



CONTRATAÇÃO(Nº da UASG – Nº no Portal Compras Governamentais):
929630 - 13/2026

PROCESSO LICITATÓRIO Nº 022/2026
PREGÃO ELETRÔNICO Nº 011/2026

CONTRATANTE: CÂMARA MUNICIPAL DE DIVINÓPOLIS –
UASG 929630

OBJETO: Contratação de solução integrada de segurança de rede do tipo Firewall de Próxima Geração (NGFW/UTM), em regime de locação com cessão de uso/comodato do appliance, incluindo fornecimento do appliance, subscrição/licenciamento durante toda a vigência contratual, suporte técnico oficial da solução, atualização tecnológica e garantia de continuidade operacional e treinamento técnico para transferência de conhecimento à equipe de Tecnologia da Informação da Câmara Municipal de Divinópolis/MG.

Observação: Havendo divergência do descritivo do item cadastrado no Portal Comprasnet com o do Edital, prevalecerá o descritivo do Edital.

VALOR TOTAL DA CONTRATAÇÃO (ESTIMADO): R\$ 102.177,96 (cem e dois mil, cento e setenta e sete reais e noventa e seis centavos).

DATA E HORÁRIO DO RECEBIMENTO DAS PROPOSTAS: até às 14 (quatorze) horas do dia 11/11/2026

DATA DA SESSÃO PÚBLICA: Dia 11/11/2026 às 14h (horário de Brasília)

CRITÉRIO DE JULGAMENTO: Menor Preço Global

MODO DE DISPUTA: Aberto e fechado.

PREFERENCIAL ME/EPP/EQUIPARADAS: SIM.

PLATAFORMA DE COMPRAS DO GOVERNO FEDERAL: www.comprasnet.gov.br



Sumário

1. DO OBJETO.....	3
2. DA PARTICIPAÇÃO NA LICITAÇÃO.....	14
3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO.....	17
4. DO PREENCHIMENTO DA PROPOSTA.....	19
5. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES.....	20
6. DA FASE DE JULGAMENTO.....	25
7. DA FASE DE HABILITAÇÃO.....	28
8. DOS RECURSOS.....	38
9. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES.....	40
10. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO.....	44
11. DAS DISPOSIÇÕES GERAIS.....	45

**CÂMARA MUNICIPAL DE DIVINÓPOLIS****PREGÃO ELETRÔNICO Nº 011/2026**

(Processo Administrativo nº 022/2026)

Torna-se público que a CÂMARA MUNICIPAL DE DIVINÓPOLIS, sediada na Rua São Paulo, 277, Centro, CEP 35500.006, Divinópolis/MG, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da Lei nº 14.133, de 1º de abril de 2021, do Decreto Municipal nº 15.995/23 e demais legislações aplicáveis nos termos do Decreto Municipal nº 15.980/23 e, ainda, de acordo com as condições estabelecidas neste Edital.

1. DO OBJETO

1.1. Constitui objeto deste PREGÃO ELETRÔNICO, a contratação de solução integrada de segurança de rede do tipo Firewall de Próxima Geração (NGFW/UTM), em regime de locação com cessão de uso/comodato do appliance, incluindo fornecimento do appliance, subscrição/licenciamento durante toda a vigência contratual, suporte técnico oficial da solução, atualização tecnológica e garantia de continuidade operacional e treinamento técnico para transferência de conhecimento à equipe de Tecnologia da Informação da Câmara Municipal, conforme quantidades, especificações e condições descritas neste Edital e em seus anexos:

Item	Descrição da Solução	Catmat/ Catser	Quant	Unidade	Valor unitário	Valor Total
01	Fornecimento de solução integrada de segurança de rede do tipo Firewall de próxima geração (NGFW), em regime de locação com cessão de uso/comodato do appliance Conforme quantitativos e especificações constantes na tabela item 1.2 e anexo I do Termo de Referência.	27090	12	Mês	R\$ 8.514,83	R\$ 102.177,96
TOTAL MENSAL ESTIMADO						R\$ 8.514,83
TOTAL ANUAL ESTIMADO						R\$ 102.177,96



1.2. O objeto constitui solução única e integrada, correspondente ao Item 01 desta contratação, sendo os componentes descritos na tabela abaixo partes indissociáveis da solução, não constituindo itens autônomos para fins de disputa, julgamento, adjudicação ou contratação. A proposta deverá contemplar integralmente todos os componentes e respectivos quantitativos, licenças, subscrições, funcionalidades, suporte, atualizações e demais recursos necessários ao atendimento dos requisitos e especificações técnicas estabelecidos no Termo de Referência e em seus anexos.

Tabela de composição do Item 01 - Solução Integrada de Firewall NGFW			
Componente	Descrição	Quant	Unid.
Appliance NGFW	Appliance dedicado de Firewall de Próxima Geração – NGFW, novo, em linha de produção atual, disponibilizado em regime de locação com cessão de uso/comodato. O equipamento deverá atender integralmente às especificações mínimas de hardware, capacidade, suficiente para suportar toda a demanda prevista da rede institucional, incluindo sistema operacional/firmware nativo ou homologado, kit de instalação em rack e demais componentes e acessórios necessários ao funcionamento da solução, conforme especificações do Anexo I.	1	Unidade
Licenciamento/ Subscrição de Segurança	Licenciamento, subscrição ou disponibilização integral de todos os recursos de segurança necessários ao appliance NGFW durante toda a vigência contratual, com capacidade técnica e de licenciamento para suportar no mínimo 500 dispositivos, abrangendo, quando aplicável à arquitetura ofertada, IPS, antivírus, antimalware, filtragem de conteúdo, controle de aplicações, inspeção de tráfego, análise comportamental, Inteligência Artificial – IA e/ou Machine Learning, inteligência de ameaças e demais funcionalidades de segurança, conforme especificações anexo I.	1	Conjunto
Conectividade segura/VPN	Licenciamento, habilitação ou disponibilização dos recursos necessários à conectividade segura via VPN IPsec, SSL VPN, VPN baseada em TLS/SSL ou tecnologia equivalente, abrangendo a solução durante toda a vigência contratual. Quando tais funcionalidades forem nativas ou já estiverem abrangidas pelo licenciamento principal da plataforma, não será exigido licenciamento específico adicional, desde que permaneçam integralmente disponíveis.	1	Conjunto
Plataforma de gerenciamento centralizado	Licenciamento, subscrição ou disponibilização da plataforma de gerenciamento centralizado do appliance NGFW, recurso tecnológico integrante da solução ofertada, disponibilizado em nuvem, ambiente local, híbrido ou tecnologia equivalente, válido durante toda a vigência contratual, permitindo o gerenciamento centralizado do appliance, visualização das informações operacionais, geração de alertas e relatórios, backup automático das configurações com retenção mínima de 5 (cinco) versões válidas, gerenciamento de políticas e acompanhamento dos indicadores de saúde operacional da solução.	1	Plataforma
Garantia, suporte oficial e atualização tecnológica	Disponibilização, durante toda a vigência contratual, da documentação técnica oficial, acesso aos recursos e portais oficiais aplicáveis, imagens e atualizações oficiais de firmware/software, licenças e subscrições, garantia, suporte técnico oficial da solução, atendimento aos níveis de serviço previstos neste documento e seus anexos, substituição de hardware quando necessária e mecanismos de atualização tecnológica/Hardware Refresh, inclusive nas hipóteses de descontinuidade, perda de suporte ou incapacidade de atendimento aos requisitos contratados.	1	Serviço



