TERMO DE REFERÊNCIA Nº 102/ 2026.

Processo Administrativo nº. PMC/ 16224/2009

Órgão responsável: Secretaria Municipal de Administração.

1. DO OBJETO

1.1. Dispensa por emergência para contratação de empresa especializada para a prestação de serviço de suporte técnico especialista em Microsoft Office365 e Microsoft Windows Server ADM Active Directory e solução integrada de segurança que possibilite a visibilidade e controle de tráfego, filtragem de conteúdo web, filtro de dados, VPN, servidores web dedicado na nuvem para hospedagem do site e solução de rede wireless como serviço gerenciado e controlador na nuvem, durante o período de 12 (doze) meses, conforme especificações e condições estabelecidas neste edital ou até a conclusão do processo licitatório em andamento.

1.2. Os serviços são classificados como comuns, uma vez que, os padrões de desempenho e qualidade podem ser objetivamente definidos pelo Documento de Oficialização de Demanda.

1.3. A presente contratação encontra respaldo institucional, conforme previsão no item 31, do Plano de Contratações Anual de 2026, estando alinhado com o Planejamento da Administração.

1.4. O presente Termo de Referência tem como base legal a Lei Federal nº. 14.133/2021.

2. DOS FUNDAMENTOS DA CONTRATAÇÃO

2.1. Trata-se de dispensa de licitação realizada sob a obediência ao estabelecido no inciso VIII, do art. 75, da Lei n. 14.133/2021, onde se verifica ocasião em que a mesma é cabível conforme abaixo:

> ***Art. 75*** *- É dispensável a licitação:*
>
> *[...]*
>
> ***VIII*** *- nos casos de emergência ou de calamidade pública, quando caracterizada urgência de atendimento de situação que possa ocasionar prejuízo ou comprometer a continuidade dos serviços públicos ou a segurança de pessoas, obras, serviços, equipamentos e outros bens, públicos ou particulares, e somente para aquisição dos bens necessários ao atendimento da situação emergencial ou calamitosa e para as parcelas de obras e serviços que possam ser concluídas no prazo máximo de 1 (um) ano, contado da data de ocorrência da emergência ou da calamidade, vedadas a prorrogação dos respectivos contratos e a recontratação de empresa já contratada com base no disposto neste inciso.*

2.2. A gestão eficiente da infraestrutura tecnológica das Secretarias Municipais é essencial para garantir a continuidade dos serviços públicos e a proteção das informações institucionais. Nesse cenário, a implementação de uma solução de segurança baseada em Appliance Next Generation Firewall (NGFW) é fundamental para assegurar a integridade, confidencialidade e disponibilidade dos dados, bem como a proteção contra ameaças cibernéticas cada vez mais sofisticadas.

2.3. **Atendimento à Lei 14.133/2021:**

2.3.1. A nova legislação de licitações e contratos estabelece princípios voltados à eficiência, segurança e governança nas contratações públicas. A aquisição de solução de segurança NGFW por meio de pregão eletrônico está alinhada a esses princípios, garantindo a mitigação de riscos operacionais e a proteção dos ativos de informação do município.

2.4. **Proteção da Infraestrutura Tecnológica:**

2.4.1. A solução NGFW oferece funcionalidades avançadas como inspeção profunda de pacotes (DPI), prevenção contra intrusões (IPS), controle de aplicações, filtragem de conteúdo web, proteção contra malware e ameaças avançadas (APT), além de VPN segura. Tais recursos são essenciais para proteger a rede corporativa contra ataques externos e internos.

2.5. **Garantia de Disponibilidade dos Serviços:**

2.5.1. A indisponibilidade de sistemas críticos pode impactar diretamente o atendimento ao cidadão. O NGFW contribui para a alta disponibilidade da rede, prevenindo incidentes de segurança que possam causar interrupções nos serviços públicos digitais.

2.6. **Transparência e Conformidade com a LGPD:**

2.6.1. A implementação de mecanismos robustos de segurança da informação está diretamente relacionada ao cumprimento da Lei Geral de Proteção de Dados (LGPD). O NGFW permite controle e auditoria de tráfego, garantindo rastreabilidade e proteção de dados pessoais tratados pela administração pública.

2.7. **Melhoria na Gestão de Riscos:**

2.7.1. Com visibilidade completa do tráfego de rede e capacidade de resposta automatizada a incidentes, os gestores de TI passam a ter maior controle sobre os riscos cibernéticos, permitindo decisões mais assertivas e baseadas em evidências.

2.8. **Adaptação às Necessidades Locais:**

2.8.1. A solução NGFW pode ser configurada conforme as necessidades específicas do ambiente municipal, considerando o porte da rede, os sistemas utilizados e os níveis de criticidade dos serviços.

2.9. **Padronização da Segurança da Informação:**

2.9.1. A adoção de uma solução padronizada de segurança em todas as unidades administrativas, autarquias e demais órgãos municipais fortalece a governança de TI, garantindo uniformidade nas políticas de segurança, controle centralizado e maior eficiência operacional.

2.10. **Coerência com Diretrizes Nacionais e Boas Práticas:**

2.10.1. A implementação de soluções de segurança da informação está alinhada às boas práticas recomendadas por frameworks como ISO 27001, NIST e diretrizes de governo digital, demonstrando o comprometimento do município com a proteção de seus ativos digitais.

2.11. **Eficiência Operacional e Redução de Custos:**

2.11.1. A centralização da segurança em uma solução NGFW reduz a necessidade de múltiplas ferramentas isoladas, diminuindo custos com licenciamento, suporte e gestão operacional, além de simplificar a administração do ambiente.

2.12. **Facilitação da Auditoria e Monitoramento:**

2.12.1. A solução permite geração de relatórios detalhados sobre eventos de segurança, acessos e incidentes, facilitando auditorias internas e externas, bem como o atendimento aos órgãos de controle.

2.13. **Modernização da Infraestrutura de TIC:**

2.13.1. A adoção de tecnologias avançadas de segurança posiciona o município de forma estratégica frente aos desafios atuais de cibersegurança, garantindo maior resiliência digital.

2.14. **Agilidade na Resposta a Incidentes:**

2.14.1. Agilidade na Resposta a Incidentes e Padronização da Segurança da Informação.

2.14.2. A adoção de solução de segurança baseada em Appliance Next Generation Firewall (NGFW) proporciona recursos avançados de detecção, prevenção e resposta automatizada a incidentes, permitindo atuação tempestiva frente a ameaças cibernéticas, com significativa redução de impactos operacionais e garantia da continuidade dos serviços públicos essenciais.

2.14.3. Adicionalmente, a padronização dessa solução em todas as autarquias municipais e na Câmara Municipal promove a uniformização das políticas de segurança da informação, o controle centralizado do tráfego de rede e a aplicação consistente de mecanismos de proteção, elevando o nível de maturidade da governança de TIC no âmbito municipal.

2.14.4. Tal medida fortalece a rastreabilidade, o monitoramento e a capacidade de auditoria dos eventos de segurança, assegurando maior transparência, controle e conformidade

com normativas legais e boas práticas de segurança da informação, inclusive no que se refere à proteção de dados pessoais e à mitigação de riscos institucionais.

2.14.5. Nesse contexto, a padronização da solução NGFW contribui diretamente para a construção de um ambiente tecnológico mais seguro, resiliente e integrado, alinhado às diretrizes de governo digital e à necessidade de proteção dos ativos críticos da Administração Pública Municipal.

2.15. **Atendimento às Novas Regras do Decreto**:

2.15.1. O Decreto nº 10.540/2020 representa um marco na busca por eficiência e integração nos processos municipais, determinando a padronização dos sistemas utilizados pelas entidades. A adoção de uma mesma "linguagem" nos sistemas torna-se fundamental para atender a esse novo cenário normativo a partir de 2024.

2.16. **Facilitação da Comunicação Interinstitucional com Segurança:**

2.16.1. A utilização de uma solução NGFW padronizada possibilita o estabelecimento de políticas unificadas de segurança, controle de tráfego e comunicação segura entre as autarquias municipais e a Câmara Municipal. A interoperabilidade segura, inclusive por meio de VPNs e segmentação de rede, contribui para a integração dos sistemas, evitando vulnerabilidades, retrabalhos e inconsistências nos fluxos de informação.

2.17. **Eficiência Operacional e Redução de Custos:**

2.17.1. A centralização da segurança em uma solução NGFW reduz a complexidade da gestão de múltiplas ferramentas isoladas, promovendo maior eficiência operacional. Além disso, a padronização contribui para a otimização de recursos, reduzindo custos com licenciamento, treinamento, manutenção e suporte técnico, bem como minimizando impactos decorrentes de incidentes de segurança.

2.18. **Transparência, Rastreabilidade e Conformidade:**

2.18.1. A uniformização da solução de segurança fortalece a capacidade de monitoramento, auditoria e rastreabilidade dos eventos de rede. A geração de logs e relatórios detalhados permite maior transparência na gestão dos ativos tecnológicos, facilitando a prestação de contas aos órgãos de controle e assegurando conformidade com legislações como a LGPD.

2.19. **Modernização e Resiliência Cibernética:**

2.19.1. A adoção de tecnologia NGFW representa um avanço significativo na modernização da infraestrutura de TIC do município, incorporando recursos avançados de prevenção, detecção e resposta a incidentes. Essa medida posiciona o município de forma proativa frente às crescentes ameaças cibernéticas, garantindo maior resiliência e continuidade dos serviços públicos digitais.

2.20. **Agilidade na Implementação de Atualizações e Políticas de Segurança:**

2.20.1. A padronização da solução NGFW permite a implementação ágil e coordenada de atualizações, correções de segurança e novas políticas de proteção em todo o ambiente municipal. Isso assegura que todas as unidades administrativas estejam continuamente protegidas, atualizadas e em conformidade com as melhores práticas e normativas em constante evolução.

2.20.2. Diante do exposto, a contratação de uma solução de segurança baseada em Appliance Next Generation Firewall (NGFW), por meio de pregão eletrônico, configura-se como medida estratégica, necessária e alinhada ao interesse público, visando à proteção da infraestrutura tecnológica do Município de Congonhas.

2.20.3. Tal investimento não apenas assegura o cumprimento das exigências legais e normativas vigentes, especialmente no que tange à segurança da informação e à proteção de dados, como também promove ganhos substanciais em termos de disponibilidade, integridade e confidencialidade dos sistemas e serviços públicos digitais.

2.20.4. Adicionalmente, a implementação da solução contribuirá para a mitigação de riscos cibernéticos, o fortalecimento da governança de TIC e o aumento da eficiência operacional, refletindo diretamente na melhoria da qualidade e da continuidade dos serviços prestados à população.

2.20.5. Considerando o vencimento em 04/05/2026 do CONTRATO PMC/050/2022 vinculado ao pregão presencial PCM/PREGÃO 113/2021, cujo objeto tem como por objetivo a contratação de empresa especializada para a prestação de serviço de suporte técnico especialista em Microsoft Office365 e Microsoft Windows Server ADM Active Directory e solução integrada de segurança que possibilite a visibilidade e controle de tráfego, filtragem de conteúdo web, filtro de dados, VPN, servidores web dedicado na nuvem para hospedagem do site e solução de rede wireless como serviço gerenciado e controlador na nuvem, para a Prefeitura Municipal de Congonhas – MG.

2.20.6. Considerando que já está em tramitação novo processo licitatório, iniciado através da Comunicação Interna nº 7722 do dia 02/02/2026. Considerando ser um serviço de natureza continuada de extrema importância para o funcionamento dos setores da administração pública.

