.122.8.** Suportar diferentes distribuições de Kubernetes em ambientes VMWare e Red Hat OpenShift.

## 5.18. APPLIANCE DE BACKUP EM DISCO (02 UNIDADES)

**5.18.1.** Deverá obrigatoriamente fazer uso de sistemas inteligentes de armazenamento de backup em disco, baseado em "Appliance", que se entende como um subsistema com o propósito específico de entrada dos dados de backup, desduplicação e replicação;

**5.18.2.** O "Appliance" deverá ser composto, de processamento e armazenamento integrado, dedicado única e exclusivamente, à execução das atividades de entrada, desduplicação e replicação dos dados enviados pelos servidores de backup;

**5.18.3.** O hardware do "Appliance" não poderá ser compartilhado com nenhum outro software;

**5.18.4.** O Sistema Operacional do equipamento deverá ser licenciado e nativo do produto. Não serão aceitas as modalidades OEM de sistemas operacionais de propósito geral, tal como Windows ou Unix/Linux;

**5.18.5.** A desduplicação deve segmentar os dados em blocos de tamanho variável ajustado automaticamente pelo algoritmo do appliance;

**5.18.6.** A desduplicação deverá ser global considerando todos os dados armazenados no equipamento em sua total capacidade disponível, ou seja, deverá comparar e identificar dados duplicados provenientes de diferentes servidores e protocolos de acesso de forma a atingir melhores taxas de desduplicação, mesmo que estejam em partições lógicas ou físicas diferentes do mesmo subsistema. Será facultada a utilização de soluções que não fazem uso da desduplicação global, desde que a área líquida solicitada seja acrescida em 50% (cinquenta por cento) de forma a compensar a menor eficiência deste tipo de tecnologia;

**5.18.7.** Possuir tecnologia de desduplicação de dados em linha (inline), ou seja, os dados de backup são desduplicados em CPU e memória antes mesmo de sua gravação em disco. Não serão aceitas soluções que realizem a desduplicação após a gravação do dado no disco (pós-processo) ou mesmo híbridas que realizem parte do processo antes e parte após a gravação do dado no disco;

**5.18.8.** A solução deve fazer uso de recursos dedicados para realizar a compressão dos dados via hardware após a desduplicação dos dados, de forma que este processo de compressão não deve impactar o desempenho do equipamento. Será facultada a utilização de soluções que não fazem uso de compressão após a desduplicação, desde que a área líquida solicitada seja acrescida em 50% (cinquenta por cento) de forma a compensar a menor eficiência deste tipo de tecnologia;

**5.18.9.** O sistema inteligente de armazenamento de backup em disco deve permitir realizar a replicação otimizada dos dados (off-host) sem onerar a CPU dos servidores de backup;

**5.18.10.** O sistema inteligente de armazenamento de backup em disco deve permitir replicar os dados através de rede IP de forma criptografada;

**5.18.11.** Deve suportar replicação 1 para N, N para 1 (várias origens e 1 destino) e cascata;

**5.18.12.** O sistema inteligente de armazenamento de backup em disco deverá ser capaz de suportar falhas de até dois discos, devendo ser fornecido com proteção RAID-6 ou similar;

**5.18.13.** Devido ao tempo de reconstrução do RAID em caso de falha do disco, a área de armazenamento da solução deverá ser disponibilizada em conjuntos de discos rígidos com tecnologia SAS com capacidade máxima de 8TB (oito terabytes) brutos cada.

**5.18.14.** O sistema inteligente de armazenamento de backup deve ser fornecido com no mínimo um disco "Hot-Spare" para cada RAID group ou gaveta de discos;

**5.18.15.** O(s) disco(s) de "hot spare" devem ser utilizados de forma global dentro do Appliance;

**5.18.16.** A solução deverá possuir sistema de proteção interno utilizando snapshots internos que permitam melhorar a segurança dos dados e índices e permitir a recuperação para um momento anterior;

**5.18.17.** Deverá possuir mecanismos que não permitam a inconsistência dos dados mesmo em casos de interrupção abrupta ou desligamento acidental, por meio de memória não volátil dedicada a operações de escrita ou recurso similar.

**5.18.18.** Deve possuir mecanismo inteligente que verifique continuamente de forma automática a integridade lógica dos dados, "ponteiros" e índices armazenados (fim-a-fim) no hardware com correção automática das falhas encontradas, de forma a garantir a consistência de todo o conteúdo em sua total capacidade, sem a utilização de scripts e/ ou composições feitas exclusivamente para atendimento a esse item.

**5.18.19.** Deverá possuir interface de administração GUI e CLI;

**5.18.20.** A solução ofertada deve suportar a integração comprovada por matriz de compatibilidade com o software Oracle RMAN e estar inscrita na lista de fabricantes homologados pelo Oracle Backup Solutions Program (BSP) através do site (http://www.oracle.com/technetwork/database/features/availability/bsp-088814.html), permitindo que o backup e restore do banco de dados Oracle possam ser feitos diretamente para o Appliance, sem utilização de software adicional de backup;

**5.18.21.** A solução deverá suportar a criptografia dos dados desduplicados sem necessidade de equipamento adicional;

**5.18.22.** Permitir o particionamento lógico da área de armazenamento (*Mult-Tenant*), sem prejuízo as características de dês duplicação solicitadas neste certame;

**5.18.23.** A controladora deve possuir no mínimo 2 processadores *multi-core*;

**5.18.24.** A controladora deve possuir ao menos 192GB de memória RAM. Não serão aceitas como memória a utilização de tecnologias Flash, SSD ou qualquer outra tecnologia de extensão de memória cache;

**5.18.25.** A solução deve fazer uso de discos do tipo SSD (*Solid State Drive*) para aceleração dos dados. Será facultada a oferta do dobro (2x) de memória

cache solicitada neste certame para as soluções que não fazem uso de discos Flash ou SSD para aceleração, de forma a compensar a menor eficiência deste tipo de equipamento.

**5.18.26.** Deverá possuir no mínimo 100TB úteis, base 10, sem considerar ganhos com dês duplicação e compressão de dados;

**5.18.27.** Deverá suportar as seguintes interfaces de interconexão com os servidores de *backup*: interfaces Fibre *Channel* (FC) 16Gb, interfaces 10GbE e 25Gb Ethernet;

**5.18.28.** O equipamento deve estar licenciado para permitir acesso através de: CIFS, NFS, NDMP, VTL (Virtual *Tape Library*);

**5.18.29.** O equipamento deve fazer uso de API para permitir que os backups sejam acessados e enviados para o repositório de backup sem que o volume esteja montado no servidor de backup, eliminando qualquer risco de propagação *Ransomware* e acesso aos dados de backups armazenados;

**5.18.30.** Deve permitir a emulação de Tape *Libraries* Virtuais (VTL) utilizando protocolo *Fiber Channel,* suportando no mínimo;

**5.18.31.** 64 (sessenta e quatro) *Tape Libraries* Virtuais (VTL);

**5.18.32.** 540 (quinhentos e quarenta) *Tape Drivers* em VTL;

**5.18.33.** 64.000 (sessenta e quatro mil) cartuchos de fitas em VTL;

**5.18.34.** Deverá ser fornecido com no mínimo 04 (quatro) portas Ethernet 25Gbps ótico padrão SFP28;

**5.18.35.** Devem ser fornecidos com pelo menos 04 (quatro) cabos DAC (*Direct Attach Cable*) *twinax* passivo (25Gbps) padrão SFP28 de 03 (três) metros. Os cabos fornecidos deverão ser do mesmo fabricante do appliance e compatíveis com os switches ofertados.

**5.18.36.** Deverá possuir performance de ingestão de no mínimo 27TB/hora de dados transferidos;

**5.18.37.** Deve suportar no mínimo 270 *jobs* de gravação simultanêa.

**5.18.38.** Deverá utilizar padrão de criptografia AES-256 para replicação dados em trânsito (*in-flight*) e em repouso (*at-rest*). Seguindo, no mínimo, as regras estabelecidas para o nível de segurança do padrão FIPS 140-2.

**5.18.39.** O processo de exclusão dos dados armazenados (data *shredding*) deve seguir os padrões de segurança estabelecidos no *National Institute of Systems and Technology* (NIST) SP800-88.

**5.18.40.** A solução deve possuir recurso de mídia WORM (*Write Once Read Many*) SEC 17a-4 (f) de proteção contra alteração/regravação e exclusão dos dados armazenados, permitindo somente uma única escrita e múltiplas leituras, garantindo integridade e autenticidade, deste modo a solução não deverá permitir que usuários consigam alterar ou apagar dados protegidos, até que o tempo de retenção configurado tenha expirado. Será facultada a utilização de softwares externos desde que licenciado para toda capacidade fornecida sem ônus para CONTRATANTE.

**5.18.41.** Deverá ter suporte ao protocolo de monitoramento SNMP v2 e v3;

**5.18.42.** O equipamento deve suportar nativamente enviar de forma dês duplicada e criptografada os dados de backup para um armazenamento em nuvem pública ou privada utilizando-se de políticas internas de movimentação baseadas no tempo de acesso dos dados. O licenciamento desta funcionalidade não faz parte deste certame;

**5.18.43.** As rotinas internas de manutenção dos dados de backup armazenados como: Validação de integridade (data *integrity*), devem ser executados em paralelo com as rotinas de backup e recuperação, ou seja, a solução ofertada não deve exigir parada ou interrupção (*blackout window*) das atividades de *backup/restore* para tarefas internas do equipamento.

**5.18.44.** Deve possuir fontes redundantes possibilitando a substituição sem a necessidade de parada do sistema.

**5.18.45.** A solução deve possuir no próprio hardware do equipamento função de "*call-home*" ou *e-mail* para notificar de forma automática quaisquer problemas para a central do fabricante.