Tabela de composição do Item 01 - Solução Integrada de Firewall NGFW			
Treinamento e transferência de conhecimento	Treinamento técnico destinado à equipe de Tecnologia da Informação da Câmara Municipal, com carga horária mínima de 8 (oito) horas, abrangendo as funcionalidades efetivamente contratadas e observando os requisitos estabelecidos no anexo I deste documento.	1	Serviço

1.3. Todos os equipamentos e componentes físicos fornecidos para composição da solução deverão ser entregues em estado de novo e sem uso anterior, sendo vedado o fornecimento de equipamentos ou componentes reconicionados, remanufaturados ou refurbished. O appliance de Firewall NGFW deverá, adicionalmente, corresponder a modelos integrantes da linha atual do fabricante e regularmente comercializados na data da entrega, observadas as condições de conformidade e ciclo de vida estabelecidas no item 1.4 deste Edital.

1.4. Não serão aceitos softwares ou firmwares em versões beta, experimentais ou não oficiais, nem appliance que, na data da entrega, tenha atingido os marcos de End-of-Life (EOL), End-of-Sale (EOS) ou End-of-Support (EOSP), conforme as definições e informações oficiais do fabricante, devendo o equipamento permanecer em linha de comercialização regular, com suporte técnico e atualizações oficiais disponíveis, observadas as exigências de continuidade tecnológica estabelecidas no Termo de Referência.

1.5. Independentemente da origem da solução ofertada, é indispensável que esta disponha de suporte técnico em território nacional, mecanismos compatíveis com políticas de soberania de dados, conformidade com a LGPD e recursos adequados de auditoria, rastreabilidade de acessos e gestão da segurança da informação.

1.6. A contratada deverá garantir a modernização contínua da plataforma sempre que o appliance, sistema operacional, licenciamento ou componente integrante da solução fornecida entrar em processo de descontinuidade, fim de suporte, fim de venda ou fim de vida útil e essa condição comprometer o suporte, a atualização, a segurança, a compatibilidade ou o atendimento aos requisitos contratados, bem como nos casos de incompatibilidade técnica ou incapacidade comprovada de atendimento aos requisitos contratados sem ônus adicional para a Câmara Municipal de Divinópolis.

1.7. As características, funcionalidades, capacidades e especificações técnicas mínimas a serem atendidas pela solução de Firewall de Próxima Geração (NGFW) estão estabelecidas no Anexo I do Termo de Referência.

1.8. Havendo divergência entre a descrição do item constante neste Edital e a descrição do item correspondente no CATMAT/CATSER apresentado no portal COMPRASNET, deverá prevalecer a descrição constante neste Edital.

1.9. A presente contratação caracteriza-se como solução de Tecnologia da Informação e Comunicação – TIC de natureza composta, integrada e comum, compreendendo a disponibilização de 01 (um) appliance de Firewall NGFW em regime de locação com cessão de uso/comodato, licenciamentos e subscrições, suporte técnico, atualização tecnológica e demais recursos e serviços associados previstos no Termo de Referência e em seus anexos. Seus padrões de desempenho e qualidade podem ser objetivamente definidos por meio de especificações usuais de mercado.

1.10. A contratação possui natureza continuada, sem dedicação exclusiva de mão de obra, considerando a



necessidade permanente de disponibilidade da solução, dos licenciamentos, subscrições, atualizações e suporte técnico durante toda a vigência contratual, indispensáveis à manutenção da segurança e da continuidade operacional da rede institucional.

1.11. O objeto desta contratação não se enquadra como sendo bem de luxo, conforme art. 42, II, da Portaria nº 188/23 desta Câmara Municipal.

1.12. Na elaboração da proposta, a licitante deverá identificar e considerar todos os dispositivos, componentes e acessórios específicos da solução ofertada que, conforme as especificações e recomendações do fabricante, sejam necessários à sua adequada instalação e funcionamento, incluindo, quando aplicável, cabos de alimentação, adaptadores, acessórios de montagem, componentes para acesso administrativo local ou recuperação e demais itens necessários. Todos esses componentes deverão estar incluídos na proposta e no preço ofertado, sem ônus adicional para a Contratante, não abrangendo adequações ou ampliações da infraestrutura elétrica predial, cuja disponibilização observará o disposto no item 1.13 deste Edital.

1.13. A Câmara Municipal de Divinópolis disponibilizará a infraestrutura física e elétrica predial necessária à implantação da solução, compatível com as condições do ambiente previamente informadas e com os requisitos desta contratação. Caberá à Contratada fornecer, juntamente com a solução e sem custo adicional posterior, os dispositivos, componentes e acessórios complementares de proteção elétrica que sejam necessários ao perfeito funcionamento dos equipamentos ofertados, conforme previsto no item 1.12 deste Edital.

1.14. A responsabilidade por eventual dano aos equipamentos será apurada de acordo com sua causa e com as obrigações atribuídas a cada parte, observada a existência de nexo entre o fato ocorrido e o dano verificado. A Administração responderá pelas ocorrências comprovadamente decorrentes de falha ou inadequação da infraestrutura física ou elétrica predial sob sua responsabilidade, enquanto a Contratada responderá pelos danos decorrentes de vício, defeito, inadequação ou ausência dos equipamentos, dispositivos de proteção, componentes ou acessórios cujo fornecimento lhe seja atribuído nos termos desta contratação.

Detalhamento básico da solução

1.15. A solução a ser contratada compreenderá uma infraestrutura integrada de proteção, composta pelos seguintes pilares:

1.15.1. **Capacidade Operacional e Continuidade da Solução:** A solução deverá ser composta por 01 (um) appliance dedicado de Firewall NGFW, dimensionado para atender integralmente, de forma individual, à demanda institucional e aos parâmetros mínimos de desempenho estabelecidos no Termo de Referência e em seus anexos. A continuidade operacional da solução será assegurada pela capacidade do equipamento, pelos mecanismos de monitoramento, suporte técnico, contingência, restauração, substituição de hardware e atualização tecnológica previstos na contratação, não sendo exigida redundância física mediante cluster de appliances em Alta Disponibilidade (HA).

1.15.2. **Inteligência de Segurança e Análise Comportamental:** A solução deverá possuir recursos avançados de inspeção profunda de pacotes, análise comportamental, correlação automatizada de eventos e mecanismos de detecção de ameaças, podendo utilizar inteligência artificial (IA), Machine Learning (ML) ou tecnologias funcionalmente equivalentes, permitindo identificar atividades suspeitas, tentativas de exploração, ransomwares e outras ameaças cibernéticas modernas.