2.20.7. A nova contratação dos serviços de Appliance Next Generation Firewall (NGFW) foi iniciada em fevereiro de 2026, na LEI N.º 14.133, DE 1º DE ABRIL DE 2021, todavia não haverá prazo legal para a conclusão do processo licitatório e prazos legais para implantação e migração de sistema pela vencedora do certame.

2.20.8. Faz necessário a contratação por dispensa por 12 meses ou até a conclusão do processo licitatório em andamento seja concluído.

2.20.9. A justificativa contempla a caracterização da situação de dispensa emergencial (art. 75, Lei n. 14.133/2021), com os elementos necessários à sua configuração (art. 6º,

XXIII, d e art. 18, § 1º, III, ambos da Lei n. 14.133/2021). Os atos em que se verifique a dispensa de licitação fogem ao princípio constitucional da obrigatoriedade de realização de certame, consagrando-se como exceções a este princípio normativo. Assim trata-se de ato discricionário, mas que devido a sua importância e necessidade extrema de idoneidade, se submete ao crivo de devida justificativa que o ateste. No presente caso encontra-se justificada a dispensa requerida dado o fato da presente contratação estar dentro do disposto no inciso VIII, do art. 75, da Lei 14.133/2021, o que justifica a contratação emergencial, já que se trata de serviço essencial e sua interrupção pode comprometer diretamente o trabalhos a serem executados pelos servidores em atendimento ao munícipes em todas as Secretarias, da Prefeitura Municipal de Congonhas , implicando em sérios transtornos e comprometendo o funcionamento regular do Órgão, torna-se imprescindível a contratação de empresa para execução dos serviços.

2.20.10. Em suma vislumbramos que a presente contratação de ser respaldada pela lei geral de Licitações nº 14.133/2021, devendo também obedecer todos os ditamos exigidos, sendo assim vimos que a presente licitação deveria ser executada na forma eletrônica porem vale ressaltar que no caso em tela se torna inviável a elaboração, por mais que a forma eletrônica traz uma celeridade processual, o procedimento atual não permite, O § 3º do artigo 75 da Lei n. 14.133/2021 prescreve que as hipóteses de dispensa dos seus incisos I e II devem ser "preferencialmente precedidas de divulgação de aviso em sítio eletrônico oficial, pelo prazo mínimo de 3 (três) dias úteis, com a especificação do objeto pretendido e com a manifestação de interesse da Administração em obter propostas adicionais de eventuais interessados, devendo ser selecionada a proposta mais vantajosa."

2.20.11. Para as demais hipóteses de dispensa de licitação previstas no artigo 75 da Lei n. 14.133/2021, mesmo que os valores ultrapassem os limites dos incisos I e II do mesmo artigo, a dispensa de licitação eletrônica deve ser utilizada "quando cabível", na expressão do inciso III do artigo 4º da Instrução Normativa n. 67/2021. Ressalta-se que, quando for cabível, os agentes administrativos não estão livres para deixarem de utilizar a dispensa de licitação eletrônica, que passa a ser a regra, cujo não emprego demanda a existência de algum motivo ou razão. Sucede que a dispensa de licitação eletrônica é cabível nas situações em que a escolha do futuro contratado for pautada no critério preço, sem que aspectos qualitativos sejam determinantes ou relevantes, o que constitui a maioria expressiva dos casos de dispensa de licitação. Sendo assim, a não utilização da dispensa de licitação eletrônica passa a ser a exceção, que tem lugar em casos específicos, como os que envolvem emergências, inovação tecnológica, serviços técnicos especializados de natureza predominantemente intelectual e outras situações de dispensa, insista-se, em que o fator determinante ou relevante para a Administração escolher o futuro contratado seja o qualitativo.

2.20.12. Vale trazer também o decreto Municipal Nº 7.653, de 19 de Outubro de 2023, ao qual

dispõe sobre o procedimento de dispensa de licitação da lei geral de licitações 14.133/2021, nesse diapasão vislumbramos que o mesmo segue fielmente o regramento da lei geral, uma vez que o caráter preferencial do procedimento eletrônico está vinculado aos incisos I e II do art. 75 da lei 14.133/21, sendo assim vimos que no caso em comento torna-se necessário a realização da dispensa de forma presencial tendo vista a não obrigatoriedade no decreto Municipal bem como a necessidade imediata de início de contrato, para o bem da continuada do serviço público.

2.20.13. Ressalta-se que, em 02/02/2026, foi devidamente autorizada a abertura do procedimento licitatório, contendo todos os elementos necessários ao regular prosseguimento do feito, notadamente o Documento de Oficialização da Demanda (DOD), o Estudo Técnico Preliminar (ETP) e o Mapa de Gerenciamento de Riscos, em conformidade com as disposições da Lei nº 14.133/2021.

2.20.14. Na sequência, em 12/02/2026, os autos foram encaminhados à Central de Planejamento, Estruturação e Monitoramento de Processos Licitatórios, a qual procedeu à análise inicial e remeteu o processo à área de Compras, responsável pela realização da pesquisa de preços e elaboração da estimativa de valor da contratação, etapa essencial para aferição da vantajosidade econômica.

2.20.15. Concluída essa fase, o processo foi encaminhado à área de Orçamento para a devida verificação e bloqueio orçamentário, assegurando a compatibilidade da despesa com a previsão orçamentária vigente. Posteriormente, os autos seguiram à área responsável pela condução do pregão, para elaboração da minuta do edital e seus anexos.

2.20.16. Adicionalmente, o processo será submetido à área de Economia para definição dos índices contábeis aplicáveis, bem como à Procuradoria Municipal para análise jurídica quanto à regularidade do procedimento. Por fim, será encaminhado à Controladoria Interna do Município para emissão de checklist e apontamentos técnicos, garantindo o cumprimento dos princípios da legalidade, eficiência, controle e governança.Com Joel de Menezes Niebuhr, devemos convir que para que um serviço seja tido por contínuo faz-se necessário, antes de mais nada, que seu conteúdo jurídico seja uma obrigação de fazer (obligatio faciendi) e não uma obrigação de dar, como é próprio das aquisições. Assevera ainda ao renomado autor:

2.20.17. “Em abordagem inicial, serviços contínuos, como o próprio nome revela, são aqueles prestados sem interrupção, sem solução de continuidade. Portanto, serviços que são prestados eventualmente não são qualificados como contínuos. Todavia, para qualificar serviço como contínuo não é necessário que o prestador do serviço realize algo em favor da contratante diariamente. Por exemplo, serviços de manutenção de bens móveis ou imóveis são qualificados como contínuos, muito embora não seja usual necessitar os préstimos do contratado diariamente. Então, a rigor, serviços contínuos

são aqueles em que o contratado põe-se à disposição da Administração de modo ininterrupto, sem solução de continuidade. Em vista disso, pode-se dizer que, em regra, os serviços contínuos correspondem à necessidade permanente da Administração, a algo que ela precisa dispor sempre, ainda que não todos os dias.

2.20.18. Nessa senda, "a identificação dos serviços de natureza contínua não se faz a partir do exame propriamente da atividade desenvolvida pelos particulares, como execução da prestação contratual. A continuidade do serviço retrata, na verdade, a permanência da necessidade pública a ser satisfeita". Vimos também que no momento da formalização do procedimento licitatório a época a mesma foi fundamentada no art. 57, inciso II, pois o mesmo tratava de aluguel de equipamento e a utilização de programa de informática, podendo a duração estender-se pelo prazo de até 48 (quarenta e oito) meses após o início da vigência do contrato, porem no momento dessa avalição o houve um equívoco pela área requisitante por entender que se tratava de serviço de TIC, e um serviço ou bem de Tecnologia da informa e comunicação, e sim contrato de prestação de serviço continuado.

2.20.19. Lado outro trazemos também a possibilidade de prorrogação pela superveniência de fato excepcional ou imprevisível, estranho a vontade das partes, do artigo 57 , §1º, inciso II da lei 8.666/93, porem na referida lei não há previsão legal prorrogação deste tipo de contrato além dos 48 (quarenta e oito) meses previstos no inciso IV, nem mesmo a excepcionalidade do §4º se aplica a presente situação, vez que menciona, de forma expressa, a sua aplicação ao inciso II do CAPUT do art.57, ou seja serviços continuados, vejamos:

> **§ 4º Em caráter excepcional, devidamente justificado e mediante autorização da autoridade superior, o prazo de que trata o inciso II do caput deste artigo poderá ser prorrogado por até doze meses.**

2.20.20. Vale trazer baila a necessidade de exemplificar a escolha do fornecedor em questão, sendo a empresa NETSOL LTDA-ME, um ponto relevante além do menor preço ofertado, a empresa em questão já é a empresa que presta serviço dentro da municipalidade ou seja traria para os cofres públicos uma economicidade por se tratar de um sistema já operacionalizado pelo ente, sendo que seria tão somente a continuidade do trabalhos e serviços já contratados. Vale trazer também que a empresa em questão apresenta todos os requisitos para continuidade do serviço.

2.20.21. A prestação de serviço disponibilizada pela empresa supracitada é compatível e não apresenta grandes diferenças que venha a influencia na preferência, ficando esta escolha vinculada apenas à verificação do critério do menor preço.

2.20.22. Quer dizer, excepcionar a regra de realização de licitação não significa que não haja formalidades a serem observadas pelo administrador e requisitos a serem preenchidos para viabilizar a contratação direta. Dito isto, e no que é pertinente à espécie, consigna-se, inicialmente, que "emergência" traduz a necessidade de pronto

atendimento a determinado interesse, sendo inviável aguardar os trâmites ordinários da licitação, sob pena de não atendimento ou prejuízo de atendimento a alguma demanda social. No caso em apreço, a propósito, aguardar todo o trâmite licitatório fragilizaria, sem margem para dúvidas, ainda mais a população que mais precisa da prestação estatal, dando azo a um cenário de nítida injustiça social e vulnerabilidade.

2.20.23. No mesmo sentido, de acordo com entendimento do TCU:

> "Nas contratações diretas fundadas em emergência (art. 24, inciso IV, da Lei 8.666/1993), **cabe ao gestor demonstrar a impossibilidade de esperar o tempo necessário à realização de procedimento licitatório**, em face de risco de prejuízo ou comprometimento da segurança de pessoas e de bens públicos ou particulares, além de justificar a escolha do fornecedor e o preço pactuado. (Acórdão 1130/2019- Primeira Câmara | Relator: BRUNO DANTAS)" (grifei)

2.20.24. No que tange, pois, à contratação direta de serviço de locação de geradores, para atendimento a uma situação emergencial, com fulcro, portanto, no art. 75, inc. VIII, da Nova Lei de Licitações, é preciso que o gestor, no bojo do processo administrativo, e de forma clara e objetiva, demonstre a emergência e justifique a impossibilidade de aguardar o tempo necessário à realização de licitação para adquirir aquela determinada quantidade do produto desejado.

2.20.25. A respeito do tema, seguem julgados do TCU:

> "A contratação emergencial só deve atender a situação emergencial até a realização de nova licitação (art. 24, inciso IV, da Lei 8.666/1993). (Acórdão 2988/2014-Plenário | Relator: BENJAMIN ZYMLER)". "A contratação direta emergencial, fundamentada no art. 24, inciso IV, da Lei 8.666/1993, **deve se restringir somente à parcela mínima necessária para afastar a concretização do dano ou a perda dos serviços executados**, devendo a solução definitiva, conforme o caso, ser objeto de licitação formal. (Acórdão 6439/2015- Primeira Câmara | Relator: AUGUSTO SHERMAN)".