## 5.19. REQUISITOS GERAIS DE FUNCIONALIDADES E LICENCIAMENTOS PARA FIREWALL (02 UNIDADES TIPO 01 E 120 UNIDADES TIPO 02)

**5.19.1.** Deverá possuir controle de acesso à internet por endereço IP de origem e destino;

**5.19.2.** Deverá possuir controle de acesso à internet por subrede;

**5.19.3.** Deverá suportar tags de VLAN (802.1q);

**5.19.4.** Deverá possuir ferramenta de captura de pacotes para diagnóstico do tipo tcpdump ou similar;

**5.19.5.** Deverá possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;

**5.19.6.** Deverá possuir integração com tokens para autenticação de dois fatores;

**5.19.7.** Deverá suportar single-sign-on para Active Directory e RADIUS;

**5.19.8.** Deverá possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

**5.19.9.** Deve suportar NAT64 e NAT46;

**5.19.10.** Deverá permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

**5.19.11.** Deverá permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br;

**5.19.12.** Deverá possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;

**5.19.13.** Deverá suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGP;

**5.19.14.** Deverá possuir funcionalidades de DHCP Cliente, Servidor e Relay;

**5.19.15.** Deverá permitir o funcionamento em modo transparente tipo "bridge" sem alterar o endereço MAC do tráfego;

**5.19.16.** Deverá suportar PBR – Policy Based Routing;

**5.19.17.** Deverá permitir a criação de VLANS no padrão IEEE 802.1q;

**5.19.18.** O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS)

**5.19.19.** Deverá suportar roteamento multicast PIM Sparse Mode e Dense Mode;

**5.19.20.** Deverá permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos: TCP, UDP, ICMP e IP;

**5.19.21.** Deverá permitir o agrupamento de serviços;

**5.19.22.** Deverá permitir o filtro de pacotes sem a utilização de NAT;

**5.19.23.** Deverá permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

**5.19.24.** Deverá possuir mecanismo de anti-spoofing;

**5.19.25.** Deverá permitir criação de regras definidas pelo usuário;

**5.19.26.** Deverá permitir o serviço de autenticação para tráfego HTTP e FTP;

**5.19.27.** Deverá permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;

**5.19.28.** Deverá possuir a funcionalidade de balanceamento e contingência de links;

**5.19.29.** Deverá suportar sFlow;

**5.19.30.** O dispositivo deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando, ao menos: Yahoo! Messenger, MSN Messenger, ICQ, AOL Messenger, BitTorrent, eDonkey, GNUTella, KaZaa, Skype e WinNY;

**5.19.31.** Deverá ter a capacidade de permitir a criação de regras de firewall específicas para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows;

**5.19.32.** Deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;

**5.19.33.** Deverá permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação;

**5.19.34.** Deverá suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP;

**5.19.35.** Deverá permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN tagged;

**5.19.36.** Deverá possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS;

**5.19.37.** Deverá suportar SIP, H.323 e SCCP NAT Traversal;

**5.19.38.** Deverá permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras.

## 5.20. FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

**5.20.1.** Deverá permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;

**5.20.2.** Deverá permitir modificação de valores DSCP para o DiffServ;

**5.20.3.** Deverá permitir priorização de tráfego e suportar ToS;

**5.20.4.** Deverá limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web;

**5.20.5.** Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

**5.20.6.** Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

**5.20.7.** Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

**5.20.8.** Deverá permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação;

**5.20.9.** Deverá controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino;

**5.20.10.** Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

**5.20.11.** Deverá ter a capacidade de permitir a criação de perfis de controle de banda específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows.

## 5.21. FUNCIONALIDADE DE ANTI-SPAM DE GATEWAY

**5.21.1.** Deverá permitir, na funcionalidade de AntiSpam, verificação do cabeçalho SMTP do tipo MIME;

**5.21.2.** Deverá possuir filtragem de e-mail por palavras chaves;

**5.21.3.** Deverá permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;

**5.21.4.** Deverá possuir, para a funcionalidade de AntiSpam, o recurso de RBL;

**5.21.5.** Deverá permitir a checagem de reputação da URL no corpo mensagens de correio eletrônico.

## 5.22. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

**5.22.1.** Deverá possuir solução de filtro de conteúdo Web integrado à solução de segurança;

**5.22.2.** Deverá possuir, pelo menos, 70 (setenta) categorias para classificação de sites Web;

**5.22.3.** Deverá possuir base mínima contendo 100.000.000 (cem milhões) de sites internet Web já registrados e classificados;

**5.22.4.** Deverá possuir a funcionalidade de cota de tempo de utilização por categoria;

**5.22.5.** Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como:

**5.22.5.1.** Proxy anônimo;

**5.22.5.2.** Webmail;

**5.22.5.3.** Instituições de saúde;

**5.22.5.4.** Notícias;

**5.22.5.5.** Phishing;

**5.22.5.6.** Hackers;

**5.22.5.7.** Pornografia;

**5.22.5.8.** Racismo;

**5.22.5.9.** Websites pessoais;

**5.22.5.10.** Compras;

**5.22.6.** Deverá permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

**5.22.7.** Deverá permitir a criação de categorias personalizadas;

**5.22.8.** Deverá permitir a reclassificação de sites Web por URL.

**5.22.9.** Deverá prover Termo de Responsabilidade on-line para aceite pelo usuário, a ser apresentado toda vez que houver tentativa de acesso a determinado serviço permitido ou bloqueado;

**5.22.10.** Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

**5.22.11.** Deverá possuir integração com tokens para autenticação de 2 fatores;

**5.22.12.** Deverá exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;

**5.22.13.** Deverá permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;

**5.22.14.** Deverá permitir a criação de listas personalizadas de URLs permitidas e bloqueadas;

**5.22.15.** Deverá permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;

**5.22.16.** Deverá filtrar o conteúdo baseado em categorias em tempo real;

**5.22.17.** Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

**5.22.18.** Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

**5.22.19.** Deverá ser capaz de categorizar a página Web por URL.

**5.22.20.** Deverá possuir Proxy Explícito e Transparente;

**5.22.21.** Deverá implementar roteamento WCCP e ICAP.

## 5.23. FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO

**5.23.1.** Deverá permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;

**5.23.2.** Deverá possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas;

**5.23.3.** Deverá permitir funcionar em modo transparente, *sniffer* e *router*;

**5.23.4.** Deverá possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;

**5.23.5.** Deverá permitir a criação de padrões de ataque manualmente;

**5.23.6.** Deverá possuir integração à plataforma de segurança;

**5.23.7.** Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a webserver, para que seja usado para proteção específica de Servidores Web;

**5.23.8.** Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como *Denial of Service* (DoS) do tipo *Flood*, *Scan*, *Session* e *Sweep*;

**5.23.9.** Deverá possuir mecanismos de detecção/proteção de ataques;

**5.23.10.** Deverá possuir análise de protocolos;

**5.23.11.** Deverá possuir detecção de anomalias;

**5.23.12.** Deverá possuir detecção de ataques de RPC (*Remote Procedure Call*);

**5.23.13.** Deverá possuir proteção contra-ataques de SMTP (*Simple Message Transfer Protocol*), IMAP (*Internet Message Access Protocol*), *Sendmail* ou POP (*Post Office Protocol*);

**5.23.14.** Deverá possuir proteção contra-ataques DNS (*Domain Name System*);

**5.23.15.** Deverá possuir proteção contra-ataques a FTP e SSH;

**5.23.16.** Deverá possuir proteção contra-ataques de ICMP (*Internet Control Message Protocol*);

**5.23.17.** Deverá possuir métodos de notificação de detecção de ataques;

**5.23.18.** Deverá possuir alertas via correio eletrônico;

**5.23.19.** Deverá possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede

**5.23.20.** Deverá ter a capacidade de resposta/logs ativa a ataques;

**5.23.21.** Deverá prover a terminação de sessões via TCP resets;

**5.23.22.** Deverá armazenar os *logs* de sessões;

**5.23.23.** Deverá atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

**5.23.24.** Deverá mitigar os efeitos dos ataques de negação de serviços;

**5.23.25.** Deverá permitir a criação de assinaturas personalizadas;

**5.23.26.** Deverá possuir filtros de ataques por anomalias;

**5.23.27.** Deverá permitir filtros de anomalias de tráfego estatístico de: *flooding*, *scan*, *source* e *destinationsessionlimit*;

**5.23.28.** Deverá suportar reconhecimento de ataques de DoS, *reconnaissance*, *exploits* e *evasion*;

**5.23.29.** Deverá suportar verificação de ataque na camada de aplicação;

**5.23.30.** Deverá suportar verificação de tráfego em tempo real, via aceleração de *hardware*;

**5.23.31.** Deverá possuir as seguintes estratégias de bloqueio: *pass*, *drop* e *reset*.

## 5.24. FUNCIONALIDADE DE VPN

**5.24.1.** Deverá possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;

**5.24.2.** Deverá possuir suporte a certificados PKI X.509 para construção de VPNs;

**5.24.3.** Deverá possuir suporte a VPNs IPSeC Site-to-Site e VPNs IPSec *Client-to-Site*;

**5.24.4.** Deverá possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;

**5.24.5.** Deverá permitir a arquitetura de VPN *hub and spoke*;

**5.24.6.** Deverá possuir suporte à inclusão em autoridades certificadoras (*enrollment*), mediante SCEP (*Simple Certificate Enrollment Protocol)* e mediante arquivos.

## 5.25. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

**5.25.1.** Deverá reconhecer, no mínimo, 2.000 (duas mil) aplicações;

**5.25.2.** Deverá possuir, pelo menos, 10 (dez) categorias para classificação de aplicações;

**5.25.3.** Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como:

**5.25.3.1.** P2P;

**5.25.3.2.** *Instant Messaging*;

**5.25.3.3.** *Web*;

**5.25.3.4.** Transferência de arquivos;

**5.25.3.5.** VoIP;

**5.25.4.** Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

**5.25.5.** Deverá ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;

**5.25.6.** Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o *Microsoft Active Directory*, reconhecendo grupos de usuários cadastrados;

**5.25.7.** Deverá permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo, as seguintes categorias: *Instant Messaging* e transferência de arquivos;

**5.25.8.** Deverá permitir criação de padrões de aplicação manualmente.

## 5.26. FUNCIONALIDADE DE BALANCEAMENTO DE CARGA

**5.26.1.** Deverá permitir a criação de endereços IPs virtuais;

**5.26.2.** Deverá permitir balanceamento de carga entre servidores;

**5.26.3.** Deverá suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP;

**5.26.4.** Deverá permitir balanceamento, ao menos, com os seguintes métodos: *Round Robin*, *Weighted*, *First Alive* e HTTP *host*;

**5.26.5.** Deverá permitir persistência de sessão por cookie HTTP ou SSL *session* ID;

**5.26.6.** Deverá permitir que seja mantido o IP de origem;

**5.26.7.** Deverá suportar SSL *offlolading* nos equipamentos;

**5.26.8.** Deverá ter a capacidade de identificar, através de *health checks*, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;

**5.26.9.** Deverá permitir que o *health check* seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP em URL configurável.

## 5.27. FUNCIONALIDADE DE VIRTUALIZAÇÃO

**5.27.1.** Deverá suportar a criação de, ao menos, 10 (dez) instâncias virtuais no mesmo *hardware*;

**5.27.2.** Deverá permitir a criação de administradores independentes para cada uma das instâncias virtuais;

**5.27.3.** Deverá permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.

## 5.28. FUNCIONALIDADE DE SD-WAN

**5.28.1.** A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.

**5.28.2.** A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos.

**5.28.3.** A solução SD-WAN deve suportar microsegmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN.

**5.28.4.** A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações.

**5.28.5.** Solução deve ser capaz de prover Zero Touch *provisioning*.

**5.28.6.** A solução de Zero Touch *provisioning* deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN.

**5.28.7.** Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Matriz x Filiais, em que a comunicação de uma Filial A para a Matriz esteja comprometida, possa ser utilizada a comunicação entre Filial B e Matriz, em que através deste circuito, a Filial A alcance a Matriz.

**5.28.8.** A solução deve ser capaz de criar VPN "*Full- Mesh*" em interface Gráfica, de forma automática, e sem que o administrador precise configurar site por site.