1.15.3. Conectividade Inteligente e SD-WAN: O sistema deverá atuar como elemento central de gerenciamento das comunicações da instituição, gerenciando de forma inteligente os links de internet. Através da tecnologia SD-WAN, a solução deverá monitorar constantemente a qualidade das conexões (latência e perda de pacotes), direcionando o tráfego crítico para o melhor link disponível e reduzindo o risco de paralisação dos serviços quando houver enlace alternativo disponível.

1.15.4. Gestão Unificada e Soberania de Dados: Todo o ecossistema de segurança deverá ser gerenciado por meio de painel centralizado, em nuvem, local, híbrido ou solução equivalente, permitindo à equipe de TI monitorar ameaças, usuários, aplicações, VPNs, links de internet, políticas de segurança, alertas e relatórios gerenciais. O ambiente prioriza a conformidade com a LGPD, mantendo trilhas de auditoria e logs detalhados de todas as conexões, assegurando a rastreabilidade necessária à segurança da informação, à auditoria e à governança institucional.

1.15.5. Sustentabilidade Tecnológica (Hardware Refresh): A plataforma de segurança como um todo será amparada por um modelo de contratação que garanta que, durante toda a vigência contratual, o equipamento e os demais componentes da solução estarão atualizados, com suporte técnico do fabricante ou fornecedor autorizado, e com substituição proativa de hardware em caso de descontinuidade de modelos (End-of-Life).

Informações sobre o ambiente atual da Câmara Municipal

1.16. A infraestrutura tecnológica da Câmara Municipal compreende rede corporativa interna, conectividade com a Internet, rede sem fio corporativa composta por 24 (vinte e quatro) pontos de acesso (APs) e interligação corporativa entre a sede, localizada na Rua São Paulo, nº 277, Centro, Divinópolis/MG, e o prédio anexo, localizado na Rua Antônio Olímpio de Moraes, nº 545, Centro, Divinópolis/MG.

A solução de Firewall NGFW deverá ser compatível com esse ambiente, permitindo o gerenciamento dos links de Internet, a redundância operacional dos links, o balanceamento de tráfego, o controle e a aplicação de políticas de segurança sobre o tráfego da rede interna e da rede Wi-Fi, bem como a integração com a interligação corporativa entre a sede e o prédio anexo. Quando tecnicamente aplicável à arquitetura adotada, deverá permitir a utilização de VPN ou mecanismo equivalente para proteção da comunicação.

Os elementos descritos neste item possuem caráter informativo quanto ao ambiente tecnológico no qual a solução será utilizada, devendo os requisitos funcionais, capacidades e especificações técnicas mínimas da solução observar o disposto no item 1.15 e no Anexo I do Termo de Referência.

1.17. O ambiente atual possui aproximadamente:

1.17.1. Rede interna cabeada com capacidade operacional estimada em 300 Mbps Full Duplex;

1.17.2. Infraestrutura de rede sem fio (Wi-Fi) com utilização aproximada de 100 Mbps Full Duplex;

1.17.3. Ambiente de acesso remoto e VPN com consumo estimado em 70 Mbps Full Duplex.

1.18. Atualmente, a infraestrutura de conectividade da Câmara Municipal opera com 3 (três) links de internet ativos. Está prevista, no âmbito de contratação correlata específica de conectividade, a substituição dessa infraestrutura por 2 (dois) links dedicados com capacidade mínima de 1 Gbps Full Duplex, destinados a proporcionar redundância operacional e balanceamento de tráfego, bem como interligação corporativa dedicada entre a sede e o prédio anexo. A solução de Firewall NGFW objeto deste Edital deverá ser compatível com essa arquitetura de conectividade, permitindo o gerenciamento dos links e a aplicação das políticas de segurança pertinentes, sem que o fornecimento dos links de internet ou da interligação corporativa Sede-Anexo integre o objeto desta contratação.



1.19. O suporte a DNS Dinâmico (DDNS) constitui funcionalidade técnica integrante da solução de Firewall NGFW, não caracterizando componente ou item autônomo para fins de disputa ou adjudicação. A solução deverá disponibilizar suporte à atualização automática de registros DNS associados a interfaces ou serviços cujos endereços IP possam sofrer alterações, quando aplicável à arquitetura de conectividade implantada, de forma a preservar a resolução de nomes e a continuidade de acesso aos serviços dependentes dessa funcionalidade. A utilização efetiva do recurso ficará condicionada às necessidades operacionais e às características dos enlaces de comunicação utilizados pela Câmara Municipal.

Sustentabilidade

1.20. A Contratada deverá observar os parâmetros de sustentabilidade disponibilizados no itens 4.6. a 4.6.7. do Termo de Referência, anexo a este edital.

Vistoria das instalações

1.21. Para o correto dimensionamento e elaboração de sua proposta, o licitante poderá realizar, se necessário, vistoria nas instalações da Câmara, acompanhado por servidor designado para esse fim, de segunda a sexta-feira, das 12h às 18h, devendo o agendamento ser previamente realizado pelo e-mail: compras@divinopolis.mg.leg.br;

1.22. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até o dia útil anterior à data prevista para a abertura da sessão pública;

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

1.24. A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo a licitante vencedora assumir os ônus das situações decorrentes da ausência de verificação;

1.25. A licitante deverá declarar que realizou a vistoria e tomou conhecimento de todas as informações e condições locais para o cumprimento das obrigações objeto da licitação ou declaração de que não realizou a vistoria e entende conhecer todos os elementos suficientes para o correto dimensionamento dos serviços a serem prestados.

Modelo de Execução do Objeto

Dos prazos e local de entrega dos equipamentos

1.26. A Contratada deverá entregar o equipamento na sede da Câmara Municipal de Divinópolis/MG, situada à Rua São Paulo, 277, Centro, Divinópolis/MG, devidamente acompanhado dos componentes, acessórios e documentação técnica previstos no Termo de Referência, bem como disponibilizar as respectivas licenças, subscrições e demais recursos necessários à posterior implantação da solução. A obrigação da Contratada deste Edital, nesta etapa, limita-se ao fornecimento e à disponibilização dos elementos integrantes da solução sob sua responsabilidade. A instalação física, configuração lógica, migração, integração, testes e homologação serão executados pela empresa responsável pela contratação correlata de serviços especializados, conforme disposto no item 1.27.

1.26.1. Após a entrega, o equipamento será inspecionado por servidor designado da Diretoria de Informática e T.I. para conferência com as especificações estabelecidas no Termo de Referência. Em caso



de desconformidade atribuível ao fornecimento, a Contratada será notificada para efetuar a substituição no prazo máximo de 03 (três) dias úteis, contado da respectiva notificação.

1.26.2. O equipamento deverá ser entregue exclusivamente durante o horário de funcionamento da Câmara Municipal de Divinópolis, em dias úteis e das 12 h às 18:00 h.

1.26.3. O prazo para entrega do appliance, disponibilização das licenças e subscrições, documentação técnica e demais componentes necessários à posterior implantação da solução será de até 20 (vinte) dias úteis, contado da notificação da Contratada pela Contratante, mediante emissão da respectiva Solicitação de Serviço.