2.20.26. Assim, alerta-se ao administrador que a contratação emergencial não pode servir de subterfúgio para, diante da flexibilização procedimental, incluir-se, no bojo da contratação, quantitativos ou objetos alheios ao premente atendimento da situação. No caso em tela fica evidenciado que gestor do presente processo está tão somente buscando a continuidade das atividades do sistema de Gestão ERP para operacionalização da máquina pública em os seus sistemas informatizados de gestão pública.

2.20.27. Portanto, não nos cabe outra saída a não ser a Solicitação de processo de Dispensa de licitação fundada no artigo 75, inciso VIII da lei 14.133/2021, uma vez que é imprescritível a continuidade do serviço, por caracterizada urgência de atendimento de situação que possa ocasionar prejuízo ou comprometer a continuidade do serviço

público, sendo necessário essa continuidade para desenvolvimento das atividades administrativas da máquina pública, mecanismo este que se tornou imprescindível para continuidade do mesmo, tendo como pilar todos os módulos de gestão administrativa operacionalizada pelo município de Congonhas-MG.

3. DO VALOR DA CONTRATAÇÃO, DA PROPOSTA E DO REGIME DE EXECUÇÃO

3.1. O custo estimado total da contratação é de **R$ 428.518,32 (quatrocentos e vinte oito mil quinhentos e dezoito e trinta e dois centavos),** conforme proposta anexa.

3.2. **PLANILHAS DE QUANTIDADES E PREÇO.**

ITEM	DESCRIÇÃO	QUANT	UNIDADE	VALOR MENSAL	VALOR 12 MESES
01	Prestação de Suporte à solução Microsoft Office 365,	1	UN	R$ 7.138,75	R$ 85.665,00
02	Prestação de suporte e configuração à servidor de administração de rede local. Microsoft Windows Server AD Active Directory.	1	UN	R$ 6.691,10	R$ 80.293,20
03	Prestação de serviço de segurança da informação com escaneamento de vulnerabilidades periódico.	1	UN	R$ 5.169,96	R$ 62.039,52
04	Solução de segurança de internet Appliance Inclui: alta disponibilidade e licenciamento incluindo relatórios	1	UN	R$ 12.963,55	R$ 155.562,60
05	Servidor Web Host em nuvem Hardware com HD de 5 Terabytes + 64 GB de RAM	1	UN	R$ 3.746,50	R$ 44.958,00
				Total=	**R$ 428.518,32**

4. DO LOCAL E DAS CONDIÇÕES DA PRESTAÇÃO DOS SERVIÇOS

4.1. Oequipamento do servidor sera instalado na Av. Júlia Kubitschek, 230, Centro Edifício Espaço JK

DTIN - Diretoria de Tecnologia da Informação - Sala CPD.

5. ESPECIFICAÇÕES TÉCNICAS

5.1. **SUPORTE TÉCNICO DO MICROSOFT OFFICE 365**

5.1.1. O serviço de suporte técnico à solução fornecida e implementada, deverá ser iniciada em até 30 dias corridos contados do recebimento da Ordem de Serviço.

5.1.2. Correção de problemas e esclarecimento de dúvidas sobre configuração, funcionamento e utilização da solução ofertada.

5.1.3. Manutenção e atualização da solução ofertada.

5.1.4. O serviço de suporte será prestado pela CONTRATADA conforme a necessidade da CONTRATANTE durante a vigência do contrato, período integral (24x7x365), sem limite de quantidade de atendimentos.

5.1.5. Os serviços serão solicitados pela equipe técnica da DTIN _ Diretoria de Tecnologia da Informação mediante abertura de atendimento junto à CONTRATADA, via chamada telefônica local ou gratuita, e-mail ou sítio na Internet.

5.1.6. A CONTRATADA após registrado atendimento deverá enviar para o e-mail dtin@congonhas.mg.gov.br com o número do registro do atendimento para acompanhamento.

5.1.7. No caso de indisponibilidade do e-mail a CONTRATADA deverá informar o número do registro do atendimento no telefone 31 3731-1300 ramais 1196.

5.1.8. O tempo máximo de resposta inicial para atendimento registrado deverá ser de 60 (sessenta) minutos.

5.1.9. Os atendimentos poderão ser realizados remotamente (via Internet, telefone ou e-mail) ou presencialmente, se necessário.

5.1.10. Todos chamados deverão ser tratados em língua portuguesa do Brasil.

5.2. **CARACTERÍSTICAS**

5.2.1. A CONTRATADA deverá instalar, configurar e parametrizar toda a solução.

5.2.2. A CONTRATADA deverá dar o treinamento técnico de toda a solução para a equipe de TI da CONTRATANTE.

5.2.3. A CONTRATANTE poderá durante o período do contrato solicitar novos treinamentos sempre que julgar necessário, sem nenhum custo adicional.

5.2.4. O pagamento do serviço contratado será efetuado mensalmente durante o período de vigência do contrato.

5.2.5. Em caso de utilização de softwares proprietários, as licenças em nome do fornecedor deverão ser apresentadas após a instalação.

5.2.6. Geração de relatórios em tempo real das atividades de correio eletrônico.

5.2.7. Permitir a configuração de múltiplos domínios.

5.2.8. Monitorar o funcionamento da solução com software de monitoramento ativo, de modo a antecipar problemas como disco lotado, alta carga de processamento e serviço indisponível.

5.3. **TIPOS DE SERVIÇOS**

5.3.1. Entende-se por suporte/manutenção o serviço de ajustes, correções e configurações nos softwares, sem custo adicional para CONTRATANTE, sob as condições abaixo especificadas:

5.3.1.1. **Manutenção Preventiva** - A manutenção preventiva corresponde às verificações e ajustes necessários ao correto funcionamento de toda a solução, atendendo questões que não alterem a estrutura do sistema.

5.3.1.2. **Manutenção Corretiva** - Manutenção de toda a solução para correção de erros nas funcionalidades e consultoria.

5.3.1.3. **Manutenção Evolutiva** (ou upgrade) - Aplicação de novas atualizações e versões, acompanhando a evolução das ferramentas no que se refere a novas funcionalidades implementadas por seus desenvolvedores, bem como correções que visam sanar eventuais falhas de segurança.

5.4. **AMBIENTE TECNOLÓGICO**

5.4.1. As atividades desenvolvidas pela CONTRATADA deverão ocorrer no ambiente computacional de produção alocados no datacenter da CONTRATADA.

5.4.2. Para alterações significativas deve se ter um plano para testes feitos em segundo ambiente dito de homologação que deverá ser criado nesta oportunidade, garantindo-se a continuidade dos serviços.

5.4.3. Os servidores físicos deverão ser baseados em estrutura Intel 64 bits.

5.5. **SOLUÇÃO DE SEGURANÇA BASEADA EM APPLIANCE NEXT GENERATION FIREWALL**

5.5.1. Prestação de serviços de solução integrada de segurança que possibilite a visibilidade e c ontrole detráfego, filtragem de conteúdo Web, prevenção contra ameaças de rede moder nas, filtro de dados, VPN e controle granular de banda de rede, compreendendo fornecim ento de equipamento e software integrados Appliance, na modalidade locação; licenciam

ento, garantia de atualização e funcionamento, com suporte técnico, durante o período d e 12 (*doze*) meses, conforme especificações e condições estabelecidas neste Edital.

5.6. **REQUISITOS TÉCNICOS**

5.6.1. Não serão permitidas soluções baseadas em sistemas operacionais abertos como FreeBSD, Debian ou mesmo Linux.

5.6.2. Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 3.0 Gbps ou superior.

5.6.3. Desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 800 Mbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item.

5.6.4. Desempenho mínimo de 3.3 Gbps de IPS.

5.6.5. Suporte mínimo de 500.000 conexões simultâneas/concorrentes no modo DPI.

5.6.6. Suporte mínimo de 20.000 novas conexões por segundo.

5.6.7. Deve suportar expansão de armazenamento interno para até 256Gb.

5.6.8. Deve possuir fonte de alimentação com chaveamento automático de 100-240 VAC.

5.6.9. Deve possuir 16 interfaces 1 GbE padrão RJ-45.

5.6.10. Deve possuir 3 interfaces 10GbE SFP+;

5.6.11. Deve possuir 1 do tipo 1 GbE RJ-45 dedicada paraa gerenciamento do equipamento.

5.6.12. Deve possuir 1 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G.

5.6.13. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 5 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 200 usuários simultâneos, com aquisição de licença complementar.

5.6.14. A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 100 usuários simultâneos, com aquisição de licença complementar.

5.6.15. Deve suportar 250 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos.

5.6.16. Deve suportar, no mínimo, 2.1 Gbps de desempenho de VPN IPSEC.

5.6.17. Os desempenhos apontados devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitados. Todos os custos oriundos do teste de bancada serão custeados pelo fornecedor/vendedor do certame.

5.6.18. O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovado através de carta de reconhecimento assinada pelo representante legal do fabricante no Brasil.

5.6.19. O Equipamento deverá ser homologado pela ANATEL.

5.6.20. Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de desempenho solicitados.

5.6.21. O licenciamento para todos os serviços de Next Generation Firewall deverá ser de no 12 (*doze*) meses.

5.6.22. A garantia do hardware deverá ser de 12 (*doze*) meses.

5.7. **CARACTERÍSTICAS GERAIS**

5.7.1. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall. O termo Next Generation Firewall doravante será empregado como NGFW ou simplesmente FIREWALL.

5.7.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões.

5.7.3. Para proteção do ambiente contra-ataques, o dispositivo de proteção deve possuir módulos de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados ao próprio appliance de NGFW.

5.7.4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

5.7.5. Define-se o termo “appliance” como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço.

5.7.6. Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de “appliance” que utilizam hardware e software de fabricantes diferentes.

5.8. **CARACTERÍSTICAS DIVERSAS**

5.8.1. Deve implementar controle do tráfego para os protocolos TCP, UDP, ICMP, e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino.

5.8.2. Implementar recurso de NAT (network address translation) tipo one-to-one, one-to-many, many-to-many, many-to-one, porta TCP de conexão (NAPT) e NAT Traversal em VPN IPSec (NAT-T) e NAT dentro do tunel IPSec.

5.8.3. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.

5.8.4. Deve possuir proteção anti-spoofing.

5.8.5. Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP;

5.8.6. Suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF.

5.8.7. Suporte a Policy-Based Routing (PBR), com a capacidade de roteamento no mínimo, mas não limitadoa: endereço de origem, endereço de destino, serviço e aplicação.

5.8.8. A solução deverá implementar tecnologia de SD-WAN (Software Defined WAN).

5.8.9. Capacidade de agregar no mínimo 4 (quatro) circuitos WAN distintos em um único canal lógico onde seja possível criar controles de caminho automático baseado em políticas, com habilidade de selecionar o melhor caminho, no mínimo, através dos seguintes parâmetros simultâneos:

5.8.9.1. Latência;

5.8.9.2. Jitter;

5.8.9.3. Perda de pacotes.

5.8.10. O administrador da solução deverá ter a capacidade de configurar o canal lógico de SD-WAN para encaminhar tráfego simultaneamente por todos os links pertencentes a esse canal logico.

5.8.11. A comutação do SD-WAN deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas.

5.8.12. A solução de SD-WAN deve permitir encaminhamento de trafego com base em assinaturas de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook.

5.8.13. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

5.8.14. Deve suportar modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

5.8.15. Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.

5.8.16. Possuir servidor de DHCP (Dynamic Host Configuration Protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e via VPN.

5.8.17. Deve suportar DHCP relay.

5.8.18. Possibilitar a aplicação de regras de firewall e IPS por IP e grupo de usuários, permitindo a definição de regras para determinado horário ou período (dia da semana e hora) com matriz de horários que possibilite o bloqueio de serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários.