**5.28.9.** A configuração VPN IPSEC deverá oferecer suporte para DH *Group*: 14 e 15.

**5.28.10.** Deve de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à um determinado IP/ range de IPs de destino.

**5.28.11.** A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv6;

**5.28.12.** A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD- WAN em condições onde a largura de banda é modificada.

## 5.29. CARACTERÍSTICAS MINIMAS DO FIREWALL (APPLIANCE DE SEGURANÇA TIPO 01)

**5.29.1.** DISPOSITIVO DE SEGURANÇA CIBERNÉTICA DISTRIBUÍDA – NGFW

**5.29.2.** Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.

**5.29.3.** Poderá ser entregue em equipamento único ou com composição de equipamentos, para atender as funcionalidades exigidas.

**5.29.4.** Deverá possuir e estar licenciado pelo período de 60 (sessenta) meses com as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, Otimização WAN, Controladora Wireless e virtualização.

**5.29.5.** Firewall com capacidade mínima de processamento de 06 (seis) Gbps.

**5.29.6.** IPS com capacidade mínima de processamento de 8 (oito) Gbps.

**5.29.7.** Proteção a ameaças avançadas, isto é, com as funções de Firewall, IPS, controle de aplicação e proteção de Malware/Antivírus ativadas, com capacidade mínima de processamento de 5 (cinco) Gbps.

**5.29.8.** Inspeção SSL Throughput com capacidade mínima de processamento de 6 (seis) Gbps.

**5.29.9.** VPN com capacidade de, pelo menos, 30 (trinta) Gbps de tráfego IPSec.

**5.29.10.** Deverá suportar 10.000.000 (dez milhões) de conexões TCP simultâneas.

**5.29.11.** Deverá suportar, pelo menos, 300.000 (trezentos mil) novas conexões TCP por segundo.

**5.29.12.** Deverá suportar, pelo menos, 1.500 (mil e quinhentos) túneis de VPN Site-Site.

**5.29.13.** Deverá suportar, pelo menos, 15.000 (quinze mil) túneis de VPN Client-Site.

**5.29.14.** Deverá possuir, pelo menos, 16 (dezesseis) interfaces RJ45.

**5.29.15.** Deverá possuir, pelo menos 6 (seis) interfaces SFP+

**5.29.16.** Deverá possuir, pelo menos 2 (duas) interfaces SFP

**5.29.17.** Deverá possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.

**5.29.18.** Deve ser fornecido pelo menos 4 (quatro) Transceivers 10 GE SFP+ SR

**5.29.19.** Deverá possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de proteção avançada durante a vigência contratual.

**5.29.20.** Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 200 (duzentos) Pontos de Acesso sem fio.

**5.29.21.** Deverá ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 60 (sessenta) equipamentos.

**5.29.22.** Deverá incluir licença para atualização de vacina de antivírus/anti-spyware.

**5.29.23.** Deverá incluir licença de atualização para filtro de conteúdo Web.

**5.29.24.** Deverá incluir licença de atualização do IPS e da lista de aplicações detectadas.

**5.29.25.** Deverá ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.

**5.29.26.** O equipamento deve possuir homologação junto à Anatel.

## 5.30. CARACTERÍSTICAS MINIMAS DO FIREWALL (APPLIANCE DE SEGURANÇA TIPO 02)

**5.30.1.** Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.

**5.30.2.** Poderá ser entregue em equipamento único ou com composição de equipamentos, para atender as funcionalidades exigidas.

**5.30.3.** Firewall com capacidade mínima de processamento de 1 (um) Gbps.

**5.30.4.** IPS com capacidade mínima de processamento de 1.2 Gbps.

**5.30.5.** Proteção a ameaças avançadas, isto é, com as funções de Firewall, IPS, controle de aplicação e proteção de Malware/Antivírus ativadas, com capacidade mínima de processamento de 700 (setecentos) Mbps.

**5.30.6.** Inspeção SSL Throughput com capacidade mínima de processamento de 630 (seiscentos e trinta) Mbps.

**5.30.7.** VPN com capacidade de, pelo menos, 6.0 Gbps de tráfego IPSec.

**5.30.8.** Deverá suportar 1.000.000 (um milhão) conexões TCP simultâneas.

**5.30.9.** Deverá suportar, pelo menos, 35.000 (trinta e cinco mil) novas conexões TCP por segundo.

**5.30.10.** Deverá suportar, pelo menos, 200 (duzentos) túneis de VPN Site-Site.

**5.30.11.** Deverá suportar, pelo menos, 500 (quinhentos) túneis de VPN Client-Site.

**5.30.12.** Deverá possuir porta de comunicação serial ou USB para testes e configuração do equipamento.

**5.30.13.** Deverá possuir, pelo menos, 8 (oito) interfaces RJ45.

**5.30.14.** Deverá possuir licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades de proteção avançada durante a vigência contratual.

**5.30.15.** Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 30 (trinta) Pontos de Acesso sem fio.

**5.30.16.** Deverá ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 20 (vinte) equipamentos.

**5.30.17.** Deverá incluir licença para atualização de vacina de antivírus/anti-spyware.

**5.30.18.** Deverá incluir licença de atualização para filtro de conteúdo Web.

**5.30.19.** Deverá incluir licença de atualização do IPS e da lista de aplicações detectadas.

**5.30.20.** Deverá ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.

**5.30.21.** O equipamento deve possuir homologação junto à Anatel.

**5.30.22.** RACK SERVIDOR (02 unidades)

**5.30.22.1.** Profundidade de aproximadamente 1070 mm e largura padrão de 19 polegadas;

**5.30.22.2.** Altura de 42u;

**5.30.22.3.** Com base e pés reguláveis, compensação de desníveis e Rodízios giratórios com travamento;"

**5.30.22.4.** Chassi em aço e pintura eletrostática;

**5.30.22.5.** Capacidade de carga estática de pelo menos 1300kg;

**5.30.22.6.** Trilhos de montagem vertical ajustáveis;

**5.30.22.7.** Porta frontal e traseira perfuradas e com fechaduras com Chave;"

**5.30.22.8.** Porta traseira bipartida.

**5.30.22.9.** Deverá acompanhar:

**5.30.22.10.** 2 (duas) pdu's de no mínimo 16a, com pelo menos 20 (vinte) saídas nbr14136 e 1 (uma) entrada iec c20;

**5.30.22.11.** 2 (dois) cabos de alimentação para pdu com comprimento de 1,8m e capacidade de 16a e entrada nbr 14136 e saída iec c19."

**5.30.23.** NOBREAK 10KVA (2 unidades)

**5.30.23.1.** Montagem em rack 19" nobreak;

**5.30.23.2.** Deve possuir pelo menos 2 células de baterias internas;

**5.30.23.3.** Tipo on line de dupla conversão;

**5.30.23.4.** Saída: potência de saída mínima de 10000va – 10000w;

**5.30.23.5.** Tensão nominal de saída: 230v;

**5.30.23.6.** Eficiência mínima de 92% a plena carga;

**5.30.23.7.** Onda senoidal de saída;

**5.30.23.8.** Entrada: distorção harmônica de entrada (ithd): inferior a 5% a plena carga;

**5.30.23.9.** Tensão nominal de entrada: 230v;

**5.30.23.10.** Frequência de 50/60hz autosetting;

**5.30.23.11.** Bateria: bateria tipo chumbo-ácido livre de manutenção à prova de manutenção;

**5.30.23.12.** Tempo de recarga típico: 2,5horas;

**5.30.23.13.** Comunicação e gerenciamento: porta de interface rj-45, smartslot (1 slot).

**5.30.23.14.** Painel de controle:

**5.30.23.15.** Display de led com barra gráfica para carga e bateria e indicadores de online;

**5.30.23.16.** Troca de bateria;

**5.30.23.17.** Nível de carga e bypass;

**5.30.23.18.** Porta de interface ethernet e software de gerenciamento em web;

**5.30.23.19.** Função snmp, com gerenciamento local e remoto do nobreak via protocolo tc/ip.

**5.30.23.20.** Permite o monitoramento das funções do nobreak;

**5.30.23.21.** Registra ocorrência da rede elétrica e do funcionamento do nobreak com data, hora e tipo de evento;

**5.30.23.22.** Alarmes audiovisuais (sonoro e leds):

**5.30.23.23.** Informam problemas no nobreak como anormalidades na rede elétrica e final do tempo de autonomia;

**5.30.23.24.** Possuir função mute;

**5.30.23.25.** Deverá recarregar automaticamente as baterias, manter as baterias em plena carga;

**5.30.23.26.** Permite ser ligado na ausência de rede elétrica;

**5.30.23.27.** Possuir bypass automatizado e manual;

**5.30.23.28.** Proteção contra surtos e filtragem: filtragem de polos múltiplos de ruídos;

**5.30.23.29.** Passagem do surto de pelo menos 400J;

**5.30.23.30.** Deverá acompanhar:

**5.30.23.31.** Sensor de temperatura com leitura em °c;

**5.30.23.32.** Sensor de umidade relativa do ar;

**5.30.23.33.** Trilhos para montagem em rack 42u.

## 5.31. SERVIÇOS DE IMPLANTAÇÃO:

**5.31.1.** O serviço de implantação de infraestrutura de Data Center envolve o planejamento, design, instalação e configuração de todos os componentes necessários para criar um ambiente de Data Center funcional e eficiente.

**5.31.2.** Planejamento e Design: Avaliação das necessidades de infraestrutura, incluindo requisitos de energia, refrigeração, espaço físico e capacidade de rede, definição dos objetivos de desempenho, disponibilidade e escalabilidade do Data Center. Elaboração de um plano de layout físico e lógico, incluindo a localização de servidores, racks, sistemas de refrigeração, sistemas de energia, cabos e conexões de rede. Visto que a Prefeitura disponibilizará uma sala completa o levantamento e obrigatório no intuito de não haver riscos para implantação da solução como todo.

**5.31.3.** Instalação Física: Preparação do espaço físico do Data Center, este alocado em sala disponibilizada pela CONTRATANTE, incluindo por obrigação da CONTRATADA instalação de racks, gabinetes e outros móveis e equipamentos necessários para abrigar os componentes de TI.

**5.31.4.** Implantação de Equipamentos: Montagem e instalação de servidores, sistemas de armazenamento, switches de rede, roteadores, firewalls e outros dispositivos de hardware que forem necessários para o pleno funcionamento do ambiente incluindo conexão de cabos de rede, fibra óptica, cabos de energia e outros cabos necessários para interconectar os dispositivos e garantir conectividade adequada.

**5.31.5.** Configuração e Teste: Configuração inicial de todos os dispositivos de hardware e software de acordo com as especificações do projeto, realização de testes de funcionalidade, desempenho e segurança, de forma transparente sem interrupções ou paradas, para garantir que todos os sistemas estejam operando corretamente e atendendo aos requisitos.