Da transferência de conhecimento e realização de treinamento

1.26.4. O treinamento técnico será destinado à equipe de Tecnologia da Informação da Câmara Municipal, com o objetivo de proporcionar conhecimento prévio da ferramenta, promover o nivelamento técnico e desenvolver a capacidade de acompanhamento e interlocução sobre a solução fornecida.

1.26.5. O treinamento deverá possuir carga horária mínima de 8 (oito) horas, podendo ser estendida, caso necessário, para assegurar a abordagem integral do conteúdo programático previsto no Anexo I do Termo de Referência. O treinamento poderá ser realizado de forma presencial, remota ou híbrida, ou por meio de cursos em videoaulas, desde que sejam asseguradas condições adequadas para a efetiva transferência de conhecimento.

1.26.5.1. O conteúdo programático possui caráter de capacitação técnica e transferência de conhecimento, não implicando transferência à equipe da Câmara Municipal das responsabilidades de administração, configuração, monitoramento ou sustentação operacional continuada da solução, atribuídas à empresa responsável pela contratação específica dos serviços especializados correlatos.

1.26.6. O treinamento poderá ser ministrado pelo fabricante, parceiro autorizado ou fornecedor da solução, desde que o instrutor possua conhecimento técnico compatível com a solução ofertada, comprovado por certificação emitida pelo fabricante, habilitação técnica equivalente ou experiência profissional compatível na solução ofertada.

1.26.7. Ao término do treinamento, deverá ser disponibilizado material didático, documentação técnica ou conteúdo equivalente utilizado durante a capacitação, em formato digital, bem como emitido certificado, declaração ou documento equivalente que comprove sua realização.

Da implantação e configuração inicial da solução de Firewall NGFW

1.27. A implantação física, a configuração lógica, a migração, a integração com os ambientes existentes, a orientação operacional relacionada ao ambiente implantado, os testes, a homologação e os demais serviços especializados necessários à implantação e configuração da solução **não fazem parte do objeto desta contratação**, sendo de responsabilidade de empresa contratada especificamente para a prestação desses serviços.

1.27.1. A atuação dessa empresa não eximirá a Contratada de suas responsabilidades contratuais, nem impedirá o seu acionamento direto pela Administração, permanecendo integralmente responsável pelo atendimento, pelo suporte técnico e pelo cumprimento dos níveis de serviço estabelecidos nesta contratação, no que se refere às obrigações que lhe competem.



1.28. À empresa fornecedora do appliance e dos demais componentes da solução caberá, no âmbito desta contratação, a disponibilização da documentação técnica oficial da solução ofertada, o acesso aos portais do fabricante, quando aplicável, o fornecimento dos licenciamentos, imagens oficiais de firmware e respectivas atualizações, o suporte técnico do fabricante ou de parceiro autorizado, bem como a prestação das informações técnicas necessárias à implantação da solução e o apoio técnico à empresa responsável pela implantação e configuração, sempre que necessário.

Do suporte técnico e Acordo de Nível de Serviço (SLA)

1.29. A Contratada deverá disponibilizar suporte técnico sem custo adicional para a Contratante, com a finalidade de esclarecimento de dúvidas acerca da solução ofertada ou abertura de chamados técnicos.

1.29.1. Para os incidentes classificados como Críticos, o atendimento deverá estar disponível em regime 24x7, com contagem ininterrupta dos respectivos prazos de resposta e restabelecimento.

1.29.2. O suporte técnico deverá ser prestado por meio de chat, telefone, e-mail ou canais equivalentes, com atendimento por profissional humano especializado, em língua portuguesa.

1.29.3. O suporte deverá possibilitar escalonamento e atendimento por profissionais especializados em áreas específicas sempre que necessário à resolução de incidentes críticos ou complexos.

1.30. A Contratada deverá disponibilizar, adicionalmente, canal ou ferramenta para abertura, registro, acompanhamento e consulta dos chamados, podendo ser utilizado sistema WEB, e-mail, software específico ou outra solução tecnológica adequada, de forma a permitir à Contratante o adequado acompanhamento das solicitações e de seu respectivo andamento.

1.31. Os chamados deverão ser recebidos e tratados por equipe técnica especializada da Contratada, que deverá adotar postura proativa e iniciar imediatamente as providências necessárias para identificação, diagnóstico e correção das falhas, mediante atendimento remoto ou, quando tecnicamente necessário, mediante o envio de equipe técnica presencial à Sede da Câmara.

1.31.1. A Contratada deverá assegurar, durante toda a vigência contratual, capacidade de atendimento técnico presencial no Município de Divinópolis/MG, sempre que a natureza da ocorrência exigir intervenção física relacionada às obrigações do fornecimento da solução, especialmente em situações envolvendo falha de hardware, necessidade de substituição de equipamento ou outra providência que não possa ser solucionada exclusivamente por atendimento remoto.

1.31.2. A capacidade de atendimento presencial poderá ser disponibilizada por equipe própria da Contratada ou por empresa, parceiro técnico ou prestador de serviços formalmente vinculado à Contratada, desde que possua qualificação compatível com a solução ofertada e condições de atendimento que permitam o cumprimento dos prazos estabelecidos nos Acordos de Nível de Serviço – SLA.

1.31.3. A Contratada deverá comprovar essa capacidade antes do início da execução contratual, mediante contrato, instrumento de parceria, declaração de disponibilidade, acordo de prestação de serviços ou documento equivalente que demonstre a efetiva disponibilidade da estrutura de atendimento.

1.31.4. Não será exigida sede, filial ou estabelecimento da Contratada no Município de Divinópolis, sendo suficiente a demonstração de estrutura própria ou de terceiro que permita o atendimento presencial dentro dos prazos contratuais.



1.32. A Contratada deverá manter sistema de controle e registro de chamados, acessível à Contratante, que permita a abertura, o acompanhamento e a consulta das solicitações, mantendo histórico das ocorrências, respectivas datas, providências adotadas e soluções apresentadas.

1.33. O suporte técnico deverá ser prestado conforme a criticidade dos incidentes ou solicitações, observando os tempos máximos de resposta e restabelecimento definidos na tabela abaixo, sendo aplicável aos incidentes classificados como Críticos o regime de atendimento contínuo previsto no item 1.29.1.

Criticidade	Descrição	Tempo Máximo de Resposta	Tempo Máximo para Restabelecimento
Crítica	Indisponibilidade total do appliance NGFW ou da solução decorrente de falha de hardware, firmware, licenciamento, subscrição ou funcionalidade nativa da plataforma, bem como comprometimento grave de segurança decorrente de falha nativa da solução.	30 minutos	24 horas corridas
Alta	Degradação severa de desempenho ou falha parcial de serviços essenciais do appliance NGFW ou da solução, decorrente de falha de hardware, firmware, licenciamento, subscrição ou funcionalidade nativa da plataforma, ou comprometimento relevante de segurança atribuível ao produto, sem caracterizar indisponibilidade total.	1 hora	16 horas úteis
Média	Falhas em funcionalidades nativas da plataforma, firmware, relatórios, licenciamento ou subscrições, ou depreciação moderada atribuível ao produto sem interrupção total dos serviços.	4 horas	24 horas úteis
Baixa	Solicitações administrativas relacionadas a licenciamento, subscrições, garantia ou suporte oficial, dúvidas técnicas sobre funcionalidades nativas ou demandas vinculadas ao produto sem impacto significativo na continuidade operacional.	8 horas	48 horas úteis

1.34. Os prazos de resposta e restabelecimento previstos no item 1.33 serão contados a partir da abertura formal do chamado junto à Contratada, realizada diretamente pela Administração ou, mediante sua autorização, pela empresa responsável pelos serviços especializados correlatos, observadas as condições de registro e acompanhamento previstas no item 1.32.