5.8.19. Deve permitir a utilização de regras de Anti-Vírus, Anti-Spyware, IPS e filtro de conteúdo web por segmentos de rede. Todos os serviços devem ser suportados no mesmo segmento de rede, VLAN ou zona de segurança.

5.8.20. Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares p2p (peer-to-peer) incluindo, no mínimo, Kazaa, Limewire, Morpheus e Napster e de comunicadores instantâneos (instant messengers) incluindo, no mínimo, ICQ, WhatsApp, Google Talk, Skype e IRC, para usuários da rede, individualmente ou em grupo.

5.8.21. Deve ter suporte a proteção e identificação de hosts possivelmente infectados com “botnets”. A solução ofertada deve permitir ao administrador a possibilidade de apenas registrar e identificar as máquinas possivelmente contaminadas, além de ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, bem como ativar tal funcionalidade especificando análise por regra de firewall, permitindo assim maior granularidade da gestão e do recurso.

5.8.22. Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques DoS (denial-of-service) e DDoS devidamente licenciados.

5.8.23. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.

5.8.24. Detectar e bloquear a origem de portscans.

5.8.25. Deve permitir o bloqueio de ataques.

5.8.26. Deve permitir o bloqueio de exploits conhecidos.

5.8.27. O gateway Anti-Vírus deve suportar a análise de pelo menos os protocolos HTTP, FTP, IMAP, e SMTP.

5.8.28. Deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL, que deverá ser decriptografado de forma transparente à aplicação.

5.8.29. Implementar DSCP (Differentiated Services Code Points).

5.8.30. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, SIP, RTP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro da rede.

5.8.31. Implementar controle e gerenciamento de banda para a tecnologia VoIP (Voice OverIP) sobre diferentes segmentos de rede com inspeção profunda de segurança sobre este serviço.

5.8.32. Implementar mecanismo de sincronismo de horário através do protocolo NTP.

5.8.33. Possuir suporte ao protocolo SNMP versões 2 e 3.

5.8.34. Possuir suporte a log via syslog.

5.8.35. Possuir suporte aos protocolos de roteamento RIP, OSPF e BGP. As configurações de RIP e OSPF devem ser configuradas através da interface gráfica.

5.8.36. O fabricante ou o produto deve possuir certificado ICSA (International Computer Security Association) para FIREWALL, ou CC (Common Criteria). Será aceito certificado equivalente ao ICSA, emitido por órgãos nacionais com competência para tal, desde que nos moldes deste, ou seja, certificado baseado na versão ou release atual do firewall, com manutenção recorrente deste certificado a cada mudança de versão, ou após determinado período de tempo, e baseado em normas nacionais e internacionais de segurança da informação.

5.8.37. Visando estabelecer efetividade de segurança dos firewalls de nova geração e assegurar que o fornecedor tenha uma solução já testada e comprovada por um órgão independente de mercado, o fabricante da solução deverá ser avaliado e certificado pelo NetSecOPEN, além de ser avaliado e citado pelo Gartner MQ (Magic Quadrant for Network Firewalls) nos relatórios de 2019 ou mais recentes.

5.8.38. Reconhecer aplicações como, no mínimo, peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail.

5.8.39. Para tráfego criptografado SSL/TLS, deve de-criptografar pacotes possibilitando a leitura de payload dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante.

5.8.40. Controle, inspeção e de-criptografia de SSL/TLS por política para tráfego de entrada (Inbound) ou Saída (Outbound) com suporte a no mínimo, SSLv23, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3

5.9. **CARACTERÍSTICAS DE VPN**

5.9.1. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site, com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

5.9.2. Suportar algoritmos de criptografia 3DES, AES 128 e AES 256.

5.9.3. Suportar algoritmos Hash no mínimo SHA-1, SHA-256 e SHA-384.

5.9.4. Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits.

5.9.5. Deverá suportar algoritmo Internet Key Exchange (IKE)v1 e v2.

5.9.6. Autenticação via de tuneis IPSec via certificado digital para VPNs Site-to-Site e Client-to-Site.

5.9.7. A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android.

5.9.8. Solução deve suportar VPNs baseadas em políticas, e VPNs baseadas em roteamento estático e/ou dinâmico.

5.9.9. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo Site-to-Site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

5.9.10. Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos.

5.9.11. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário.

5.9.12. Permitir criação de políticas de roteamento estático utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego, sendo este visto pela regra de roteamento como uma interface simples de rede para encaminhamento do tráfego.

5.9.13. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

5.9.14. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, certificados digitais e XAUTH client authentication.

5.9.15. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário.

5.9.16. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

5.10. **ALTA DISPONIBILIDADE**

5.10.1. Devem ser fornecidos 02 (dois) appliances de NGFW com gerenciamento unificado, novos e sem uso anterior, funcionando em alta disponibilidade. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta. O software deverá ser fornecido em sua versão mais atualizada.

5.10.2. A solução deve ser entregue operando em alta disponibilidade no modo Ativo/Standby, com as implementações de Failover.

5.10.3. Não serão permitidas soluções de cluster (HA) que façam com que os equipamentos se reiniciem após qualquer modificação de parâmetro/configuração realizada pelo administrador.

5.10.4. A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster.

5.10.5. A solução deve operar em alta disponibilidade implementando monitoramento lógico de um host na rede, e possibilitar failover.

5.10.6. A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover.

5.10.7. A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster incluído, mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança.

5.10.8. A solução deve permitir visualizar no equipamento principal, o status da comunicação entre os parceiros do cluster, status de sincronização das configurações, status atual do equipamento redundante.

5.11. **CONTROLE DE AMEAÇAS**

5.11.1. Para as ameaças de dia-zero, a solução deve ter a habilidade de prevenir o ataque antes de qualquer assinatura ser criada. Deve possuir módulo de Anti-Vírus e Anti-Bot integrado ao próprio appliance de segurança.

5.11.2. A solução de Anti-Virus integrada deve ter capacidade de analisar arquivos maiores que 1Gbps.

5.11.3. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas.

5.11.4. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego.

5.11.5. Implementar funcionalidade de detecção e bloqueio de “call-backs”.

5.11.6. A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede.

5.11.7. A solução Anti-bot deve possuir mecanismo de detecção que inclua reputação de endereço IP.

5.11.8. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS.

5.11.9. Implementar interface CLI segura através do protocolo SSH.

5.11.10. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream.

5.11.11. A solução deve permitir criar regras de exceção de acordo com a proteção.

5.11.12. Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts, ou incidentes referentes a vírus e Bots;

5.11.13. Permitir o bloqueio de malwares (vírus, worms, spyware e etc).

5.11.14. A solução deve ser capaz de proteger contra-ataques a DNS.

5.11.15. A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares.

5.11.16. A solução deve ser capaz de prevenir acesso a websites maliciosos.

5.11.17. A solução deve ser capaz de realizar inspeção de tráfego SSL/TLS e SSH.

5.11.18. A solução deverá receber atualizações de um serviço baseado em cloud.

5.11.19. A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos.

5.11.20. A solução Anti-Vírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS.

5.11.21. A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade

5.11.22. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance de firewall, onde sua console de gerência deverá residir na mesma console centralizada dos appliances de segurança, com suporte a pelo menos 3.000 assinaturas;

5.11.23. A solução de IPS deverá possuir os seguintes mecanismos de detecção: assinaturas e trabalhar em conjunto com o controle de aplicações;

5.11.24. A solução de IPS deve fazer a inspeção de todo o pacote, independentemente do tamanho;

5.11.25. A solução de IPS deve fazer a inspeção de todo o trafego de forma bidirecional, analisando qualquer tamanho de pacote sem degradar a performance do equipamento solicitada neste edital;

5.11.26. Possuir capacidade de remontagem de pacotes para identificação de ataques;

5.11.27. O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;

5.11.28. Para cada proteção de segurança, deve ser possível consultar informações no site do fabricante.

5.11.29. A ferramenta de log deve possuir a capacidade de criar uma regra de exceção a partir do log visualizado na gerência centralizada;

5.11.30. As regras de exceção devem possuir: origem, destino e serviço;

5.11.31. A solução deve ser capaz de inspecionar tráfego HTTPS.

5.11.32. 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;

5.11.33. Detecção de anomalias;

5.11.34. A solução de IPS deve possuir política capaz de definir o modo de operação (bloqueio ou detecção);

5.11.35. O módulo de IPS deve possuir assinaturas voltadas para ambientes de servidores de SMTP, Web e DNS;

5.11.36. O mecanismo de inspeção deve receber e implementar em tempo real atualizações de novas assinaturas sem a necessidade de reiniciar o appliance;

5.11.37. Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na origem e destino;

5.11.38. A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações web, serviços de e-mail, DNS, FTP, SQL Injection, ataques a sistemas operacionais e VOIP;

5.11.39. Deve incluir proteção contra worms;

5.11.40. Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades e a evolução ao logo do tempo dispondo o sumario quantitativo das ameaças analisadas.

5.11.41. A solução deve possuir esquema de atualização de assinaturas através de um click;

5.11.42. Atualização de modo offline, onde poder ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução;

5.11.43. A solução deve suportar importar certificados de servidor para inspeções de tráfego seguro HTTP (HTTPS) de entrada. Depois de importar esses certificados, a solução deve permitir o IPS para Inspeção segura HTTP(HTTPS);

5.11.44. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos;

5.11.45. A solução deverá possuir proteções para sistemas SCADA;

5.11.46. Solução deverá permitir que o administrador bloqueie facilmente o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente os ranges de endereços IP dos países que deseja bloquear.

5.12. **PROTEÇÃO CONTRA ATAQUES AVANÇADOS**

5.12.1. A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de “call-backs”.

5.12.2. Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS.

5.12.3. A solução deve ser capaz de inspecionar o tráfego criptografado SSL/TLS e SSH.

5.12.4. Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle.

5.12.5. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real.

5.12.6. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb.

5.12.7. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android.

5.12.8. Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware.

5.12.9. A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.

5.12.10. A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este seja responsável por atualizar toda a base de segurança dos appliance através de assinaturas.

5.12.11. Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados.

5.12.12. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e quaisquer outros mecanismos de redirecionamento de tráfego;

5.12.13. Conter ameaças avançadas de dia zero.

5.12.14. Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador.

5.12.15. Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;

5.12.16. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos.

5.12.17. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado.

5.12.18. Implementar a análise de arquivos executáveis, DLLs e ZIP no ambiente controlado.

5.12.19. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP , IMAP e CIFS.

5.12.20. Mitigar ameaças de dia zero de forma transparente para o usuário final.

5.12.21. Mitigar ameaças de dia zero através de tecnologias de emulação e código de registro.

5.12.22. Implementar mecanismo de pesquisa por diferentes intervalos de tempo.

5.12.23. Mitigarameaças de dia zero via tráfego de internet.

5.12.24. Permitir a contenção de ameaças de dia zero sem a alteração da infra-estrutura de segurança.

5.12.25. Mitigarameaças de dia zero que possam burlar o sistema operacional emulado.

5.12.26. A solução deve permitir a criação de listas brancas (whitelist) baseaas no MD5 do arquivo.

5.12.27. Mitigar ameaças de dia zero antes da execução e evasão de qualquer código malicioso.

5.12.28. Conter e mitigar exploits avançados.

5.12.29. A análise em nuvemou local deve prover informações sobre as ações do malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo malware, gerar assinaturas de Anti-Vírus e Anti-Spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede).