**5.31.6.** Documentação e Treinamento: Documentação completa de toda a infraestrutura do Data Center, incluindo diagramas de rede, listas de equipamentos, procedimentos de manutenção e políticas de segurança e treinamento para administradores de sistemas e operadores de Data Center sobre como operar, monitorar e manter a infraestrutura de forma eficaz, indicado por corpo técnico da prefeitura.

**5.31.7.** Manutenção e Suporte: Estabelecimento de procedimentos e políticas de manutenção preditiva e preventiva para garantir a disponibilidade contínua e o desempenho otimizado do Data Center estando suporte técnico 24x7 para lidar com problemas de operação, falhas de hardware, atualizações de software e outras questões que possam surgir.

## 6. MODELO DE GESTÃO DO CONTRATO QUE DESCREVE COMO A EXECUÇÃO DO OBJETO SERÁ ACOMPANHADA E FISCALIZADA:

### 6.1. DA METODOLOGIA DE TRABALHO:

**6.1.1.** Reunião de alinhamento:

**6.1.1.1.** Deverá ser realizada até o 1º (primeiro) dia útil após a assinatura do Contrato, na Sede da PREFEITURA DE TRÊS LAGOAS/MS, situado à Avenida Antônio Trajano, nº 30, Centro, Três Lagoas MS, uma reunião de alinhamento, conforme agendamento efetuado pelo Gestor do Contrato, com o objetivo de:

**6.1.1.2.** Indicar formalmente um preposto e gerente de projetos exclusivos aptos a representá-la junto ao CONTRATANTE, que deverá responder pela fiel execução do Contrato.

**6.1.1.3.** Nivelar os entendimentos acerca das condições estabelecidas neste documento e no Contrato, esclarecendo, caso necessário, possíveis dúvidas acerca do objeto.

**6.1.1.4.** Receber o repasse de informações a respeito dos sistemas corporativos do CONTRATANTE.

**6.1.1.5.** Apresentar um número de telefone que possibilite ligações para sua central de suporte técnico bem como a outros meios para fins de abertura, acompanhamento de chamados e resolução de dúvidas sobre os Sistemas.

**6.1.1.6.** Após a reunião de alinhamento deverá ser gerada uma Ata com o resultado da mesma e está deverá ser assinada pelo Gestor do Contrato e pela CONTRATADA.

**6.2. DO PLANO DE IMPLANTAÇÃO:**

**6.2.1.** A CONTRATADA, no prazo de até 5 (cinco) dias úteis, contados a partir do primeiro dia útil após a reunião de alinhamento (Kick-Off), deverá apresentar ao Gestor do Contrato o Plano de Implantação.

**6.2.2.** O Gestor do Contrato deverá fazer análise do Plano de Implantação apresentado pela CONTRATADA, podendo propor alterações e/ou ajustes.

**6.2.3.** Caso haja a necessidade de alterações e/ou ajustes no Plano de Implantação da Solução, a Contratada terá o prazo de até 5 (cinco) dias consecutivos, contados a partir do primeiro dia útil após o recebimento da notificação pelo PREFEITURA DE TRÊS LAGOAS/MS, para reapresentá-lo ao Gestor do Contrato.

**6.2.4.** Após as alterações e ajustes necessários, o Gestor do Contrato aprovará o Plano de Implantação, o qual deverá fazer parte integrante do Contrato.

**6.3. SUPORTE TÉCNICO ESPECIALIZADO E SLA:**

**6.3.1.** Serviço Técnico Especializado

**6.3.1.1.** Os profissionais podem ser dedicados para este contrato estando alocados ou não dentro da estrutura do órgão desde que sigam a seguinte hierarquia de atendimento.

**6.3.1.1.1.** Analistas de Suporte Nível I;

**6.3.1.1.2.** Analistas de Suporte Nível II;

**6.3.1.1.3.** Analistas de Suporte Nível III.

**6.3.1.2.** O papel de cada nível de analista é descrito na relação abaixo:

**6.3.1.2.1.** Analista de Suporte Nível I – Centralização de todos os atendimentos realizando análise baseada no catálogo de serviços para escalonamento dos chamados;

**6.3.1.2.2.** Analista de Suporte Nível II – Atendimento as operações a nível de sistemas operacionais de Data Center, serviços de rede, operação do backup e aplicações existentes da CONTRATANTE;

**6.3.1.2.3.** Analista de Suporte Nível III – Atendimento a soluções de rede e infraestrutura de Data Center, auxílio em problemas técnicos de alto impacto e prioridade, manutenção da infraestrutura física e lógica que suportam as aplicações.

**6.3.1.3.** Organização das atividades:

**6.3.1.3.1.** No momento de instalação dos equipamentos pela CONTRATADA, deverá ser feito a interligação e integração com o ambiente atual;

**6.3.1.3.2.** Este serviço foi dividido em atividades e devem ser cumpridas durante todo o período do contrato de acordo com a definição entre a CONTRATANTE e a CONTRATADA no momento de planejamento.

**6.3.1.4.** Atividade 1 – Instalação e Integração:

**6.3.1.4.1.** Analisar e documentar os serviços, infraestrutura física e lógica atuais da PREFEITURA DE TRÊS LAGOAS/MS de modo que evite qualquer imprevisibilidade no momento da prestação dos serviços pela CONTRATADA;

**6.3.1.4.2.** Planejar e documentar a execução dos serviços a nível detalhado descritos abaixo de forma estratégica em formato passo a passo com cronograma uma vez que serão executados

em sua maioria no momento de produção de modo que evite qualquer imprevisibilidade na prestação dos serviços e gere impacto no ambiente incluindo os procedimentos de Rollback em caso de falha;

**6.3.1.4.3.** Fornecer equipamentos do tipo appliances hiperconvergentes, switches ethernet de ultrabaixa latência 25Gbit Ethernet para rede LAN – Local Área Network, Firewall e Appliance de Backup especificados neste Termo de Referência;

**6.3.1.4.4.** Fornecer licenças de software do tipo VMware vSphere Enterprise Plus, VSAN Enterprise e vCenter Standard para o cluster hiperconvergente especificados neste Termo de Referência;

**6.3.1.4.5.** Fornecer licenças sistemas operacionais como Microsoft Windows Server 2022 ou superior e Red Hat Enterprise Linux com capacidade ilimitada de VMs especificados neste Termo de Referência;

**6.3.1.4.6.** Fornecer licenças do tipo CAL de acesso para serviços Microsoft na quantidade de 2000 usuários especificados neste Termo de Referência;

**6.3.1.4.7.** Fornecer licenças de software de proteção de dado como Software de Backup com a capacidade para proteger todas as VMs criadas durante o período do contrato especificados neste Termo de Referência;

**6.3.1.4.8.** Instalar e atualizar a nova infraestrutura física e lógica no data center seguindo as melhores práticas de segurança, alta disponibilidade, desempenho e monitoramento de acordo com cada fabricante dos equipamentos fornecidos e padronizações de mercado;

**6.3.1.4.9.** Criar cluster de virtualização com o software VMware na infraestrutura nova com as mais recentes atualizações e melhores práticas de segurança, proteção de dados, alta disponibilidade, desempenho e preparado para replicar ao site secundário;

**6.3.1.4.10.** A CONTRATADA deve migrar todos os serviços atuais virtualizados e físicos para a nova plataforma de virtualização

atendendo as métricas levantadas de criticidade, segurança, performance, licenciamento e disponibilidade;

**6.3.1.4.11.** A CONTRATADA deve testar os serviços migrados de forma que seja possível liberar os recursos da infraestrutura antecessora para a desativação e remoção dos equipamentos;

**6.3.1.4.12.** Será responsável pelo bom funcionamento assim como aplicar as melhores práticas da rede de data center com escopo aos switches CORE e Topo de Rack de data center bem como switches de borda especificados neste termo de referência;

**6.3.1.5.** Atividade 2 – Operacionalização dos Sistemas:

**6.3.1.5.1.** Por meio de especialistas em seu quadro de funcionários deverá implementar, gerenciar, manter e realizar manutenções periódicas nos sistemas utilizados pela PREFEITURA DE TRÊS LAGOAS/MS;

**6.3.1.5.2.** Será responsável pelo bom funcionamento assim como aplicar as melhores práticas em sistemas operacionais Microsoft Windows e Linux;

**6.3.1.5.3.** Será responsável pelo bom funcionamento assim como aplicar as melhores práticas em plataformas de aplicações Web de mercado como IIS, Apache, Java, NGINX e outros;

**6.3.1.5.4.** Será responsável pelo bom funcionamento assim como aplicar as melhores práticas em bancos de dados de mercado como MySQL, MariaDB, PostgreSQL, Oracle, SQL Server e outros;

**6.3.1.5.5.** Será responsável pelo bom funcionamento assim como aplicar as melhores práticas em serviços de rede como DNS, DHCP, File Server, Gerenciamento de Usuários, Gerenciamento de Certificados e outros;

**6.3.1.5.6.** Será responsável pelo bom funcionamento assim como aplicar as melhores práticas em serviços de rede para desenvolvimento ágil e micro serviços;

**6.3.1.5.7.** Realizar manutenções periódicas em todas a plataformas assim como as atualizações dos ambientes.

**6.3.1.6.** Atividade 3 – Proteção de Dados:

**6.3.1.6.1.** A CONTRATADA será responsável por definir junto a CONTRATANTE a política de proteção de dados (Backup);

**6.3.1.6.2.** Criar as rotinas de backup;

**6.3.1.6.3.** Monitorar para que sejam cumpridas todas as rotinas;

**6.3.1.6.4.** Realizar testes de recuperação periodicamente em ambiente separado para garantia da salvaguarda;

**6.3.1.6.5.** Executar os processos de restauração de dados quando solicitados pela CONTRATANTE;

**6.3.1.6.6.** Enviar relatórios periódicos da realização do Backup.

**6.3.1.7.** Atividade 4 – Monitoramento:

**6.3.1.7.1.** Criar sistema de monitoramento proativo e/ou reativo para cada um dos componentes da infraestrutura física e lógica que deverá monitorar, alarmar, informar e registrar todo problema vindo da infraestrutura dos sites primário e secundário;

**6.3.1.7.2.** Apresentar através de gráficos em Dashboard o monitoramento dos recursos mais críticos para visualização em TV na sala dos analistas da CONTRATADA;

**6.3.1.7.3.** Sincronizar o horário de todos os componentes da infraestrutura física e lógica através de servidor NTP/SNTP local para que os logs sejam correlatos;

**6.3.1.7.4.** Configurar em cada componente da infraestrutura física e lógica o envio de logs para servidor de logs local e/ou SIEM;

**6.3.1.7.5.** Os alertas deverão ser enviados para e-mail e/ou SMS e/ou mensagem eletrônica dos responsáveis técnicos da CONTRATADA quando em nível de Erro ou Crítico;

**6.3.1.7.6.** Os equipamentos e softwares de missão crítica deverão enviar mensagens de alertas para os dashboards automaticamente em caso de alertas e falhas.