1.35. A Contratada deverá estar pronta para atuar com agilidade, mantendo equipe técnica habilitada e qualificada para os serviços, bem como todos os equipamentos, ferramentas e peças de reposição eventualmente necessárias aos atendimentos.

1.36. Nos casos em que for identificada falha física de hardware que comprometa total ou parcialmente a operação da solução, a Contratada deverá adotar imediatamente todas as medidas tecnicamente necessárias ao restabelecimento da solução dentro do SLA definido para a criticidade do incidente, empregando, conforme tecnicamente adequado à ocorrência, contingência temporária, appliance substituto, equipamento reserva ou solução técnica equivalente. Quando necessária a substituição física definitiva do equipamento, esta deverá ocorrer no prazo máximo de 2 (dois) dias úteis, por equipamento de capacidade igual ou superior, sem comprometer os tempos máximos de restabelecimento previstos no item 1.33.

Dos dados armazenados e segurança da informação

1.37. A contratada e seus profissionais deverão respeitar a Política de Segurança da Informação da Câmara Municipal de Divinópolis, bem como as demais normas aplicáveis a tratamento de dados e segurança da informação.



1.38. Todas as informações obtidas pela Contratada em razão da execução contratual deverão ser tratadas como confidenciais, incluindo, entre outras, dados, documentos, topologia de rede, configurações, regras de firewall, vulnerabilidades identificadas, credenciais, informações de endereçamento, registros de eventos, logs e demais informações técnicas ou institucionais relacionadas à infraestrutura da Câmara Municipal. É vedada sua reprodução, utilização, compartilhamento ou divulgação para finalidade diversa da execução do contrato, salvo mediante autorização expressa da Administração ou quando decorrente de obrigação legal, devendo ser observadas as disposições da Constituição Federal, da Lei nº 14.133/2021, da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) e das demais normas aplicáveis.

1.39. A obrigação de sigilo e confidencialidade prevista no item anterior aplica-se à Contratada, a seus representantes, empregados, parceiros, prestadores de serviços e demais terceiros por ela utilizados, permanecendo vigente mesmo após o encerramento ou término da contratação.

1.40. Ao término da vigência contratual, em caso de não renovação, substituição da solução ou encerramento do contrato, a contratada deverá providenciar a retirada do equipamento fornecido em até 15 (quinze) dias úteis, responsabilizando-se pela destinação ambientalmente adequada, descarte ecológico quando aplicável e sanitização segura de dados eventualmente armazenados no equipamento.

Do Backup das Configurações da Solução

1.41. A solução contratada deverá disponibilizar funcionalidade de backup periódico e automatizado das configurações do appliance de firewall, configurável para execução com periodicidade mínima diária, bem como permitir a geração de cópias adicionais sob demanda e a restauração das configurações quando necessária.

1.42. A funcionalidade de backup deverá permitir a retenção de, no mínimo, 5 (cinco) versões válidas das configurações, com identificação das versões existentes e possibilidade de restauração em caso de falha, erro operacional, substituição de equipamento, atualização malsucedida, desastre ou necessidade de reversão.

1.43. A configuração, administração, acompanhamento e validação das rotinas de backup, incluindo a verificação de sua execução, integridade, disponibilidade e retenção, bem como a geração de cópia extraordinária antes de alterações relevantes em regras, VPNs, NAT, SD-WAN, integrações, atualizações de firmware ou outras mudanças com potencial impacto operacional, serão realizadas pela empresa contratada para a prestação dos serviços especializados correlatos, responsável pela administração e sustentação operacional da solução.

1.43.1. A responsabilidade operacional atribuída à empresa contratada para a prestação dos serviços especializados correlatos não afasta a obrigação da Contratada de manter disponíveis, licenciados e plenamente funcionais, durante toda a vigência contratual, os recursos tecnológicos de backup, versionamento e restauração exigidos para a solução.

Obrigações da contratante e da contratada

1.44. As obrigações da contratante e da contratada estão disponibilizadas nos itens 6.1 a 6.2.1.23 do Termo de Referência.

CRITÉRIOS DE MEDIÇÃO E PAGAMENTO



1.45. Para avaliar a qualidade na execução dos serviços, a Contratante utilizará o Instrumento de Medição de Resultados (IMR), conforme modelo previsto no Anexo III do Termo de Referência.

1.46. O IMR verificará a conformidade da execução dos serviços com as exigências estabelecidas no Termo de Referência e a obtenção dos resultados esperados, com base em critérios objetivos previamente definidos pela Câmara.

1.47. Os critérios estabelecidos no IMR servirão como base para a mensuração dos resultados alcançados pela Contratada, impactando diretamente no valor dos pagamentos devidos, bem como podendo fundamentar a aplicação de penalidades, inclusive multas e eventual rescisão contratual, em caso de descumprimento.

Do recebimento

1.48. O recebimento provisório se dará no ato da entrega dos equipamentos e licenças mediante conferência, pela equipe de T.I e fiscal do Contrato, da conformidade dos equipamentos fornecidos às especificações constantes no termo de referência e na proposta realinhada.

1.49. Constatada qualquer irregularidade, desconformidade ou pendência, a Contratada será formalmente comunicada para que proceda à respectiva correção ou substituição, sem prejuízo da aplicação das medidas e sanções cabíveis.

1.50. O recebimento definitivo ficará condicionado à verificação da conformidade do appliance NGFW e dos demais componentes da solução fornecida, incluindo licenciamentos, subscrições, documentação técnica, acessos oficiais, garantia, suporte técnico e funcionalidades exigidas no Termo de Referência e em seus anexos, mediante conferência documental e verificações técnicas pertinentes às obrigações da Contratada. A conclusão dos serviços de implantação física, configuração lógica, migração, integração, testes e homologação operacional, atribuídos à contratação correlata de serviços especializados, não constituirá condição para o recebimento definitivo deste fornecimento, sem prejuízo da responsabilidade da Contratada por eventuais falhas ou desconformidades dos componentes da solução sob sua responsabilidade.

1.51. Constatadas pendências, falhas ou desconformidades, a Contratada deverá providenciar sua correção no prazo estabelecido pela Contratante, contado da respectiva comunicação, ficando o recebimento definitivo condicionado à comprovação da regularização.

1.52. O recebimento definitivo não afasta a responsabilidade da Contratada pela qualidade, adequação e funcionamento da solução durante toda a vigência contratual.