5.12.30. Suporte a submissão manual de arquivos para análise através do serviço de Sandbox.

5.13. **CARACTERÍSTICAS DE FILTRO DE CONTEÚDO WEB**

5.13.1. Possuir filtro de conteúdo integrado ao NGFW para classificação de páginas web com, no mínimo, 50 (cinquenta) categorias distintas, com mecanismo de atualização e consulta automáticas.
5.13.2. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs, através da integração com serviços de diretório, Active Directory e base de dados local
5.13.3. Devem ser fornecidas licenças de filtro de conteúdo para cada equipamento e quantidade de usuários ilimitada, provendo atualização automática e em tempo real através da categorização contínua de novos sites da Internet, sem custo adicional, por todo o período de vigência da garantia e do contrato de manutenção e suporte técnico.
5.13.4. Permitir a customização de página de bloqueio.
5.13.5. Controle de conteúdo filtrado por categorias de sites com base de dados continuamente atualizada pelo fabricante.
5.13.6. Deve permitir submissão de novos sites para categorização.
5.13.7. Permitir a classificação dinâmica de sitesweb, URLs e domínios.
5.13.8. Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet.
5.13.9. Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web.
5.13.10. Permitir aplicar a política de filtro de conteúdo baseada em horário do dia, bem como dia da semana.

5.14. **CARACTERÍSTICAS DE AUTENTICAÇÃO**

5.14.1. Prover autenticação de usuários para os serviços Telnet, FTP, HTTP e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea.
5.14.2. Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Tacacs+, Single Sign On e API.
5.14.3. Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento.
5.14.4. Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo NGFW.
5.14.5. Permitir o controle de acesso por usuário, para plataformas Microsoft Windows de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado sem a instalação de softwares adicionais nas estações de trabalho e sem configuração adicional no browser.
5.14.6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no NGFW.

5.14.7. Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando.
5.14.8. Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida.
5.14.9. Suportar a criação de túneis seguros sobre IP (IPSEC tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet

5.15. **CARACTERÍSTICAS DE ADMINISTRAÇÃO**

5.15.1. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o NGFW, cada um responsável por determinadas tarefas da administração.
5.15.2. Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o NGFW.
5.15.3. Possuir mecanismo para realizar remotamente, através de interface gráfica, cópias de segurança (backup) e restauração de configurações e sistema operacional.
5.15.4. Possuir mecanismo para agendamento realização das cópias de segurança(backups) de configuração.
5.15.5. Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP.
5.15.6. A solução deve permitir ao administrador aplicar ajustes rápidos das melhores práticas de segurança no dispositivo com apenas um clique, possibilitando implementar as melhores práticas recomendadas pelo fabricante.
5.15.7. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do NGFW e a remoção de qualquer uma destas sessões ou conexões.
5.15.8. Permitir a visualização, em forma gráfica, do percentual do uso de CPU e quantidade de tráfego de rede em todas as interfaces do NGFW em tempo real.
5.15.9. Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados.
5.15.10. Deve suportar minimamente dois tipos de negação de tráfego nas políticas de firewall: Descarte sem notificação do bloqueio ao usuário (discard), descarte com notificação do bloqueio ao usuário (drop), descarte com opção de envio de “ICMP Unreachable” para máquina de origem do tráfego, “TCP-Reset” para o cliente, “TCP-Reset” para o servidor ou para os dois lados da conexão.
5.15.11. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas.
5.15.12. Ser capaz de visualizar, de forma direta no appliance e em tempo real estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento.
5.15.13. Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitir a emissão deste relatório em formato PDF.

5.15.14. Ser capaz de visualizar, de forma direta no appliance e em tempo real, a largura de banda utilzida por política, por protocolo TCP/UDP IPV4 e IPV6.

5.15.15. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização.

5.15.16. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (considerando a existência do filtro de conteúdo Web).

5.15.17. Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreio das configurações aplicadas no produto.

5.15.18. Ser capaz de implementar a funcionalidade de "Zero-Touch", permitindo que o equipamento se provisione autônoma e automaticamente no sistema de gestão centralizada.

5.15.19. A solução deve possuir mecanismo de gerenciamento através de aplicativo móvel, com disponibilidade para os sistemas operacionais IOS e Android.

5.15.20. O aplicativo móvel deve possibilitar conexão ao dispositivo via protocolo HTTPS e conexão USB.

5.15.21. O gerenciamento via aplicativo móvel deve permitir visualização de status de consumo de banda, CPU, conexões ativas dos dispositivos e topologia do NGFW.

5.15.22. O aplicativo móvel deve permitir visualização de status das ameaças observadas e bloqueadas pelas funcionalidades de segurança de NGFW.

5.15.23. O aplicativo móvel deve permitir visualização dos últimos logs gerados no NGFW.

5.15.24. O aplicativo móvel deve permitir diagnósticos simples na solução, como testes ICMP e verificação DNS.

5.15.25. O aplicativo móvel deve permitir configurar interfaces, objetos e políticas de acesso, além de exportar configurações.

5.15.26. O recurso de Alta Disponibilidade deverá ser suportado em modo Bridge.

5.15.27. Possuir Mecanismo de IPS / IDS, com suporte a pelo menos 5.000 assinaturas de ataques, aplicações ou serviços, completamente integrados ao Firewall.

5.15.28. Possuir interface orientada a linha de comando para a administração do firewall a partir do console ou conexão SSH suportando está múltiplas sessões simultâneas.

5.15.29. Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.

5.15.30. Capacidade para realizar filtragens/inspeções dentro de portas TCP conhecidas por exemplo porta 80 http, buscando por aplicações que potencialmente expõe o ambiente como: P2P, Kazaa, Morpheus, BitTorrent ou messengers.

5.15.31. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD. O perfil de cada usuário deverá ser obtido automaticamente através de regras no Firewall DPI (Deep Packet Inspection) sem a necessidade de uma nova autenticação como por exemplo, para os serviços de navegação a Internet atuando assim de forma toda transparente ao usuário. Serviços como FTP, HTTP, HTTPS devem apenas consultar uma base de dados de usuários e grupos de servidores 2003/2008/2012 com AD.

5.15.32. Os Throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de

todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitados. Todos os custos oriundos do teste de bancada serão por conta do fornecedor.

5.16. **CERTIFICAÇÕES**

5.16.1. O equipamento deve comprovar através de documento do portfólio de forma pública o desempenho de todas as funcionalidades habilitadas em modo DPI ou, e através de comprovação técnica atestada por simulador de tráfego. Os custos relativos ao simulador de tráfego, caso utilizado, correrão por conta da CONTRATADA.
5.16.2. O Fabricante deve comprovar participação no MAPP da Microsoft, a comprovação deverá ser feita através do https://www.microsoft.com/en-us/msrc/mapp.
5.16.3. A Sandbox do fabricante deve ser testada pelo ICSA LABs, obtendo no mínimo 99% de efetividade contra ameaças desconhecidas do tipo "ZERO-DAY".
5.16.4. A performance mínima da plataforma de segurança, considerando as funcionalidades de firewall de aplicação, IPS, gateway antivírus e análise profunda de pacotes, operando todas simultaneamente, também deverá ser comprovada através de documento do portfólio ou comprovação técnica atestada por simulador de tráfego. Os custos relativos ao simulador de tráfego, caso utilizado, correrão por conta da CONTRATADA.
5.16.5. A Solução de NGFW deve ser avaliada e certificada pelo teste de performance de NGFW do laboratório NetSecOPEN. https://www.netsecopen.org/certifications.

5.17. **AUTENTICAÇÃO**

5.17.1. Prover autenticação de usuários para os serviços Telnet, FTP, HTTP, HTTPS e Gopher, utilizando as bases de dados de usuários e grupos de servidores NT e Unix, de forma simultânea.
5.17.2. Permitir a utilização de LDAP, AD e RADIUS.
5.17.3. Permitir o cadastro manual dos usuários e grupos diretamente na interface de gerência remota do Firewall, caso onde se dispensa um autenticador remoto para o mesmo.
5.17.4. Permitir a integração com qualquer autoridade certificadora emissora de certificados X509 que seguir o padrão de PKI descrito na RFC 2459, inclusive verificando as CRLs emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo firewall via protocolos HTTP e LDAP.
5.17.5. Permitir o controle de acesso por usuário, para plataformas Windows Me, NT, 2000, 2000, XP, Windows 7, Windows 8 e Windows 10 de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado.
5.17.6. Possuir perfis de acesso hierárquicos.
5.17.7. Permitir a restrição de atribuição de perfil de acesso à usuário ou grupo independente ao endereço IP da máquina que o usuário esteja utilizando.
5.17.8. Suportar padrão *IPSEC*, de acordo com as RFCs 2401 a 2412, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão.
5.17.9. Suportar a criação de túneis IP sobre IP (*IPSEC Tunnel*), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

5.18. **FILTRO WWW**

5.18.1. Possuir módulo integrado ao mesmo Firewall DPI (*Deep Packet Inspection*) para classificação de páginas web com no mínimo 56 categorias distintas, com mecanismo de atualização automática.
5.18.2. Deverão ser fornecidas licenças de Filtro de Conteúdo durante a vigência do contrato.
5.18.3. Controle de conteúdo filtrado por categorias de filtragem com base de dados continuamente atualizada e extensível.
5.18.4. Capacidade de submissão instantânea de novos sites e palavras chaves.
5.18.5. Permitir a classificação dinâmica de sites Web, URLs e domínios.
5.18.6. Suporte à filtragem para, no mínimo, 56 categorias e com, pelo menos, as seguintes categorias: violência, nudismo, roupas intimas/banho, pornografia, armas, ódio / racismo, cultos / ocultismo, drogas / drogas ilegais, crimes / comportamento ilegal, educação sexual, jogos, álcool / tabagismo, conteúdo adulto, conteúdo questionável, artes e entretenimento, bancos / e-trading, chat, negócios e economia, tecnologia de computadores e Internet, e-mail pessoal, jogos de azar , hacking, humor, busca de empregos, newsgroups, encontros pessoais, restaurantes / jantar, portais de busca, shopping e portais de compras, MP3, download de software, viagens e WEB hosting.
5.18.7. O administrador de política de segurança poderá definir grupos de usuários e diferentes políticas de filtragem de sites WEB, personalizando quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet.
5.18.8. O administrador de política de segurança poderá personalizar quais zonas de segurança, em cada um dos firewalls da rede, terão aplicadas as políticas de filtragem de WEB, e de maneira centralizada.
5.18.9. O administrador poderá adicionar filtros por palavra-chave de modo específico e individual em cada um dos firewalls da rede, de forma centralizada.
5.18.10. A política de Filtros de conteúdo deverá ser baseada em horário do dia e dia da semana.
5.18.11. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação.
5.18.12. Possibilitar a filtragem da linguagem Javascript e de applets Java e Active-X em páginas WWW, para o protocolo HTTP.
5.18.13. Deverá ser fornecida todas as atualizações de software assim como a atualização da base de conhecimento (*URLs categorizadas*), sem custo adicional, pelo período de vigência do contrato.

5.19. **ADMINISTRAÇÃO**

5.19.1. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas da administração.

5.19.2. Fornecer interface gráfica que permita a realização de cópias de segurança (*backups*) e sua posterior restauração remotamente, sem necessidade de se reinicializar o sistema.

5.19.3. Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica.

5.19.4. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall e a remoção de qualquer uma destas sessões ou conexões.

5.19.5. Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento.

5.19.6. Permitir a visualização de estatísticas do uso de CPU, memória da máquina onde o firewall está rodando e tráfego de rede em todas as interfaces do Firewall através da interface gráfica remota, em tempo real e em forma tabular e gráfica.

5.19.7. Permitir a conexão simultânea de vários administradores, sendo um deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas. Permitir que o segundo ao se conectar possa enviar uma mensagem ao primeiro através da interface de administração.