**6.3.2.** Especificação dos Serviços:

**6.3.2.1.** Independentemente do escalamento entre os níveis de suporte sob responsabilidade da CONTRATADA, o chamado deve atender globalmente os tempos máximos estabelecidos para incidentes e requisições de serviço. Os incidentes, requisições e problemas serão

classificados de acordo com os critérios estabelecidos pela Prefeitura, considerando-se impacto, urgência e prioridade:

**6.3.2.1.1.** Urgência: a urgência é determinada pela necessidade da instituição em ter os serviços para aquele usuário ou área restabelecidos, ou as suas solicitações atendidas dentro de um determinado prazo. Usuários ou áreas distintas têm requisitos de urgência distintos, dependendo da sua importância para os serviços prestados pela instituição. A urgência também é determinada pelo aumento da gravidade do incidente com o não atendimento em curto prazo;

**6.3.2.1.2.** Impacto: o impacto reflete o efeito de uma requisição, incidente ou problema sobre o negócio ou ativos de TIC da Prefeitura. A classificação dos incidentes, requisições e problemas quanto ao impacto será determinada pela abrangência do incidente e a quantidade de sistemas ou pessoas afetadas;

**6.3.2.1.3.** Prioridade: a prioridade estabelece a relação de ordem de atendimento dos chamados, nos quais as requisições, incidentes e problemas devem ser resolvidos e atendidos. Ela definirá o prazo para início de atendimento e é um importante balizador do esforço a ser empreendido no atendimento;

**6.3.3.** Critérios para definição da urgência das solicitações:

| ' | **Fatos Determinantes** |
|---|---|
| Crítica | •O equipamento ou o serviço precisa ser restabelecido imediatamente.<br>•O dano ou o impacto causado pela falha aumenta significativamente com o tempo.<br>•A área de atividade ou sistema que o requisitante opera são críticos. |
| Alta | •O equipamento ou o serviço precisa ser restabelecido o mais rápido possível.<br>• Definido para serviços de grande importância. |
| Média | • O equipamento ou o serviço deve ser restabelecido assim que possível. |
| Baixa | • Por necessidade do cliente não há possibilidade de intervenção imediata.<br>• O serviço pode ser agendado para uma data específica, a posteriori. |

**6.3.4.** Critérios para Definição do Impacto das Solicitações:

| Impacto | Fatos Determinantes |
|---|---|
| Crítico | Incidentes ou problemas que causem impacto negativo generalizado, e que prejudiquem a imagem institucional da CONTRATANTE.<br>Qualquer incidente ou problema relativo à indisponibilidade ou mau funcionamento de um ou mais equipamentos, serviços ou sistemas críticos de uso coletivo, tais como: serviços de correio eletrônico, servidor de banco de dados, servidor de aplicação, servidor de domínio, servidor de arquivos, servidor de proxy, etc.<br>Qualquer incidente ou problema cujo não atendimento comprometa os serviços de TIC prestados à comunidade externa.<br>•Incidentes ou problemas que impeçam ou inviabilizem os trabalhos de uma área ou unidade da organização (ex. Gabinete, Diretoria, Coordenação, etc.).<br>• Indisponibilidade em serviços internos não críticos, mas que afetam todos os usuários internos. |
| Alto | A falha impossibilita o trabalho diário de um ou mais usuários (ex. problema em um equipamento ou sistema específico não crítico, falha no funcionamento do acesso à rede em uma sala ou setor, indisponibilidade da estação de trabalho do usuário).<br>• O equipamento ou serviço fornecido está operacional, mas apresenta algumas funções principais, ou partes delas, com erros, provocando assim uma queda na qualidade do trabalho normal. |
| Médio | A falha afeta o trabalho diário de um ou mais usuários.<br>• O equipamento ou serviço de uso coletivo encontra-se operando de modo normal, mas algumas funções secundárias apresentam falhas ou lentidão.<br>• Trata-se de requisição de serviço cujo não atendimento imediato impeça o trabalho principal do usuário. |
| Baixo | O equipamento ou serviço apresenta falha, mas por necessidade do usuário não há possibilidade de intervenção imediata ou de paralisação.<br>• O serviço afetado está operando, mas no modo de contingência.<br>• Trata-se de requisição de serviço que pode ser atendida em algum horário posterior sem que haja prejuízo do desempenho das atividades do usuário.<br>• A solicitação é uma requisição de mudança programada.<br>• O serviço pode ser agendado para uma data específica, a posteriori. |

**6.3.4.1.** Os critérios definidos nos dois itens acima serão balizadores para a categorização dos chamados no ITSM. A partir das definições de '"impacto" e "urgência" de cada solicitação, o sistema deverá estabelecer a prioridade do atendimento. A área de gestão da Prefeitura definirá o impacto associado aos diferentes atendimentos presentes no Catálogo de Serviços, e a urgência das solicitações de cada uma das áreas funcionais ou sistemas afetados pelo incidente. A partir das classificações de impacto e urgência, e do cruzamento destas informações, será determinada a prioridade de cada requisição de serviço, de acordo com a matriz de prioridades abaixo.

**6.3.4.2.** A cada valor de prioridade entre um e cinco está associado um SLA relativo ao tempo de início de atendimento e ao tempo total para a solução.

**6.3.4.3.** Os usuários das Secretarias, dos Gabinetes, do Controle Interno, da Consultoria Jurídica e da Presidência, são considerados usuários especiais.

**6.3.4.4.** O atendimento aos usuários especiais, deverá contar com, no mínimo, um funcionário dedicado exclusivamente à tarefa durante todo o período de funcionamento do órgão.

**6.3.5.** Matriz de Definição da Prioridade no Atendimento, em Função do Impacto e da Urgência:

| | | Matriz de Prioridade | | | |
|---|---|---|---|---|---|
| Urgência | Crítica | 1 | 1 | 1 | 1 |
| | Alta | 3 | 3 | 2 | 1 |
| | Média | 4 | 3 | 3 | 1 |
| | Baixa | 5 | 4 | 3 | 1 |
| | | Baixo | Médio | Alto | Crítico |
| | | Impacto | | | |

**6.3.5.1.** Os prazos para atendimento estão listados na tabela a seguir: Prazos máximos para início de tratamento e para solução de incidentes e requisições:

| Prioridade | Tempo de início do tratamento do chamado | Tempo máximo para a solução do chamado |
|---|---|---|
| 1 | Em até 5 minutos | Em até 3 horas |
| 2 | Em até 5 minutos | Em até 6 horas |
| 3 | Em até 5 minutos | Em até 12 horas |
| 4 | Em até 5 minutos | Em até 24 horas |
| 5 | Em até 5 minutos | Em até 48 horas ou em data posterior programada |

**6.3.5.2.** O rol de serviços que deverá constar no Catálogo de Serviços inicial será definido pela Prefeitura e será de responsabilidade da CONTRATADA implementá-lo no ambiente da Prefeitura. Após a entrega por parte da CONTRATADA, a Prefeitura poderá, a seu critério, sugerir ajustes necessários no catálogo de serviços.

**6.3.5.3.** Quando tratar-se de requisição de serviço que puder ser agendada para data posterior, ela deverá ter o "impacto" e a "urgência"

definidos como "baixos", e deverá ser definida no ITSM uma data para sua execução.

**6.3.5.4.** A fim de criar um limitador do esforço máximo necessário para o cumprimento dos níveis de serviço, as solicitações classificadas como de prioridades "1" e "2" somadas não deverão exceder a 50% (cinquenta por cento) dos chamados do período mensal. Caso os chamados classificados com prioridade "1" e "2" excedam o limite máximo de 50% das solicitações em um determinado mês, não será observado pela Prefeitura o SLA correspondente no que exceder o limite.

**6.3.5.5.** O tempo máximo para solução do chamado (TMS) é o tempo máximo para a resolução do incidente ou atendimento da requisição de serviço contado do momento do início da abertura da solicitação até o fechamento dela no ITSM. Para esse cômputo, o tempo transcorrido em dias e horários não úteis (finais de semana, feriados e horários entre 18h e 07h) será desconsiderado para efeito do cálculo do SLA. Os prazos máximos para início do tratamento e de solução dos incidentes ou requisições, de acordo com o nível de prioridade de atendimento, estão descritos no próximo item.

**6.3.5.6.** O tempo de atendimento de requisições de serviço e resolução de incidentes poderá ser suspenso quando:

**6.3.5.6.1.** A resolução de um incidente depender da atuação de um grupo solucionador que não faça parte das equipes da CONTRATATADA, ou necessite da atuação de outro fornecedor da Prefeitura. Neste caso, a CONTRATADA deve evidenciar, no registro de incidente, que todas as suas atividades de análise, para resolução do incidente, foram executadas e as possibilidades de investigação esgotadas e, relacionar evidências no chamado sobre o acionamento de terceiros realizados;

**6.3.5.6.2.** O atendimento depender de informações complementares do solicitante. Neste caso a CONTRATADA deve registrar e solicitar as informações complementares a ferramenta de registro de chamados;

**6.3.6.** Níveis mínimos de serviços exigidos:

**6.3.6.1.** Foram estabelecidos Níveis Mínimos de Serviço Exigidos para a execução dos serviços contratados. Assim, os resultados serão medidos com base em indicadores, apurados temporalmente e continuamente monitorados, objetivando o cumprimento das metas estabelecidas. Este conceito vincula-se ao novo modelo de contratação de soluções de Tecnologia da Informação e Comunicações, ou seja, os serviços serão remunerados considerando parâmetros de qualidade e entrega efetiva de resultados.

**6.3.6.2.** Para apuração e comprovação da prestação do serviço, a CONTRATADA deverá entregar os relatórios de evidências, devidamente detalhados, de cada um dos níveis de serviços com seus respectivos índices, ocorrências e métricas previstas.

**6.3.6.3.** O atendimento às solicitações de serviço será controlado e mensurado por indicadores extraídos diretamente do ITSM, para efeito de acompanhamento das providências em andamento e do tempo decorrido desde sua abertura.

**6.3.6.4.** A avaliação de especificações funcionais e qualidade dos serviços por meio dos níveis mínimos de serviço exigidos são critérios claros, objetivos e mensuráveis estabelecidos pela Prefeitura com a finalidade de aferir e avaliar fatores relacionados com os serviços contratados, tais como qualidade, desempenho, disponibilidade, custos, abrangência e segurança.

**6.3.6.5.** Em caso de não cumprimento das metas de atendimento, resolução e qualidade, serão aplicados os descontos previstos no item de Abatimentos de acordo como NMA sobre o faturamento e seus subitens.