Do pagamento

1.53. O pagamento será efetuado em moeda corrente nacional, no prazo de até 10 (dez) dias úteis após o recebimento da nota fiscal, através de ordem bancária, para crédito em banco, agência e conta-corrente indicada pela contratada, ou por meio de boleto bancário.

1.54. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, quando couber.

1.55. A empresa regularmente optante pelo Simples Nacional, nos termos da Lei Complementar 123/2006, 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.

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

1.57. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhada 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 14.133/2021.

Vigência do Contrato

1.58. O contrato terá vigência de 12 (doze) meses, contados a partir da assinatura do contrato, podendo ser prorrogado sucessivamente, até a vigência máxima de 10 (dez) anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.

2. DA PARTICIPAÇÃO NA LICITAÇÃO

2.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).

2.1.1. Os interessados deverão atender às condições exigidas no cadastramento no Sicafe até o terceiro dia útil anterior à data prevista para recebimento das propostas.

2.2. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluindo a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

2.3. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou



aqueles se tornem desatualizados.

2.4. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

2.5. Será concedido tratamento favorecido para microempresas e empresas de pequeno porte e para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006.

2.6. Não poderão disputar esta licitação:

2.6.1. aquele que não atenda às condições deste Edital e seu(s) anexo(s);

2.6.2. autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados;

2.6.3. empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários;

2.6.4. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

2.6.5. aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

2.6.6. empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

2.6.7. pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de



trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

2.6.8. agente público do órgão ou entidade licitante;

2.6.9. pessoas jurídicas reunidas em consórcio;

2.6.10. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

2.6.11. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei nº 14.133, de 2021.

2.7. O impedimento de que trata o item 2.6.4 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

2.8. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 2.6.2 e 2.6.3 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

2.9. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

2.10. O disposto nos itens 2.6.2 e 2.6.3 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

2.11. A vedação de que trata o item 2.6.8 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.



3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

3.1. Na presente licitação, a fase de habilitação **sucedará** as fases de apresentação de propostas e lances e de julgamento

3.1.1. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento adotado neste edital, até a data e o horário estabelecidos para abertura da sessão pública.

3.2. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

3.2.1. está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

3.2.2. não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7º, XXXIII, da Constituição;

3.2.3. não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

3.2.4. sendo o caso, cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

3.2.5. O Licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021.

3.3. O Licitante enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa



deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3º da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.

3.4. A falsidade da declaração de que trata os itens 3.2 ou 3.3 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

3.5. Os licitantes poderão retirar ou substituir a proposta anteriormente inserida no sistema, até a abertura da sessão pública.

3.6. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

3.7. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

3.8. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:

3.8.1. a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

3.8.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.

3.9. O valor final mínimo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

3.9.1. valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço.



3.9.2. O valor final mínimo parametrizado na forma do item 3.8 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

3.10. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

3.11. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

3.12. Não cabe às licitantes, após sua abertura, alegação de desconhecimento de seus itens ou reclamação quanto ao seu conteúdo. Antes de elaborar suas propostas, as licitantes deverão ler atentamente o Edital e seus anexos.

4. DO PREENCHIMENTO DA PROPOSTA

4.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

4.1.1. Valor total;

4.1.2. Marca (se for o caso);

4.1.3. Fabricante (se for o caso);

4.1.4. Quantidade cotada (não podendo cotar em quantitativo inferior indicado no Edital);

4.2. Todas as especificações do objeto contidas na proposta vinculam o licitante.



4.3. O licitante não poderá oferecer proposta em quantitativo inferior ao máximo previsto para contratação.

4.4. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

4.5. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

4.6. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

4.7. O prazo de validade da proposta não será inferior a 60 (sessenta) dias, a contar da data de sua apresentação.

4.8. O descumprimento das regras supramencionadas pelos Contratados pode ensejar a responsabilização pelo Tribunal de Contas e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição Federal; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

5. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

5.1. A abertura da presente licitação dar-se-á automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

5.2. Os Licitantes poderão retirar ou substituir a proposta até a abertura da sessão pública.



5.3. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

5.4. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

5.5. . O lance deverá ser ofertado pelo valor global;

5.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital;

5.7. O licitante somente poderá oferecer lance de menor valor ou maior percentual de desconto ao último por ele ofertado e registrado pelo sistema.

5.8. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R\$ 0,10 (dez centavos).

5.9. O Licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

5.10. A etapa de lances da sessão pública será do modo ABERTO E FECHADO, conforme Art. 56, I e II da Lei nº 14.133/2021.

5.11.Os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

5.11.1. A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

5.11.2. Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste



prazo.

5.11.3. No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

5.11.4. Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

5.12. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores ou decrescente de descontos.

5.13. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

5.14. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

5.15. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

5.16. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

5.17. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

5.18. Uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.



5.18.1. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

5.18.2. A melhor classificada nos termos do subitem anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

5.18.3. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

5.18.4. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

5.19. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

5.19.1. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, nesta ordem:

5.19.1.1. disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

5.19.1.2. avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;

5.19.1.3. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

5.19.1.4. desenvolvimento pelo licitante de programa de integridade, conforme orientações



dos órgãos de controle.

5.19.2. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

5.19.2.1. empresas estabelecidas no território do Estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de Município, no território do Estado em que este se localize;

5.19.2.2. empresas brasileiras;

5.19.2.3. empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

5.19.2.4. empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

5.20. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo definido para a Licitação, o pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

5.20.1. Não será admitida a previsão de preços diferentes em razão de local de execução dos serviços ou de qualquer outro motivo.

5.20.2. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

5.20.3. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

5.20.4. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.



5.20.5. O pregoeiro solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

5.20.6. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

5.21. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

6. DA FASE DE JULGAMENTO

6.1. Encerrada a etapa de negociação, o Pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item 2.6 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

6.1.1. SICAF;

6.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/ceis>); e

6.1.3. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/cnep>).

6.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei nº 8.429, de 1992.

6.3. Caso conste na Consulta de Situação do Licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas. (IN nº 3/2018, art. 29, caput)



6.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. (IN nº 3/2018, art. 29, §1º).

6.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação. (IN nº 3/2018, art. 29, §2º).

6.3.3. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

6.4. Caso a licitante provisoriamente classificada em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, a Pregoeira verificará se faz jus ao benefício, em conformidade com os itens 2.5 e 3.3 deste Edital.

6.5. Verificadas as condições de participação e de utilização do tratamento favorecido, a Pregoeira examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no artigo 29 a 35 da IN SEGES nº 73, de 30 de setembro de 2022.

6.6. Será desclassificada a proposta vencedora que:

6.6.1. conter vícios insanáveis;

6.6.2. não obedecer às especificações técnicas contidas no Termo de Referência;

6.6.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

6.6.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

6.6.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.