5.19.8. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (*em caso de existência de um filtro de conteúdo Web*), maiores emissores e receptores de e-mail.

5.19.9. Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML: máquinas acessadas X serviços bloqueados, usuários X URLs acessadas, usuários X categorias Web bloqueadas (*em caso de utilização de um filtro de conteúdo Web*).

5.19.10. Possibilitar a geração dos relatórios sob demanda e através de agendamento diário, semanal e mensal. No caso de agendamento, os relatórios deverão ser publicados de forma automática em pelo menos três servidores web diferentes, através do protocolo FTP.

5.20. **LOG**

5.20.1. Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo.

5.20.2. Prover mecanismo de consulta às informações registradas integrado à interface de administração.

5.20.3. Possibilitar o armazenamento de seus registros (*log e/ou eventos*) na mesma plataforma de gerenciamento.

5.20.4. Possibilitar a recuperação dos registros de log e/ou eventos armazenados em máquina remota, através de protocolo criptografado, de forma transparente através da interface gráfica.

5.20.5. Possibilitar a análise dos seus registros (*log e/ou eventos*) por pelo menos um programa analisador de log disponível no mercado.

5.20.6. Possuir sistema de respostas automáticas que possibilite alertar imediatamente o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de Traps SNMP.

5.20.7. Possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (*sniffer*) via interface gráfica, podendo opcionalmente exportar os dados visualizados para arquivo formato PCAP e permitindo a filtragem dos pacotes por protocolo, endereço IP origem e/ou destino e porta IP origem e/ou destino, usando uma linguagem textual.

5.20.8. Permitir a visualização do tráfego de rede em tempo real tanto nas interfaces de rede do Firewall quando nos pontos internos do mesmo: anterior e posterior à filtragem de pacotes, onde o efeito do NAT (*tradução de endereços*) é eliminado.

5.21. **TREINAMENTO**

5.21.1. A CONTRATADA deverá capacitar tecnicamente a equipe que irá gerenciar a solução na CONTRATANTE em todas as funcionalidades exigidas.

5.21.2. O treinamento deverá ser ministrado por técnico certificado da empresa fabricante do equipamento.

5.21.3. A CONTRATANTE poderá durante o tempo do contrato solicitar novos treinamentos sempre que julgar necessário, sem nenhum custo adicional.

5.21.4. Todo material necessário para o treinamento, caso necessário, deverá ser fornecido pela CONTRATADA.

5.22. **RELATÓRIOS**

5.22.1. A solução deverá possuir sistema de relatório próprio fornecido pelo fabricante na plataforma Windows, VMware ou Cloud.

5.22.2. Caso a solução de relatórios seja fornecida em nuvem, o armazenamento deverá ser de no mínimo 3 meses de dados.

5.22.3. Fornecer gerência remota do sistema de relatórios, com interface gráfica nativa.

5.22.4. A interface gráfica deverá possuir mecanismo que permita a gerência e emissão de relatórios de forma remota de múltiplos firewalls.

5.22.5. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML, PDF e CSV: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web), maiores emissores e receptores de e-mail, detecção de intrusos, intrusos bloqueados e alvos, para vírus e spywares bloqueados, alvos e detectados.

5.22.6. Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML: máquinas acessadas X serviços bloqueados, usuários X URLs acessadas, usuários X categorias Web bloqueadas (em caso de utilização de um filtro de conteúdo Web).

5.22.7. Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo.

5.22.8. Possibilitar o armazenamento de seus registros (log e/ou eventos) na mesma plataforma de gerenciamento.

5.22.9. Possibilitar a recuperação dos registros de log e/ou eventos armazenados em máquina remota, através de protocolo criptografado, de forma transparente através da interface gráfica.

5.22.10. Possibilitar a análise dos seus registros (log e/ou eventos) por pelo menos um programa analisador de log disponível no mercado.

5.22.11. Possuir sistema de respostas automáticas que possibilite alertar imediatamente o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de Traps SNMP.

5.23. **SUPORTE ESPECIALISTA SOLUÇÃO DE ACTIVE DIRECTORY (*AD*)**

5.23.1. Instalação, configuração de um Active Directory (*AD*) em um Servidor Windows.

5.24. **INSTALAÇÃO DE SERVIDORES**

5.24.1. Instalação de Service Pack e fixes que se façam necessários no servidor Windows;
5.24.2. Configuração do servidor, observando critérios de segurança e performance;
5.24.3. Criação e Configuração de Active Directory, seguindo padronização de segurança;
5.24.4. Promoção dos servidores para Controladores de Domínio (*Domain Controllers*).

5.25. **ACTIVE DIRECTORY**

5.25.1. Criação de estrutura do Active Directory, contemplando Unidades Organizacionais (*OU's*) de forma a atender às necessidades do cliente, no que se refere às futuras aplicações de políticas através de GPO;
5.25.2. Configuração de replicação das configurações entre os Domain Controllers;
5.25.3. Cadastramento de usuários com scripts contendo instruções básicas de logon;
5.25.4. Criação de subnet referente ao(s) site(s) do cliente;
5.25.5. Testes de replicações entre servidores Domain Controllers da rede (*dois sentidos*).

5.26. **DNS**

5.26.1. Instalação do serviço DNS nos servidores Domain Controllers da rede corporativa;
5.26.2. Criação e configuração de zona integrada ao Active Directory;
5.26.3. Criação de Zona reversa para domínio criado.

5.27. **GROUP POLICY OBJECTS (GPO)**

5.27.1. É altamente aconselhável a abordagem de GPO`s em domínios com Active Directory, visto que os benefícios são inúmeros, no sentido de proporcionar segurança e padronização do ambiente computacional de uma empresa.

5.27.2. O objetivo principal da GPO é manter o ambiente computacional da empresa de forma mais homogênea possível, através da utilização de *templates* já previamente definidos, possibilitando uma administração mais segura e eficaz dos computadores constantes em rede.

5.27.3. Ativação de Acesso Remoto às estações de trabalho, através de ferramenta nativa;
5.27.4. Padronização de armazenamento da pasta Meus Documentos, utilizando a opção FOLDER REDIRECTORY;
5.27.5. Mensagem de aviso referente à utilização de recursos da rede corporativa;
5.27.6. Padronização de papel de parede nas estações de trabalho da rede coorporativa;
5.27.7. Padronização de proteção de tela nas estações de trabalho da rede coorporativa;
5.27.8. Padronização de usuários com direitos administrativos nas estações de trabalho;
5.27.9. Configuração do serviço de Atualizações Automáticas para servidor WSUS;
5.27.10. Padronização das seguintes configurações do Internet Explorer:
5.27.11. Definição de página inicial;
5.27.12. Limpeza de *Temporary Internet Files* após fechamento do mesmo;
5.27.13. Limpeza das configurações de detecção automática de proxy;
5.27.14. Desativar armazenamento automático de senhas no Internet Explorer;
5.27.15. Definição de Políticas de senhas para Usuários e Administradores da rede:
5.27.16. Padronização da senha do usuário ADMINISTRADOR nas estações de trabalho;

5.28. **SERVIDOR DHCP**

5.28.1. Permitir a configuração automática das interfaces de rede dos equipamentos da prefeitura, facilitando e tornando mais segura a configuração de rede destes (*computadores, smarphones, impressoras, cameras, etc*).
5.28.2. Permitir fixar os IP's de acordo com o mac address (*endereço único da interface de rede*) de cada dispositivo.
5.28.3. Servidor de envio de e-mails (*SMTP*) com capacidade sup 200 e-mails por dia com anexo.

5.29. **TERMO DE REFERÊNCIA SCAN DE VULNERABILIDADES**

5.29.1. A contratada deverá a cada 6 meses realizar a Varredura de Vulnerabilidades com objetivo de identificar vulnerabilidades que criminosos digitais possam utilizar para causar prejuízos à prefeitura. O criminoso digital pode ser identificado como um agente malicioso que tem conhecimento avançado das tecnologias para espionar, roubar e causar interrupção nos negócios. Ele pode ser um concorrente, funcionário mal-intencionado, cliente ganancioso ou até mesmo um cidadão de outro país que quer utilizar sua rede para ter ganhos financeiros na internet.

5.29.2. Itens a serem verificados:

5.29.2.1. Identificar vulnerabilidades que hackers possam utilizar;
5.29.2.2. Identificar principais alvos (pessoas, servidores e clientes);
5.29.2.3. Identificar falhas no sistema que pode ser explorada por criminosos;
5.29.2.4. Identificar fraudes que podem estar acontecendo;
5.29.2.5. Identificar vazamentos ou roubo de informações;
5.29.2.6. Bloquear ataques futuros e ataques em andamento;
5.29.2.7. Mapear os riscos e avaliar maturidade de segurança cibernética da empresa;

5.29.3. Ao final a contratada deverá fornecer dois relatórios:

5.29.3.1. Sumário Executivo: quantidade de vulnerabilidades encontradas, gravidade das vulnerabilidades, maturidade de segurança cibernética da empresa, atual nível de risco cibernético e possíveis sugestões diante do cenário encontrado;

5.29.3.2. Relatório Técnico: vulnerabilidades encontradas, descrição da vulnerabilidade, solução para correção, classificação de risco, informações adicionais e referências;

5.29.4. Importante: trechos mais técnicos do relatório final podem estar no idioma inglês.

5.29.5. A contratada deverá utilizar pelo menos uma ferramenta comercial de mercado, não sendo aceitos testes utilizando apenas ferramentas gratuitas.

5.30. **SERVIDOR DEDICADO NA NUVEM PARA HOSPEDAGEM DE SITES**

5.30.1. Contração de um Servidor Dedicado na nuvem para hospedagem de site da Prefeitura de Congonhas e hospedagem de um Servidor de mensagens instantânea privativo e gerenciamento de DNS.

5.31. **REQUERIMENTOS**

5.31.1. Sistema Operacional Ubuntu 16.04 LTS.
5.31.2. Servidor Web Apache 2.4 com módulos: MOD-Rewrite, Open SSL, CSPAM, MOD Security.
5.31.3. Linguagem HTML, PHP Versão 8, Perl 5.24.
5.31.4. Banco de dados MySQL 8.0, Postgre 13.4.
5.31.5. Espaço 1 TB com disco SSD.
5.31.6. Memória 16GB.
5.31.7. Processador 4 cores.
5.31.8. Certificado SSL para página Web sem custo de certificação para o Município.
5.31.9. Fazer a hospedagem de domínios virtuais pretendentes ao Município de Congonhas e seus subdomínios na internet.
5.31.10. As páginas podem ser criadas em HTML, APACHE, Java, Perl e PHP.
5.31.11. Permite a atualização das páginas web do site por FTP de forma rápida e segura. Também pode ser usado para troca de arquivos entre empresas.
5.31.12. Possibilitar dar nomes válidos na Internet (*DNS*) e publicado domínio do Município.
5.31.13. Permiti a criação de bases de dados que podem ser consultadas através de comandos SQL.
5.31.14. Banda de 100 MB.
5.31.15. Oferecer Hospedagem *WordPress* gerenciada que estão incluídos a instalação e configuração do *WordPress*.
5.31.16. Antivírus e AntiSpam.
5.31.17. Monitoramento 24x7.

5.31.18. Proteção contra ataques WordPress.
5.31.19. Backups diários e atualização automática do *WordPress*, temas e *plugins*.