**6.3.6.6.** Será possível a alterar ou a renegociar os níveis de serviços, desde que essa alteração ou renegociação:

**6.3.6.6.1.** Esteja prevista no edital e no contrato;

**6.3.6.6.2.** Seja tecnicamente justificada;

**6.3.6.7.** Não implique acréscimo ou redução do valor contratual do serviço além dos limites de 25% permitidos pelo art. 125, da Lei 14.133/2021;

**6.3.6.8.** Não configure descaracterização do objeto licitado

**6.3.7.** Descrição dos indicadores de níveis mínimos de serviço (NMS) exigidos:

| ID | Indicadores de níveis de serviço | Fórmula de cálculo | Unidade de medida | Meta exigida |
|---|---|---|---|---|
| NS01 | Índice de ineficácia de resolução | Total de reaberturas de demandas em até 7 dias após a conclusão / Total de demandas concluídas x 100% | % | <= 1 |
| NS02 | Índice de demandas com prioridade 1 resolvidas dentro do prazo | Total de demandas com prioridade 1 resolvidas dentro do prazo / Total de demandas recebidas com prioridade 1 x 100% | % | >= 95 |
| NS03 | Índice de demandas com prioridade 2 resolvidas dentro do prazo | Total de demandas com prioridade 2 resolvidas dentro do prazo / Total de demandas recebidas com prioridade 2 x 100% | % | >= 95 |
| NS04 | Índice de demandas com prioridade 3 resolvidas dentro do prazo | Total de demandas com prioridade 3 resolvidas dentro do prazo / Total de demandas recebidas com prioridade 3 x 100% | % | >= 95 |
| NS05 | Índice de demandas com prioridade 4 resolvidas dentro do prazo | Total de demandas com prioridade 4 resolvidas dentro do prazo / Total de demandas recebidas com prioridade 4 x 100% | % | >= 95 |
| NS06 | Índice de demandas com prioridade 5 resolvidas dentro do prazo | Total de demandas com prioridade 5 resolvidas dentro do prazo / Total de demandas recebidas com prioridade 5 x 100% | % | >= 95 |

**6.3.7.1.** O cálculo dos indicadores de nível de serviço deverá levar em consideração o seguinte:

**6.3.7.2.** As metas devem ser medidas do primeiro ao último dia de cada mês. A meta exigida será apurada no último dia de cada mês e serão consideradas as demandas encerradas durante o mês;

**6.3.7.3.** A meta exigida representa o parâmetro de valor - exato (=), limite máximo (<=) ou limite mínimo (>=) que deve ser alcançado pela CONTRATADA para cada um dos indicadores;

**6.3.7.4.** Os tempos serão contados a partir do 1º contato do cliente (recebimento da solicitação inicial), mesmo quando houver transferência da solicitação entre níveis;

**6.3.7.5.** O termo "Total de demandas recebidas" refere-se aos chamados recebidos e passíveis de solução pela Central de Serviços;

**6.3.7.6.** Os indicadores serão medidos, avaliados e calculados mensalmente, tendo como referência os incidentes e requisições encerrados no mês anterior, considerando as horas úteis de trabalho da Prefeitura de Três Lagoas e o total de dias em cada mês avaliado;

**6.3.7.7.** A abrangência dos indicadores de disponibilidade e a sua forma de cálculo serão definidos pela Prefeitura, e serão aplicados pela CONTRATADA nas ferramentas de monitoramento e de estatísticas de serviço;

**6.3.7.8.** A soma total das glosas aplicadas em função do não atendimento dos níveis mínimos de serviço não deverá ser superior a 30% (trinta por cento) do faturamento mensal máximo;

**6.3.7.9.** Caso fique caracterizado que a indisponibilidade foi provocada por evento alheio à capacidade reativa e proativa da CONTRATADA, esta indisponibilidade não será considerada no cálculo do indicador de serviço;

**6.3.7.10.** As indisponibilidades programadas por mudanças autorizadas não serão computadas nos indicadores;

**6.3.7.11.** No caso dos indicadores de atendimento, não serão computados os tempos em que a solicitação aguarda retorno de informações do solicitante, ou quando não existirem todos os pré-requisitos disponíveis de imediato, como autorizações de responsabilidade da Prefeitura;

**6.3.7.12.** Para inclusão de novos serviços no Catálogo de Serviços cuja classificação de impacto seja "ALTO" ou "CRÍTICO", a Prefeitura concederá um prazo de quinze dias para a CONTRATADA readequar seus procedimentos de execução.

**6.3.7.13.** Caso sejam ativados novos sistemas ou implantadas novas áreas funcionais cuja classificação das atividades tenha urgência considerada "ALTA" ou "CRÍTICA", a Prefeitura concederá um prazo de quinze dias para a CONTRATADA adequar seus procedimentos de execução.

## 6.4. MODELO DE GESTÃO DO CONTRATO

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

**6.4.2.** Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente

pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

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

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

**6.4.5.** Preposto

**6.4.5.1.** A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

**6.4.5.2.** A PREFEITURA DE TRÊS LAGOAS/MS poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a Contratada designará outro para o exercício da atividade

**6.4.5.3.** O preposto atuará como ponto de contato principal entre a CONTRATADA e o PREFEITURA DE TRÊS LAGOAS/MS e será responsável por receber, comunicar e tomar as devidas providências em relação a todas as questões contratuais.

**6.4.5.4.** Qualquer alteração no preposto designado pela CONTRATADA deve ser comunicado por escrito ao PREFEITURA DE TRÊS LAGOAS/MS, e a CONTRATADA deve nomear um novo preposto dentro de 2 dias.

**6.4.5.5.** A CONTRATADA deve garantir que seu preposto seja plenamente informado sobre as obrigações contratuais, normas e regulamentos aplicáveis, bem como as políticas e procedimentos da instituição.

**6.4.6.** Reunião Inicial

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

**6.4.6.2.** A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em 1 (um) dia útil da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

**6.4.6.3.** A pauta desta reunião observará, pelo menos:

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

**6.4.6.5.** Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

**6.4.6.6.** Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

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

**6.4.6.8.** Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

**6.4.6.9.** A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput), nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

**6.4.6.10.** O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

**6.4.6.11.** O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização

das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º, e Decreto nº 11.246, de 2022, art. 22, II);

**6.4.6.12.** Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

**6.4.6.13.** O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV).

**6.4.6.14.** No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V).

**6.4.6.15.** O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

**6.4.7.** Fiscalização Administrativa

**6.4.7.1.** O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação do contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

**6.4.7.2.** Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

**6.4.8.** Gestor do Contrato

**6.4.8.1.** O gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).

**6.4.8.2.** O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

**6.4.8.3.** O gestor do contrato acompanhará a manutenção das condições de habilitação do contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

**6.4.8.4.** O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

**6.4.8.5.** O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

**6.4.8.6.** O gestor do contrato deverá elaborará relatório final com informações sobre a consecução dos objetivos que tenham justificado

a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

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

## 7. CRITÉRIO DE MEDIÇÃO E DE PAGAMENTO:

### 7.1. RECEBIMENTO DO OBJETO

**7.1.1.** Relatórios de Acompanhamento

**7.1.1.1.** Os relatórios de acompanhamento de serviços devem ser elaborados periodicamente pela equipe de fiscalização do contrato com vistas a subsidiar o gestor do contrato na apuração do valor mensal da contratação a ser autorizado para fins de pagamento.

**7.1.1.2.** Esse instrumento de controle deve possuir no mínimo a apuração dos indicadores de níveis de serviços, ocorrências e demais informações necessárias à correta identificação do valor mensal a ser pago referente à execução das Ordens de Serviços.

**7.1.1.3.** Logo, configuram-se em ferramentas imprescindíveis para fiscalização e gestão do contrato, proporcionando ainda a técnicos e gestores o acesso a informações e estatísticas importantes para tomadas de decisões acerca do desempenho da área de TI como um todo.

**7.1.1.4.** A produção desse relatório deve se basear em informações extraídas de ferramentas e softwares sob a gestão da contratante e ou contratada, não devendo se basear exclusivamente em informações fornecidas pela contratada.

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

**7.1.3.** Os serviços poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de **5 dias corridos,** a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

**7.1.4.** O recebimento definitivo ocorrerá no prazo de **5 dias corridos**, a contar do recebimento da nota fiscal ou instrumento equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

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

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

**7.1.7.** O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

**7.2. DO PAGAMENTO**

**7.2.1.** O pagamento será efetuado de acordo com o fornecimento, no prazo de até 30 (trinta) dias mediante apresentação da Nota Fiscal ou documento equivalente, devidamente atestada, juntamente das certidões de regularidade fiscal em plena validade, previstas na Lei 14.133/2021.

**7.2.2.** A Contratada deverá obrigatoriamente encaminhar os seguintes documentos quando da entrega:

**7.2.2.1.** Nota Fiscal ou documento equivalente gerada de acordo com o fornecimento das quantidades de serviços entregues e solicitados na Autorização de Fornecimento/Ordem de Serviço;

**7.2.2.2.** Prova de regularidade para com a Fazenda Federal, Estadual e/ou Municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei;

**7.2.2.3.** Prova de regularidade relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;

**7.2.2.4.** Prova de regularidade perante a Justiça do Trabalho;

**7.2.3.** A falta de um dos documentos dispostos na Lei Federal nº 14.133/2021 e suas alterações, poderá implicar no não recebimento.

**7.3. SANÇÕES:**

**7.3.1.** Do Nível Mínimo de Serviço (NMS):

**7.3.1.1.** Termos de Serviço a serem observados pela CONTRATADA e Sanções Aplicáveis.

**7.3.1.2.** Tabela de pontuação para glosas referente à Central de Serviços:

| ID | Termo de Serviço | Referência | Pontuação |
|---|---|---|---|
| TS01 | Permitir a presença de profissional sem crachá. | Por ocorrência | 1 |
| TS02 | Manter profissionais sem formalização ou sem a qualificação exigida para executar os serviços contratados. | Por dia, para cada profissional | 1 |
| TS03 | Deixar de apresentar os relatórios consolidados para a fiscalização contratual, conforme exigências do Termo de Referência, dentro do prazo definido de cinco dias úteis. | Por dia de atraso | 1 |
| TS04 | Deixar de analisar a viabilidade e o impacto da instalação de novas soluções e correções. | Por ocorrência | 1 |
| TS05 | Deixar de aplicar as políticas de controle de acesso e de gestão da identidade de usuários de TIC. | Por ocorrência | 1 |
| TS06 | Deixar de realizar os testes e análises de vulnerabilidades e potenciais falhas de segurança, conforme política de segurança da informação. | Por ocorrência | 1 |
| TS07 | Deixar de participar, quando solicitado, de reunião com a equipe de gestão de TIC da CONTRATANTE. | Por ocorrência | 1 |
| TS08 | Registro de incidente de indisponibilidade de serviços sendo monitorados por usuário sem o devido registro anterior do ticket por ferramenta de monitoração. | Por ocorrência | 1 |
| TS09 | Suspender ou interromper, salvo por motivo de força maior ou caso fortuito, os serviços solicitados. | Por ocorrência | 3 |
| TS10 | Finalizar a requisição de serviço ou incidente sem a anuência do solicitante, sem que o incidente tenha sido solucionado, ou deixar de realizar os testes para aferir a efetiva resolução. | Por ocorrência | 3 |
| TS11 | Alocar profissional sem capacidade técnica necessária ao pleno atendimento do objeto contratado ou sem atender às qualificações exigidas | Por ocorrência | 3 |