6.7. Conforme disposto no art 34 da IN SEGES/ME nº 73 de 30 de setembro de 2022, será considerado indício de inexecução as propostas apresentadas com valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

6.7.1. A inexecução, na hipótese de que trata o item 6.7, só será considerada após diligência do pregoeiro, que comprove:

6.7.1.1. que o custo do licitante ultrapassa o valor da proposta; e

6.7.1.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

6.8. Se houver indícios de inexecução da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a execução da proposta.

6.9. Caso o custo global estimado do objeto licitado tenha sido decomposto em seus respectivos custos unitários por meio de Planilha de Custos e Formação de Preços elaborada pela Administração, o Licitante classificado em primeiro lugar será convocado para apresentar Planilha por ele elaborada, com os respectivos valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.

6.10. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço ou diminuição do desconto e que se comprove que este é o bastante para arcar com todos os custos da contratação;

6.10.1. O ajuste de que trata este item se limita a sanar erros ou falhas que não alterem a substância das propostas;

6.11. Considerando as especificidades técnicas do objeto, a Pregoeira solicitará orientação técnica à unidade administrativa competente, aos servidores do setor técnico demandante ou, quando necessário, a profissional especialmente contratado para essa finalidade, a fim de subsidiar a análise das propostas, dos atestados de capacidade técnica, das declarações, da documentação técnica dos fabricantes e dos demais aspectos que exijam conhecimento especializado, inclusive a análise da conformidade técnica da proposta e a conferência da qualificação dos profissionais, sem prejuízo de sua competência para a condução do procedimento licitatório e para a prática dos atos que lhe são legalmente atribuídos.



6.12. O licitante provisoriamente classificado em primeiro lugar deverá apresentar, quando convocado pela Administração, na fase de julgamento da proposta, a documentação técnica oficial do fabricante relativa à solução de Firewall NGFW ofertada, incluindo catálogos, folders, datasheets, fichas técnicas ou outros documentos técnicos oficiais ou equivalentes, conforme previsto no item 9.31 do Termo de Referência, que permitam a verificação objetiva do atendimento às especificações e aos requisitos técnicos exigidos neste Termo de Referência e em seus anexos. A documentação será utilizada para análise da conformidade técnica da proposta, não se confundindo com os documentos de habilitação técnico-operacional da licitante, observados os procedimentos de diligência e eventual demonstração técnica previstos neste instrumento. O não atendimento aos requisitos técnicos mínimos exigidos, após a análise da documentação apresentada e, quando cabíveis, os procedimentos de diligência e demonstração técnica, implicará a desclassificação da proposta, observadas as disposições do Edital e da legislação aplicável.

7. DA FASE DE HABILITAÇÃO

7.1. Os documentos previstos no Termo de Referência, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

7.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

7.2. Os documentos exigidos para fins de habilitação poderão ser apresentados em original ou cópia.

7.3. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133/2021.

7.4. Será verificado se o Licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133/2021).

7.5. Será verificado se o Licitante apresentou no sistema, sob pena de inabilitação, a declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas, quando for o caso.



7.6. O Licitante deverá apresentar, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

7.7. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

7.7.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir. (IN nº 3/2018, art. 4º, §1º, e art. 6º, §4º).

7.8. É de responsabilidade do Licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados. (IN nº 3/2018, art. 7º, caput).

7.8.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

7.9. A verificação pela Pregoeira, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

7.9.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de DUAS HORAS, prorrogável por igual período, contado da solicitação da Pregoeira.

7.10. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao Licitante vencedor.

7.10.1. Os documentos relativos à regularidade fiscal que constem do Termo de Referência somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do Licitante mais bem classificado.

7.11. Após a entrega dos documentos para habilitação, **não** será permitida a substituição ou a apresentação



de novos documentos, salvo em sede de diligência, para (Lei 14.133/21, art. 64, e IN 73/2022, art. 39, §4º):

7.11.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

7.11.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

7.12. Na análise dos documentos de habilitação, a comissão de contratação poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

7.13. Na hipótese de o Licitante não atender às exigências para habilitação, o Pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital, observado o prazo disposto no subitem 7.9.1.

7.14. Somente serão disponibilizados para acesso público os documentos de habilitação do Licitante cuja proposta atenda ao Edital de Licitação, após concluídos os procedimentos de que trata o subitem anterior.

7.15. As microempresas e as empresas de pequeno porte deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal e trabalhista, mesmo que esta apresente alguma restrição.

7.15.1. As microempresas e empresas de pequeno porte deverão apresentar declaração de que, no ano-calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte, conforme previsão no Art. 4º, § 2º da Lei 14.133/2021, conforme anexo.

7.16. Para a habilitação jurídica, serão exigidos:

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



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

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

7.16.4. Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

7.17. Para a habilitação fiscal, social e trabalhista, serão exigidos:

7.17.1. Prova de inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ);

7.17.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria Geral da Fazenda Nacional (PGFN) referente a todos os créditos tributários federais e à dívida ativa da União;

7.17.3. Prova de regularidade com Fundo de Garantia do Tempo de serviço (FGTS);

7.17.4. Prova de inexistência de débitos inadimplentes perante a Justiça do Trabalho, mediante apresentação de certidão negativa ou positiva com efeito de negativa.

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

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

7.17.6. Declaração de que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos



do art. 7º. XXXIII da Constituição Federal.

7.17.7. Para ME e EPP, declaração de que, no ano-calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

7.18. Serão exigidos os seguintes documentos para a comprovação da HABILITAÇÃO TÉCNICA:

7.18.1. Para fins de habilitação técnica, a licitante deverá comprovar aptidão para a execução do objeto desta contratação, mediante apresentação de Atestado de Capacidade Técnica Operacional, expedido por pessoa jurídica de direito público ou privado para a qual tenha fornecido ou disponibilizado solução de segurança de borda do tipo NGFW/UTM ou tecnologia equivalente, contemplando equipamentos ou appliances, licenciamento ou subscrições, garantia, atualização tecnológica e suporte técnico em ambiente corporativo ou institucional de complexidade compatível.

7.18.1.1. Para fins de comprovação da aptidão operacional, os atestados deverão demonstrar experiência na execução dos serviços pelo período mínimo de **1 (um) ano**, não havendo obrigatoriedade de serem ininterruptos.

7.18.1.2. Serão admitidos atestados relativos a soluções de fabricantes distintos daquele ofertado, desde que comprovem experiência em tecnologias e atividades de natureza e complexidade compatíveis com o objeto, não sendo exigida identidade de marca ou fabricante.

7.18.1.3. Será admitida a apresentação de um ou mais atestados complementares, desde que, em conjunto, comprovem a experiência operacional da empresa, as características compatíveis com o objeto da contratação, bem como atendam ao período mínimo de execução estabelecido no item 7.18.1.4.

7.18.1.4. Somente serão aceitos atestados de capacidade técnica expedidos após a conclusão do contrato ou, caso o contrato ainda esteja em execução, desde que tenha decorrido, no mínimo, 1 (um) ano do início de sua execução, salvo se firmado para ser executado em prazo inferior.

7.18.1.5. Os atestados de capacidade técnica deverão conter, no mínimo, a identificação da pessoa jurídica emitente, CNPJ, endereço, identificação do responsável pela emissão, descrição dos serviços prestados, período de execução, local de prestação dos serviços, bem como demais informações necessárias à verificação da compatibilidade com o objeto da contratação.