5.32. **SUPORTE REMOTO CONTINUADO**

5.32.1. A CONTRATADA deve possuir Central de Atendimento, do tipo (0800) ou número local (DDD 31), para abertura dos chamados de garantia, comprometendo-se a manter registros dos mesmos constando a descrição do problema. A CONTRATADA também deve oferecer canais de comunicação e ferramentas adicionais de suporte online como " chat", "e-mail" e página de suporte técnico na internet com disponibilidade de atualizações e " hotfixes" de drivers, BIOS, firmware, sistemas operacionais e ferramentas de troubleshooting, no mínimo.
5.32.2. Prestar atendimento 8X5 nos dias úteis.
5.32.3. Prestar atendimento em regime de plantão nos feriados e finais de semana das 8:00 as 24:00hs.
5.32.4. A CONTRATADA deve possuir Service Desk próprio permitindo abertura e acompanhamento de chamados técnicos, com atendimento em língua portuguesa e através de atendimento eletrônico via web.
5.32.5. Durante o prazo do contrato celebrado entre as partes a CONTRATADA dará garantia total sem ônus para o CONTRATANTE, a parte ou peça defeituosa, após a conclusão do respectivo analista de atendimento de que há a necessidade de substituir uma peça ou recolocá-la no sistema, salvo se quando o defeito for provocado por uso inadequado dos equipamentos.
5.32.6. Casos em que se tornará obrigatório a substituição de peças ou equipamentos do fabricante, a CONTRATADA será responsável pela retirada, remessa, recolocação e reconfiguração do equipamento, arcando com todas as despesas inerentes ao processo de substituição.
5.32.7. Os Serviços de suporte consistem na disponibilidade do Grupo de especialistas da CONTRATADA via telefone, para prestação de serviços de Suporte Técnico Remoto e aberturas de chamados de 1º, 2º e 3º nível e contempla:

5.32.7.1. Atividade técnica programada, para a realização de Manutenções e correções dos patches de segurança UpGrade e UpDate do ambiente de segurança.
5.32.7.2. Realizar o acompanhamento das atualizações UpDate & Upgrade no período e verificação.
5.32.7.3. Correção de anomalias nos equipamentos Segurança.
5.32.7.4. Solucionar dúvidas quanto à operação dos módulos do Segurança.
5.32.7.5. Atualizações e correções de novos "patches" e versões para os equipamentos.

5.33. **SEGURANÇA**

5.33.1. Suporte Técnico e Substituição ao Hardware que apresentar problema.
5.33.2. A garantia de funcionamento do hardware será fornecida pelo CONTRATANTE, que deverá possuir equipamento backup para substituição imediata.

5.33.3. O atendimento será em regime 8X5, na modalidade on-site, e serão prestados pelo Fabricante ou empresa fornecedora da solução.

5.33.4. O prazo máximo para que se inicie o atendimento técnico será de 04 (*quatro*) horas corridas, contado a partir do momento em que for realizado o chamado técnico devidamente formalizado. Entende-se por início do atendimento técnico inclusive contato telefônico para identificação do tipo de ocorrência afim de preparação de peças adequadas e demais procedimentos técnicos.

5.33.5. O prazo máximo para que seja realizado o reparo do equipamento será de até 24 (*vinte e quatro*) horas corridas para as principais capitais da federação do Brasil, contado a partir do início do atendimento do chamado. Para as demais em até 5 dias úteis.

5.33.6. A manutenção corretiva, que se fará sempre que necessária ou solicitada pela CONTRATANTE, compreende o diagnóstico, assistência técnica e solução de problemas, bem como a substituição de componentes que apresentarem defeitos ou avarias, ou seja, quaisquer serviços que se fizerem necessários para deixar os equipamentos em perfeito estado de funcionamento.

5.33.7. Na manutenção corretiva, após a sua realização, deverão ser feitos testes com os equipamentos, acompanhando o seu funcionamento, pelo técnico em conjunto com o usuário, havendo a obrigatoriedade da assinatura de ambos no documento, ao final dos trabalhos.

5.33.8. Na substituição de algum componente ou periférico, devido à manutenção, este deverá ser compatível com os softwares envolvidos, e com as demais partes do equipamento

5.34. **INSTALAÇÃO E MIGRAÇÃO**

5.34.1. Todo o serviço de instalação e migração da solução atual da Prefeitura de Congonhas será de responsabilidade da CONTRATADA, que deverá realizar visita técnica para propor um cronograma de migração.

5.34.2. A CONTRATADA e a CONTRATANTE deverão elaborar um checklist que será executado após a migração, que será feita em data proposta pela Prefeitura de Congonhas.

6. DOS RECURSOS ORÇAMENTÁRIOS

6.1. Os custos com a presente contratação correrão por conta da(s) seguinte(s) dotação(ões) orçamentária(s):

11.02.04.126.0006.2031.339040

Órgão: 11

Unidade: 02

Função: 04

Sub-função: 126

Programa: 0006

Atividade: 2.031 - Informatização das Atividades Administrativas

339040 - Serviços da Tecnologia da Informação e Comunicação

7. DO PRAZO DE EXECUÇÃO E VIGÊNCIA

7.1. O prazo de execução do objeto será de 12 (doze) meses a contar da assinatura do contrato.

8. DOS REAJUSTES E DO REEQUILÍBRIO

8.1. Os preços contratados poderão ser reajustados, mediante solicitação da CONTRATADA, após o interregno mínimo de 12 (doze) meses, contados da data do orçamento estimado da contratação.

8.2. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o índice IPCA/IBGE exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

8.3. O reajuste será concedido com base na variação efetiva dos custos do contrato no período, devidamente comprovada, observando-se os parâmetros de mercado e os índices oficiais disponíveis que melhor reflitam a variação dos custos envolvidos na execução do objeto.

8.4. Para os reajustes subsequentes, será considerado como termo inicial a data do último reajuste concedido, tomando-se como referência o valor contratual então vigente.

8.5. Na hipótese de inexistência, inaplicabilidade ou inadequação de índices que reflitam fielmente a variação dos custos, poderá ser adotado outro critério que assegure a manutenção do equilíbrio econômico-financeiro do contrato, mediante justificativa técnica.

8.6. O reajuste será formalizado por meio de apostilamento, nos termos da legislação vigente.

9. DOS REQUISITOS DA CONTRATAÇÃO

9.1. Para que o objeto da contratação seja atendido é necessário o atendimento dos requisitos mínimos, dentre eles os de qualidade e capacidade de execução pelo contratado, dispostos nos artigos 62, 66 e 68 da Lei Federal nº. 14.133/2021.

9.2. A dispensa dar-se-á de acordo com os regimes jurídicos estabelecidos na Lei Federal nº. 14.133/2021.

10. DA GARANTIA DO CONTRATO

10.1. Não haverá exigência da garantia da contratação dos artigos 96 e seguintes da Lei Federal nº. 14.133/2021.

11. DA GESTÃO E FISCALIZAÇÃO DO CONTRATO

11.1. A fiscalização decorrente desta contratação, será acompanhada e fiscalizada pelos servidores indicados no item “10.9.” ou pelo respectivo substituto designado, permitida a contratação de terceiros para assisti-los e subsidia-los com informações pertinentes a essa atribuição, nos

termos do artigo 117 da Lei Federal nº. 14.133/2021.

11.2. O fiscal do contrato anotará em registro próprio todas as ocorrências relacionadas à execução do contrato, determinando o que for necessário para a regularização das faltas ou dos defeitos observados.

11.3. O fiscal do contrato informará a seus superiores, em tempo hábil para a adoção das medidas convenientes, a situação que demandar decisão ou providência que ultrapasse sua competência.

11.4. O fiscal do contrato será auxiliado pelos órgãos de assessoramento jurídico e de controle interno da Administração, que deverão dirimir dúvidas e subsidia-lo com informações relevantes para prevenir riscos na execução contratual.

11.5. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos.

11.6. Os gestores dos contratos serão os servidores indicados no item “10.9.” com atribuições administrativas e a função de administrar o contrato, desde sua concepção até a finalização, especialmente:

11.6.1. Analisar a documentação que antecede o pagamento.

11.6.2. Analisar os pedidos de reequilíbrio econômico-financeiro do contrato.

11.6.3. Analisar eventuais alterações contratuais, após ouvido o fiscal do contrato.

11.6.4. Analisar os documentos referentes ao recebimento do objeto contratado.

11.6.5. Acompanhar o desenvolvimento da execução através de relatórios e demais documentos relativos ao objeto contratado.

11.6.6. Decidir provisoriamente a suspensão da entrega de bens ou a realização de serviços.

11.7. O contratado deverá indiciar um responsável legal com respectivos contatos (e-mail, celular e WhatsApp), com poderes para representá-lo perante essa Municipalidade na execução do contrato decorrente da licitação objeto deste termo de referência.

11.8. O contratado deverá manter o preposto aceito pela Administração durante todo o fornecimento do bem para representa-lo na execução do contrato.

11.9. **GESTORES E FISCAIS DOS CONTRATOS:**

11.9.1. O gestor do contrato, será o servidor **Sr. Wanderson Ferreira Leão, Diretor de Tecnologia da Informação, matrícula nº 20146762,** com atribuições administrativas e a função de administrar o contrato, desde sua concepção até a finalização, conforme disposto no Decreto Municipal nº 7.963/2024.

11.9.2. A fiscalização decorrente desta contratação, será acompanhada e fiscalizada pelo servidor **Sr. Clever da Conceição Junior, Gerente de Tecnologia da Informação, matrícula: 20146746,** nos termos do artigo 117 da Lei Federal nº. 14.133/2021, que deverá cumprir o disposto no Decreto Municipal nº 7.963/2024.

12. DOS CRITÉRIOS DE PAGAMENTO

12.1. O pagamento será realizado através de ordem bancária, para crédito em banco, agência e conta corrente indicados pela CONTRATADA.

12.2. O prazo para liquidação da despesa será de 15 (quinze) dias úteis, a contar do atesto da nota fiscal pela Administração.

12.2.1. Para os fins de liquidação, deverá ser observado o disposto no art. 63 da Lei nº 4.320, de 17 de março de 1964, certificando-se do adimplemento da obrigação do contratado nos prazos e forma previstos no contrato.

12.3. O prazo para pagamento, será de 15 (quinze) dias úteis para pagamento, a contar da liquidação da despesa.

12.4. Para as contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021, os prazos serão reduzidos pela metade.

12.5. Estes prazos poderão ser excepcionalmente prorrogados, justificadamente, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

12.6. O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não serão computados no prazo fixado.

12.7. Na hipótese de caso fortuito ou força maior que impeça a liquidação ou o pagamento da despesa, o prazo para o pagamento será suspenso até a sua regularização, devendo ser mantida a posição da ordem cronológica que a despesa originalmente estava inscrita.

12.8. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021, quais sejam: inscrição no CPF ou no CNPJ; inscrição no cadastro de contribuintes estadual e/ou municipal; regularidade perante a Fazenda federal, estadual e/ou municipal; regularidade relativa à Seguridade Social e ao FGTS; regularidade perante a Justiça do Trabalho; cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal.

12.9. Previamente ao pagamento, a Administração deve verificar a manutenção das condições exigidas para a habilitação na licitação, ou para a qualificação, na contratação direta e

identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, mediante a consultas no CEIS e CNJ, ou outros que lhe sobrevierem.

12.10. A eventual perda das condições de que trata o caput não enseja, por si, retenção de pagamento pela Administração.

12.11. Verificadas quaisquer irregularidades que impeçam o pagamento, a Administração deverá notificar o fornecedor contratado para que regularize a sua situação, no prazo de até 30 (trinta) dias, sem prejuízo do pagamento do montante devido.

12.11.1. A permanência da condição de irregularidade, sem a devida justificativa ou com justificativa não aceita pela Administração, pode culminar em rescisão contratual, sem prejuízo da apuração de responsabilidade e da aplicação de penalidades cabíveis, observado o contraditório e a ampla defesa.