| ID | Termo de Serviço | Referência | Pontuação |
|---|---|---|---|
| | no contrato, ainda que em casos de substituição temporária. | | |
| TS12 | Recusar-se a executar serviço relacionado ao objeto do contrato, determinado pela fiscalização, por serviço. | Por ocorrência | 3 |
| TS13 | Deixar de zelar pela organização, acomodação e correta identificação dos cabos nos racks de equipamentos e patch panels, ou não cuidar da correta montagem e conservação dos equipamentos do data center e demais unidades de prestação de serviços. | Por ocorrência | 3 |
| TS14 | Utilizar indevidamente os recursos de TIC (acessos indevidos, utilização para fins particulares, etc.), salvo em situação excepcional e devidamente autorizado pela CONTRATANTE. | Por ocorrência | 3 |
| TS15 | Deixar de comunicar a CONTRATANTE, com antecedência de cinco dias úteis, a substituição de profissionais. | Por ocorrência | 3 |
| TS16 | Deixar de executar as cópias de segurança (backups) dos elementos críticos da infraestrutura da CONTRATANTE, de acordo com as políticas estabelecidas. | Por ocorrência | 3 |
| TS17 | Deixar de atualizar as políticas de backup, ou de incluir novos serviços críticos nas rotinas. | Por ocorrência | 3 |
| TS18 | Deixar de cumprir ou de implementar as rotinas em conformidade com a Política de Segurança e o Plano de Continuidade de Negócios de TIC. | Por ocorrência | 3 |
| TS19 | Deixar de planejar e instalar nos equipamentos e sistemas as atualizações e patches de segurança disponibilizados pelos fabricantes e distribuidores. | Por ocorrência | 3 |
| TS20 | Deixar de apresentar relatórios, levantamentos e inventários conforme solicitado. | Por ocorrência | 3 |
| TS21 | Deixar de documentar os incidentes e de manter completa e atualizada a Base de Dados de Configuração, inclusive no que diz respeito aos diagramas e desenhos. | Por ocorrência | 3 |
| TS22 | Deixar de produzir ou de manter atualizadas as rotinas e scripts da Base de Dados de Conhecimentos | Por ocorrência | 3 |
| TS23 | Deixar de notificar à área competente os incidentes repetitivos, quer tenham sido conhecidos por meio do monitoramento ou por notificações de usuários. | Por ocorrência | 3 |
| TS24 | Deixar de realizar o controle e a programação de processo de mudança, e a avaliação de impacto, ou realizá-los deforma deficiente ou incompleta. | Por ocorrência | 3 |
| TS25 | Deixar de comunicar a realização de mudança programada que poderá gerar indisponibilidade em sistemas ou serviços. | Por ocorrência | 3 |
| TS26 | Deixar de retirar profissional que se conduza de modo inconveniente, que não respeite as normas da STI ou que não atenda às necessidades em período de 24 horas corridas a contar da notificação da CONTRATANTE. | Por dia para cada profissional | 3 |

| ID | Termo de Serviço | Referência | Pontuação |
|---|---|---|---|
| TS27 | Deixar de documentar todas as ocorrências (incidentes, requisições, mudanças, problemas, indisponibilidades) na Ferramenta de Requisição de Serviço e Gerenciamento de TIC. | Por ocorrência | 3 |
| TS28 | Deixar de operar e monitorar proativamente o ambiente de TIC, e de atuar tempestivamente no caso de incidentes graves. | Por ocorrência | 5 |
| TS29 | Deixar de registrar solicitação para necessidade de atualização de software sob sua administração no prazo de 15(quinze) dias úteis contados da disponibilização pelo fabricante. | Por ocorrência | 5 |
| TS30 | Descumprimento de cronograma de backup | Por ocorrência | 5 |
| TS31 | Documentação da rede de dados desatualizada. | Por ocorrência | 5 |
| TS32 | Deixar de implementar scripts de monitoração nos prazos acordados. | Por ocorrência | 5 |
| TS33 | Deixar de cumprir o prazo para apresentação de proposta técnica. | Por ocorrência | 7 |
| TS34 | Permitir que violações de segurança afetem ou causem indisponibilidade dos sistemas da CONTRATANTE, sem aplicar as contramedidas necessárias. | Por ocorrência | 7 |
| TS35 | Incluir, excluir ou alterar regras dos dispositivos de segurança sem autorização da unidade responsável, ou contrariando as políticas de segurança da CONTRATANTE. | Por ocorrência | 12 |
| TS36 | Deixar de zelar pelas máquinas, equipamentos e instalações da CONTRATANTE utilizados pela CONTRATADA. | Por ocorrência | 12 |
| TS37 | Deixar de cumprir quaisquer obrigações estabelecidas no edital, não previstas nesta tabela, após reincidência formalmente notificada pela STI. | Por ocorrência | 12 |
| TS38 | Instalar qualquer software, programas, aplicativos, sistemas operacionais não licenciados (prática conhecida como pirataria de software) salvo softwares livres desde que tenha anuência da CONTRATANTE. | Por ocorrência | 12 |
| TS39 | Reincidência de falhas de segurança | Por ocorrência | 12 |
| TS40 | Causar qualquer indisponibilidade dos serviços da CONTRATANTE por motivo de imperícia na execução das atividades contratuais. | Por ocorrência | 12 |
| TS41 | Causar qualquer dano aos equipamentos da CONTRATANTE por motivo de imperícia na execução das atividades contratuais. | Por ocorrência | 12 |
| TS42 | Interromper unilateralmente a prestação de serviços sem que haja evento de força maior que o justifique. | Por dia de interrupção | 24 |
| TS43 | Perder dados ou informações corporativas por erros na operação ou inobservância dos requisitos da política de backup | Por ocorrência | 24 |
| TS44 | Fraudar, manipular ou descaracterizar indicadores/metas de níveis de serviço por quaisquer subterfúgios. | Por ocorrência de indicador manipulado | 24 |

**7.3.1.3.** Não serão permitidas ocorrências para o TS44 sem a abertura de processo administrativo para apuração de responsabilidade da CONTRATADA, além da aplicação da respectiva glosa.

**7.3.1.4.** Tabela de pontuação para glosas aplicável à Central de Serviços:

| Descrição | Referência | Pontos |
|---|---|---|
| Não atingir o índice aceitável do indicador NS1 | Por ocorrência que exceder o índice aceitável | 3 |
| Não atingir o índice aceitável do indicador NS2 | Por ocorrência que exceder o índice aceitável | 10 |
| Não atingir o índice aceitável do indicador NS3 | Por ocorrência que exceder o índice aceitável | 7 |
| Não atingir o índice aceitável do indicador NS4 | Por ocorrência que exceder o índice aceitável | 4 |
| Não atingir o índice aceitável do indicador NS5 | Por ocorrência que exceder o índice aceitável | 3 |
| Não atingir o índice aceitável do indicador NS6 | Por ocorrência que exceder o índice aceitável | 2 |

**7.3.2.** Abatimentos de acordo com o NMA sobre o faturamento:

| NMA | Abatimento |
|---|---|
| Maior ou igual a 97,5 | 0% |
| Maior ou igual a 95,0 e menor que 97,5 | 0% e notificação à CONTRATADA |
| Maior ou igual a 92,5 e menor que 95,0 | 1% |
| Maior ou igual a 90,0 e menor que 92,5 | 2% |
| Maior ou igual a 85,0 e menor que 90,0 | 4% |
| Maior ou igual a 80,0 e menor que 85,0 | 6% |
| Maior ou igual a 70,0 e menor que 80,0 | 8% |
| Maior ou igual a 60,0 e menor que 70,0 | 10% |
| Maior ou igual a 50,0 e menor que 60,0 | 15% |
| Maior ou igual a 40,0 e menor que 50,0 | 20% |
| Maior ou igual a 30,0 e menor que 40,0 | 25% |
| Maior ou igual a 0 e menor que 30,0 | 30% |

**7.3.2.1.** Após o fim do terceiro mês do início do contrato, caso a CONTRATADA apresente por duas vezes consecutivas a NMA menor que 95,00 ocorrerá o abatimento de 5% na fatura mensal, cumulativamente ao abatimento previsto na tabela acima.

**7.3.2.2.** Após o fim do terceiro mês do início do contrato, caso a CONTRATADA apresente por três vezes consecutivas a NMA menor que 80,00 será considerado inadimplemento GRAVE e aberto processo de apuração de responsabilidade para aplicação das sanções cabíveis.

**7.3.2.3.** Após o fim do terceiro mês do início do contrato, a obtenção de NMA menor ou igual a 30 (trinta) pontos, por duas vezes a cada quatro meses de execução contratual, ou ainda por cinco vezes no período completo da sua vigência caracteriza-se como inexecução contratual, ensejando a sua rescisão.

**7.3.3.** Definição de Critérios de priorização

**7.3.3.1.** Os incidentes e requisições serão classificados de acordo com os critérios estabelecidos pelo órgão.

**7.3.3.2.** É exemplo de critérios a serem adotados a criticidade, que mensura a relevância de determinado recurso (link de internet, servidores de rede, switches, sistemas, etc.) ou aplicação para o correto andamento do negócio, e a disponibilidade, que qualifica a situação do recurso ou aplicação de TIC que gerou a motivação para o chamado (a ser definido pelo atendente de primeiro nível quando da abertura do chamado), conforme diretrizes abaixo:

**7.3.3.3.** A classificação dos serviços é parte integrante do Catálogo de Serviços. Os critérios definidos acima são balizadores para a categorização dos chamados no Sistema de Gerenciamento de Chamados e de Níveis de Serviços de TIC.

**7.3.3.4.** A partir das definições de "Urgência" e "Impacto" de cada solicitação, o sistema deverá estabelecer a prioridade do atendimento, caracterizada pela sua severidade. A área de gestão do órgão definirá o impacto associado aos diferentes atendimentos presentes no catálogo de serviços, e a consequente criticidade das solicitações de cada uma das áreas funcionais ou sistemas afetados pelo incidente.

**7.3.3.5.** O atendente de primeiro nível ou um operador responsável da Central de Atendimento deverá classificar a disponibilidade para cada chamado recebido.

**7.3.3.6.** A partir do cruzamento destas informações, será determinada a prioridade de cada requisição de serviço, de acordo com a matriz de severidade, caracterizando o seu NMS específico, em termos do tempo máximo de atendimento aceitável. Isto é, a cada valor de severidade estão associados níveis de serviços mínimos relativos ao tempo de início

de atendimento e ao tempo total para a solução, para cada categoria de serviços.

**7.3.4.** Critérios de aceitação de serviços

**7.3.4.1.** Os critérios de aceitação estão associados a indicadores mínimos de serviço relacionados à não aceitação dos serviços, também chamado de indicador de desvio de qualidade.

### 7.4. MECANISMOS DE CONTROLE E ACOMPANHAMENTO

**7.4.1.** Por se tratar de contratação por pagamento fixo mensal, vinculada ao atendimento de níveis mínimos de serviços, e não se configurar como contratação com dedicação exclusiva de mão de obra, contratação por homem/hora e tampouco por postos de trabalho, durante a fase de execução do contrato:

**7.4.2.** Não é permitido exigir da CONTRATADA, na planilha de custos e formação de preços, a quantidade mínima, perfis ou base salarial dos profissionais envolvidos na prestação do serviço;

**7.4.3.** A fiscalização do contrato não poderá envolver análise de planilha de custos e formação de preços, incluindo a quantidade mínima, os perfis ou a base salarial dos profissionais envolvidos na prestação do serviço;

**7.4.4.** A contratada possui total gestão sobre a equipe do contrato, podendo realizar alterações na composição das equipes que prestam o serviço, incluindo quantidade e bases salariais dos profissionais envolvidos na prestação do serviço, bem como decidir sobre a alocação destes profissionais entre atividades e múltiplos contratos;

**7.4.5.** Deverá ser observada a vinculação aos resultados pretendidos por meio exclusivamente do atendimento aos Níveis Mínimos de Serviço previamente estabelecidos, sendo vedado a distribuição, controle e supervisão dos recursos humanos, a exemplo de quantidade de perfis, jornada, frequência ou outros critérios relacionados à alocação de mão de obra.

## 8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR:

### 8.1. FORMA DE SELEÇÃO E CRITÉRIO DE JULGAMENTO DA PROPOSTA:

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

**8.2. EXIGÊNCIAS DE HABILITAÇÃO:**

**8.2.1.** Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

**8.2.2.** Habilitação jurídica

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

**8.2.2.2.** Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

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

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

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

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

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

**8.2.2.8.** Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

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

**8.2.3.** Habilitação fiscal, social e trabalhista

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

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

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

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

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

**8.2.3.6.** Prova de regularidade com a Fazenda Municipal/Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

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

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

**8.2.4.** Qualificação Econômico-Financeira

**8.2.4.1.** Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea "c", da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;

**8.2.4.2.** Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

**8.2.4.3.** Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:

**8.2.4.4.** índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);

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

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

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

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

**8.2.4.9.** As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

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

**8.2.4.11.** Caso admitida a participação de cooperativas, será exigida a seguinte documentação complementar:

**8.2.4.12.** A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971;

**8.2.4.13.** A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

**8.2.4.14.** A comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço;

**8.2.4.15.** O registro previsto na Lei n. 5.764, de 1971, art. 107;

**8.2.4.16.** A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato;

**8.2.4.17.** Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa: a) ata de fundação; b) estatuto social com a ata da assembleia que o aprovou; c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia; d) editais de convocação das três últimas assembleias gerais extraordinárias; e) três registros de presença dos cooperados que executarão o contrato em assembleias

gerais ou nas reuniões seccionais; e f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;

**8.2.4.18.** A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

**8.2.5.** Qualificação mínima necessária da empresa e dos profissionais:

**8.2.5.1.** As qualificações e requisitos mínimos de experiência exigidas dos profissionais que deverão ser disponibilizadas pela CONTRATADA para executar as atividades objetos desta contratação são detalhados abaixo:

**8.2.5.1.1.** A licitante deverá apresentar certidão de inscrição da empresa licitante e do(s) responsável(eis) técnico(s) junto ao Conselho Regional de Engenharia e Agronomia (CREA). E deve possuir como responsável técnico da empresa pelo menos 01 (um) Engenheiro Eletricista, ou Técnico em Telecomunicação ou Tecnólogo em Rede de Computadores. No caso de certidão emitida por outra Unidade da Federação, deverá ser apresentada com o visto do CREA-MS, por ocasião da contratação.

**8.2.5.1.2.** Todos os profissionais envolvidos na execução dos serviços deverão possuir qualificação e experiência comprovadas, compatíveis com as funções a serem desempenhadas.

**8.2.5.2.** A comprovação do vínculo se fará com a apresentação de cópia de um dos seguintes documentos:

**8.2.5.2.1.** Carteira de Trabalho (CTPS), devendo ser apresentada apenas as folhas de identificação em que consta a fotografia, a de qualificação, a do último contrato de trabalho celebrado com a empresa Licitante e a página seguinte em branco, e as folhas de últimas anotações gerais e página seguinte em branco;

**8.2.5.2.2.** Certidão de registro da Pessoa Jurídica junto CREA, onde conste o profissional como integrante do quadro de responsável técnico;

**8.2.5.2.3.** Contrato Social ou equivalente, para o caso de sócios;

**8.2.5.2.4.** Contrato de Prestação de Serviços, com firmas reconhecidas de todos os pactuantes;

**8.2.5.2.5.** Contrato de Trabalho, com firmas reconhecidas de todos os pactuantes.

**8.2.5.3.** A licitante deverá adicionar às demais documentações licitatórias obrigatórias para a participação deste certame, atestado(s) de capacidade técnica expedida(s) por entidade/órgão público ou empresa privada comprovando aptidão técnica no Serviço de Outsourcing de servidores, equipamentos de armazenamento de dados (*storages*), equipamentos de rede (*switch*), appliance de backup em disco, hiperconvergência, experiencia em implantação e operação de solução de centro de operações de rede e central de serviços de TI com fornecimento equipamento, *software* e pessoas para atendimento 24x7 das atividades da Contratante pelo mínimo de 36 meses;

**8.2.5.3.1.** A comprovação da efetividade do vínculo trabalhista dos profissionais indicados com seus respectivos currículos deverá ser feita mediante cópia da carteira de trabalho CTPS, Contrato Social, Ficha de Registro de Empregados ou contrato de prestação de serviços.

**8.2.5.3.2.** A documentação (manuais/datasheet) de todos os equipamentos ofertados deve acompanhar a proposta da empresa;

**8.2.6.** Outros documentos:

**8.2.6.1.** Atestado de Vistoria emitido pelo PREFEITURA DE TRÊS LAGOAS/MS, ou, caso optar pela não realização da vistoria, Declaração formal que possui conhecimento pleno das condições e peculiaridades da contratação, responsabilizando-se por quaisquer ônus.

**8.2.6.2.** Declaração de que o licitante possui ou instalará escritório na cidade de Três Lagoas/MS, a ser comprovado no prazo máximo de 60 (sessenta) dias contado a partir da vigência do contrato.

## 9. ESTIMATIVA DO VALOR DA CONTRATRAÇÃO:

**9.1.** O custo estimado da contratação possui caráter sigiloso e será tornado público apenas e imediatamente após o julgamento das propostas.

**9.1.1.** A administração opta por não divulgar os valores referenciais. O sigilo do valor de referência é um auxiliar útil à Administração na busca pela proposta mais vantajosa, visto que, a depender da concorrência existente em razão do objeto, eventual divulgação poderia fazer o licitante se restringir a obedecer ao limite estabelecido, afastando eventual negociação efetivamente proveitosa. Assim, a ânsia em maximizar a obtenção de oferta mais proveitosa justifica, por si só, que a informação quede restrita aos autos do processo administrativo, em anexo complementar, conforme possibilita o art. 24 da Lei 14.133/2021.

**9.1.2.** Destarte, a divulgação do orçamento pode comprometer uma das finalidades do procedimento licitatório, a seleção da proposta mais vantajosa, de modo que a avaliação dos princípios administrativos incutidos no certame de faça necessária, em especial quando de eventual requerimento de divulgação.

## 10. ADEQUAÇÃO ORÇAMENTÁRIA:

**10.1.** As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral do Município deste exercício, na dotação abaixo discriminada:

**Secretaria Municipal de Governo e Políticas Públicas**

**Dotação:** 04.01.04.126.0004.2067

**Fonte:** 1.500.0000

**Ficha:** 101

**Centro de Custo:** 3.3.90.39

## 11. OUTRAS INFORMAÇÕES RELEVANTES:

**11.1.** Aspectos Legais e Regulatórios:

**11.1.1.** Conformidade com a Lei nº 14.133, de 2021 (Nova Lei de Licitações);

**11.1.2.** Atendimento às disposições da Lei Geral de Proteção de Dados (LGPD) 13.709/2018;

**11.1.3.** Homologação dos equipamentos junto à Agência Nacional de Telecomunicações (Anatel);

**11.1.4.** Cumprimento das normas de segurança da informação.

**11.2.** Sustentabilidade e Responsabilidade Social:

**11.2.1.** Observância de práticas sustentáveis na execução dos serviços;

**11.2.2.** Cumprimento de normas ambientais aplicáveis;

**11.2.3.** Responsabilidade social corporativa;

**11.2.4.** Práticas de governança corporativa.

**11.3.** Transferência de Conhecimento:

**11.3.1.** Obrigatoriedade de transferência de conhecimento para a equipe técnica da Prefeitura;

**11.3.2.** Documentação completa dos procedimentos e configurações;

**11.3.3.** Treinamento adequado para operação e manutenção básica;

**11.3.4.** Criação de base de conhecimento para suporte interno.

**11.4.** Continuidade dos Serviços:

**11.4.1.** Garantia de continuidade dos serviços durante todo o período contratual;

**11.4.2.** Plano de contingência para situações de emergência;

**11.4.3.** Backup e recuperação de dados;

**11.4.4.** Alta disponibilidade dos sistemas críticos.

**11.5.** Evolução Tecnológica:

**11.5.1.** Possibilidade de incorporação de novas tecnologias durante a vigência do contrato;

**11.5.2.** Atualizações de software e firmware;

**11.5.3.** Adaptação a novas necessidades da Prefeitura;

**11.5.4.** Escalabilidade da solução.

**11.6.** Segurança da Informação:

**11.6.1.** Implementação de políticas de segurança rigorosas;

**11.6.2.** Monitoramento contínuo de ameaças;

**11.6.3.** Resposta rápida a incidentes de segurança;

**11.6.4.** Conformidade com padrões internacionais de segurança.

**11.7.** Gestão de Riscos:

**11.7.1.** Identificação e mitigação de riscos operacionais;

**11.7.2.** Planos de contingência para diferentes cenários;

**11.7.3.** Seguro de responsabilidade civil;

**11.7.4.** Garantias contratuais adequadas.

**11.8.** Relacionamento Contratual:

**11.8.1.** Estabelecimento de canais de comunicação eficientes;

**11.8.2.** Reuniões periódicas de acompanhamento.

**11.8.3.** Relatórios de desempenho regulares.

**11.8.4.** Processo estruturado de resolução de conflitos.

Três Lagoas/MS, na data da assinatura digital.

| EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO | | |
|---|---|---|
| **NOME** | **CARGO** | **ASSINATURA** |
| **Anderson de Moraes Lopes** | **Diretor de Tecnologia da Informação** | gov.br Documento assinado digitalmente<br>ANDERSON DE MORAES LOPES<br>Data: 11/02/2026 17:08:16-0300<br>Verifique em https://validar.iti.gov.br |
| **Fagner Moreira Leal** | **Diretor de Departamento** | gov.br Documento assinado digitalmente<br>FAGNER MOREIRA LEAL<br>Data: 11/02/2026 17:10:43-0300<br>Verifique em https://validar.iti.gov.br |

Aprovador por:
(assinado digitalmente)
**ANDRÉ LUIS BACALÁ RIBEIRO**
Secretário Municipal de Governo e Políticas Públicas