12.12. É facultada a retenção dos créditos decorrente do contrato, até o limite dos prejuízos causado à Administração Pública e das multas aplicadas, nos termos do inciso IV do art. 139 da Lei nº 14.133, de 2021.

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

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

12.14.1. As retenções referentes ao Imposto sobre a Renda serão efetuadas sobre qualquer forma de pagamento, nos termos da Instrução Normativa da Receita Federal do Brasil nº 1.234/2012 e do Decreto Municipal nº 7.609/2023.

12.14.2. Não será efetuado o pagamento de Documento Fiscal emitido em desconformidade com as normas supracitadas.

12.14.3. As pessoas jurídicas amparadas por isenção, não incidência ou alíquota zero devem informar essa condição no documento fiscal, inclusive o enquadramento legal, sob pena de, se não o fizerem, sujeitarem-se à retenção do IR e das contribuições sobre o valor total do documento fiscal, no percentual total correspondente à natureza do bem ou serviço.

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

13. DAS OBRIGAÇÕES DA CONTRATANTE

13.1. A CONTRATANTE obriga-se a:

13.1.1. receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;
13.1.2. verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;
13.1.3. comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;
13.1.4. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado, a saber: Wanderson Ferreira Leão, Diretor de Área (*Tecnologia da Informação*) e Clever da Conceição Júnior, Gerente de Área (*Tecnologia da Informação*).
13.1.5. efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos;
13.2. A Administração não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução do presente Termo de Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

14. DAS OBRIGAÇÕES DA CONTRATADA

14.1. O prazo de entrega dos produtos (*hardware e software*) deverá ser de, no máximo, 30 (trinta) dias corridos após recebimento da nota de empenho com autorização de serviços.
14.2. As despesas de deslocamento, hospedagem e alimentação do(s) técnico(s), a partir da sede da CONTRATADA, serão por conta da CONTRATADA.
14.3. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com os recursos necessários ao perfeito cumprimento das cláusulas contratuais.
14.4. Utilizar empregados habilitados e com conhecimentos dos serviços a serem executados, de conformidade com as normas e determinações em vigor.
14.5. Apresentar à CONTRATANTE, quando for o caso, a relação nominal dos empregados que adentrarão o órgão para a execução do serviço, os quais devem estar devidamente identificados por meio de crachá.
14.6. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à Administração.
14.7. Instruir seus empregados quanto à necessidade de acatar as orientações da Administração, inclusive quanto ao cumprimento das Normas Internas, quando for o caso.
14.8. Não permitir a utilização do trabalho do menor.
14.9. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.
14.10. Não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, as obrigações assumidas, nem subcontratar qualquer das prestações a que está obrigada, exceto nas condições autorizadas no Termo de Referência ou na minuta de contrato.
14.11. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório

para o atendimento ao objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993.

14.12. Suporte técnico para instalação, configuração, migração, atualizações, manutenções (*preventivas, corretivas, evolutivas - ou de upgrade - da solução, sem custos*), gerenciamento e resolução de problemas para toda a plataforma CONTRATADA para as caixas postais com serviço de certificação digital.

14.13. Prestar atendimento 8X5 nos dias úteis.

14.14. Prestar atendimento em regime de plantão nos feriados e finais de semana das 8:00 as 24:00hs.

14.15. A CONTRATADA deverá instalar, ativar e migrar, o serviço no prazo máximo de 10 dias, contados a partir da assinatura do contrato.

14.16. Conforme a severidade da manutenção, deve-se estabelecer prioridades nas entregas e o respeito aos prazos de atendimento e solução do problema, conforme tabela de indicadores.

14.17. No caso de aumento dos requisitos de infraestrutura, deverá ser feita uma especificação desta necessidade, bem como um detalhamento dos riscos deste processo.

14.18. Para as alterações em que existam mudanças em tela ou de procedimentos, deve-se prever um repasse "*hands-on*" ou em outra modalidade a ser acordada, para transferência de tecnologia contemplando instalação, configuração, gerenciamento e resolução de problemas de todos os componentes.

14.19. A CONTRATADA deverá entregar à CONTRATANTE relatório mensal de nível de serviço.

14.20. Nos casos de manutenção corretiva em que houver a necessidade de prazo maior que 24 horas ou dependência de terceiros, esta deverá acordada (*documentada para registro*) e deverá ser acompanhada de cronograma de solução.

14.21. Para toda manutenção corretiva deverá ser fornecido um relatório do diagnóstico do problema e quais medidas corretivas foram adotadas pela CONTRATANTE.

14.22. A equipe ou pessoa que prestará os serviços de suporte deve estar nos quadros da CONTRATADA.

14.23. A CONTRATADA deve possuir Service Desk próprio permitindo abertura e acompanhamento de chamados técnicos, com atendimento em língua portuguesa e através de atendimento eletrônico via web.

14.24. Chamados técnicos ilimitados.

14.25. Suporte remoto para incidentes graves, em até 4 horas úteis.

14.26. Os prazos de atendimento e resolução de manutenção devem seguir os descritos nos indicadores abaixo:

14.26.1.**Indicadores**

Os chamados devem ser categorizados e atendidos de acordo com a prioridade:

PRIORIDADE	TMR	TMPR
CRÍTICA	*15 minutos*	*4 horas*
ALTA	*15 minutos*	*6 horas*

MÉDIA	*15 minutos*	*7 horas*
BAIXA	*15 minutos*	*8 horas*
PLANEJADA	*15 minutos*	-

Legenda:

Sigla	Significado	Detalhamento
MR	*Tempo Médio de Resposta*	*Via telefone em até 3 toques* *Via Web em até 15 minutos*
MPR	*Tempo Médio Para Reparo*	*Tempo para restabelecer/reinstalar um serviço depois de uma falha.*

14.27. Conforme a complexidade da manutenção solicitada deverá ser acordada entre as partes o prazo para a solução avaliando-se a sua extensão e complexidade na solução.

15. DA SUBCONTRATAÇÃO

15.1. Não será admitida a subcontratação.

16. DAS SANÇÕES

16.1. Serão aplicadas ao FORNECEDOR, garantido o contraditório e a ampla defesa, as seguintes penalidades:

16.1.1. Na hipótese de o FORNECEDOR não entregar o objeto contratado no prazo estabelecido neste Termo de Referência, caracterizar-se-á atraso, e será aplicada multa sobre o valor da contratação de:

a) 1% (*um por cento*) até o 5º (*quinto*) dia de atraso;

b) 2% (*dois por cento*) a partir do 6° (*sexto*) dia, aplicável até o 10° (*décimo*) dia de atraso.

16.1.2. O Município de Congonhas a partir do 10º (*décimo*) dia de atraso, poderá recusar a execução do objeto contratado, ocasião na qual será cobrada a multa relativa à recusa e não mais a multa diária por atraso, ante a imaculabilidade da cobrança.

a) Em caso de recusa do objeto contratado aplicar-se-á multa de 10% (*dez*) sobre o valor da contratação.

16.1.3. Caso o FORNECEDOR não atenda aos demais prazos e obrigações constantes no Edital, neste Termo de Referência e no instrumento contratual, aplicar-se-á:

b) Multa de 0,2% (*zero vírgula dois por cento*) por dia, limitada a 10% (*dez por cento*) sobre o valor da contratação.

16.1.4. A multa aplicada em razão de atraso injustificado não impede que a Administração rescinda a contratação e aplique outras sanções previstas em lei.

16.1.5. Nas hipóteses de rescisão unilateral, deve ser aplicada multa de 10% (*dez por cento*) sobre o valor da contratação.

16.1.6. Não deve haver cumulação entre a multa prevista neste artigo e a multa específica prevista para outra inexecução que enseje em rescisão. Nessa hipótese, deve ser aplicada a multa de maior valor.

16.1.7. As multas descritas serão descontadas de pagamentos a serem efetuados ou da garantia, quando houver, ou ainda cobradas administrativamente e, na impossibilidade, judicialmente.

16.1.8. O Município de Congonhas poderá suspender os pagamentos devidos até a conclusão dos processos de aplicação das penalidades.

17. DA DISPOSIÇÃO DE PROTEÇÃO E TRANSMISSÃO DE INFORMAÇÕES

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

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

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

17.4. A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado.

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

17.6. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e

responsabilidades decorrentes da LGPD.

17.7. O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

17.8. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

17.9. O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

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

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

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

18. DA DISPOSIÇÃO ANTICORRUPÇÃO

18.1. É prevista a aplicação da Lei federal nº 12.846, de 1º de agosto de 2013, regulamentada pelo Decreto Municipal n/ 6.826, de 27 de maio de 2019, de acordo com a seguinte clausula:

18.1.1. Na forma da Lei federal n° 12.846/2013, regulamentada pelo Decreto Municipal nº 6.826/2019, para a execução deste contrato, nenhuma das partes poderá oferecer, das ou se comprometer a dar a quem quer que seja, ou aceitar poderá oferecer, dar ou se comprometer a aceitar de quem quer que seja, tanto por contra própria quanto através de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou não financeiras ou benefícios de qualquer espécie que constituam prática ilegal ou de corrupção sob as leis de qualquer pais, seja de forma direta ou indireta quando ao objeto deste instrumento, ou de outra forma que não relacionada a este instrumento, devendo garantir, ainda, que seu prepostos, gestores, fiscais , servidores públicos e colaboradores ajam da forma e observando sempre a legislação pertinente.

19. DAS DISPOSIÇÕES GERAIS

19.1. O Município de Congonhas reserva-se no direito de impugnar a prestação de serviço, se esta

não estiver de acordo com as especificações contidas neste Termo de Referência.

19.2. Os casos omissos serão resolvidos com base nos dispositivos constantes na Lei Federal nº. 14.133/2021.

19.3. Fica eleito o foro da Comarca de Congonhas como único e competente para dirimir quaisquer demandas do presente contrato, por mais privilegiado que outro possa ser.

Congonhas, 28 de abril de 2026.

Douglas V. Maia Dutra
Diretoria de Licitação

APROVO o presente Termo de referência, cuja finalidade é subsidiar a contratação de todas as informações necessárias ao fornecimento, estando presentes os elementos necessários à identificação do objeto e todos os critérios para contratação de forma clara e concisa, além de cumprir com o determinado na legislação.

Congonhas, 28 de abril de 2026.

Ana Falvia Matias Araujo Silva
Secretaria Adjunta de Admniatração

B | NoPaper

Data de criação do documento: 28/04/2026 às 06:56:16

Assinantes

✓ ANA FLAVIA MATIAS ARAUJO SILVA

Assinou em 28/04/2026 às 08:30:31 com o certificado avançado da Betha Sistemas e possui a identidade verificada com o CPF ***.844.946-**

Eu, ANA FLAVIA MATIAS ARAUJO SILVA, estou ciente das normas descritas na Lei nº 14.063/2020, no que se refere aos tipos de assinaturas consideradas como válidas para a prática de atos e interações pelos Entes Públicos.

✓ Douglas Vinicius Maia Dutra

Assinou em 28/04/2026 às 08:30:32 com o certificado avançado da Betha Sistemas e possui a identidade verificada com o CPF ***.648.316-**

Eu, Douglas Vinicius Maia Dutra, estou ciente das normas descritas na Lei nº 14.063/2020, no que se refere aos tipos de assinaturas consideradas como válidas para a prática de atos e interações pelos Entes Públicos.

Veracidade do documento

Documento assinado digitalmente.
Verifique a veracidade utilizando o QR Code ao lado ou acesse o site **verificador-assinaturas.plataforma.betha.cloud** e insira o código abaixo:

KZV **K2L** **R0Z** **2N9**