7.18.1.6. Os atestados deverão ser emitidos em documento formal da contratante, preferencialmente em papel timbrado, ou outro meio idôneo e identificação do emitente, devendo conter assinatura do responsável legal ou de pessoa com poderes para atestar a execução dos serviços.

7.18.1.7. Serão admitidos atestados assinados física ou eletronicamente, desde que seja possível verificar a autoria e a integridade do documento, mediante certificação digital, código de validação, sistema eletrônico de verificação ou outro meio idôneo de conferência.

7.18.1.8. Quando a comprovação da experiência mínima exigida decorrer da apresentação de mais de um atestado, os documentos devem ser apresentados em ordem cronológica, acompanhados, quando necessário, de quadro-resumo indicativo dos períodos, quantitativos e contratantes, a fim de facilitar a análise pela Administração.

7.18.1.9. Sempre que necessário para a adequada verificação da capacidade técnica da licitante, a Administração poderá solicitar a apresentação de outros documentos idôneos relacionados aos atestados apresentados, com a finalidade de complementar ou esclarecer as informações neles constantes.

7.18.1.10. Certificações, credenciamentos ou reconhecimentos emitidos por fabricantes ou desenvolvedores poderão ser apresentados como elementos complementares, não substituindo os atestados de capacidade técnica exigidos para comprovação da capacidade técnico-operacional.

7.18.1.11. Caso haja necessidade, a Administração reserva-se o direito de solicitar a apresentação de cópia da(s) Nota(s) Fiscal(is) correspondentes ao(s) contratos ou Atestado(s) de Capacidade Técnica apresentados.

7.18.1.11.1. É de inteira e exclusiva responsabilidade do licitante, quando da apresentação de contratos, notas fiscais, balanços, declarações ou quaisquer outros documentos destinados a comprovar ou complementar os requisitos de habilitação, promover previamente a ocultação (tarjamento) dos dados pessoais de terceiros alheios à relação jurídica objeto da presente licitação que não sejam necessários à análise da documentação, especialmente números de CPF e RG, assinaturas, endereços residenciais, dados bancários e outras informações pessoais cuja divulgação não seja indispensável à finalidade do procedimento.

7.18.1.11.2. O tarjamento não poderá alcançar informações necessárias à identificação, autenticidade, integridade ou verificação do conteúdo do documento, nem prejudicar a análise dos requisitos de habilitação pela Administração.



7.18.1.11.3. Caso os dados ocultados sejam necessários para esclarecer dúvida, aferir a autenticidade ou integridade do documento, confirmar a veracidade das informações apresentadas ou realizar qualquer outra verificação indispensável à habilitação, a Administração poderá, mediante diligência, solicitar ao licitante a apresentação do documento integral, sem tarjamento.

7.18.1.12. A licitante deverá disponibilizar as informações necessárias à verificação da legitimidade dos atestados apresentados, mediante código de validação, sistema eletrônico de verificação, consulta junto ao emitente ou outro meio idôneo que possibilite à Administração confirmar a autenticidade, a validade e a correspondência das informações constantes do documento.

7.18.2. A licitante deverá comprovar que a solução ofertada é proveniente de cadeia legítima de fornecimento e que dispõe dos meios necessários para assegurar os licenciamentos, subscrições, atualizações, garantia e suporte técnico exigidos durante a vigência contratual. Essa comprovação possui finalidade distinta da qualificação técnico-operacional prevista no item 7.18.1 e não substitui os respectivos atestados de capacidade técnica.

7.18.2.1. A comprovação prevista no item 7.18.2. poderá ser realizada, conforme o modelo comercial, de distribuição ou de suporte adotado pelo fabricante ou desenvolvedor da solução, mediante um ou mais dos seguintes meios:

7.18.2.1.1. Declaração de parceria, certificado de distribuidor, revendedor, integrador, parceiro autorizado ou documento equivalente emitido pelo fabricante, desenvolvedor ou distribuidor oficial da solução;

7.18.2.1.2. Registro ou credenciamento em programa oficial de parceiros, canais, integradores, revendedores, prestadores de serviços ou equivalente;

7.18.2.1.3. Documento emitido pelo fabricante, desenvolvedor, distribuidor oficial ou representante autorizado;

7.18.2.1.4. Consulta a portal, diretório ou sistema oficial do fabricante ou desenvolvedor;

7.18.2.1.5. Documentação de licenciamento, subscrição, garantia, suporte, números de série, direitos de suporte ou instrumentos equivalentes;



7.18.2.1.6. Comprovação de suporte prestado diretamente pelo fabricante ou desenvolvedor; ou

7.18.2.1.7. Outro documento ou mecanismo idôneo e equivalente que demonstre objetivamente a legitimidade do fornecimento e a disponibilidade dos recursos e serviços exigidos.

Da validação técnica da solução ofertada

7.18.3. A validação técnica da solução ofertada terá por finalidade verificar o atendimento aos requisitos mínimos estabelecidos no Termo de Referência, conforme os critérios detalhados no anexo II do TR.

7.18.4. A comprovação do atendimento aos requisitos e às especificações técnicas exigidos para a solução ocorrerá, prioritariamente, mediante a apresentação e análise de documentação técnica oficial do fabricante, a ser apresentada pelo licitante provisoriamente classificado em primeiro lugar, quando convocado pela Administração, na fase de julgamento da proposta, conforme previsto no item 9.5 do Termo de Referência, podendo ser utilizados, isoladamente ou em conjunto, os seguintes documentos, conforme aplicável, desde que permitam a verificação objetiva dos requisitos exigidos:

- a) Datasheets oficiais;
- b) Manuais técnicos;
- c) Guias de administração (Administration Guide);
- d) Guias de instalação;
- e) Guias de arquitetura;
- f) Matrizes oficiais de funcionalidades (Feature Matrix);
- g) Notas técnicas;
- h) Release Notes;
- i) White Papers;
- j) Documentação disponibilizada oficialmente pelo fabricante;
- k) Certificações técnicas;
- l) Declarações oficiais emitidas pelo fabricante ou representante autorizado;
- m) Outros documentos técnicos oficiais ou equivalentes que permitam comprovar objetivamente o atendimento aos requisitos do Termo de Referência e de seus anexos.

7.18.5. Quando a documentação apresentada não permitir comprovação objetiva de determinado requisito técnico exigido ou houver dúvida quanto ao seu atendimento, a Administração realizará diligência destinada exclusivamente ao esclarecimento da informação. A diligência poderá consistir na apresentação de documentação complementar, esclarecimentos técnicos ou demonstração técnica da ferramenta ofertada.



Demonstração técnica da solução apresentada

7.18.6. A demonstração técnica dos requisitos será realizada de forma complementar, somente quando a análise da documentação técnica apresentada pela licitante e a realização de diligência técnica forem insuficientes para comprovar, de forma objetiva, o atendimento de determinado requisito técnico da solução ofertada.

7.18.6.1. A demonstração será limitada às funcionalidades ou requisitos específicos objeto de dúvida, não sendo necessária a demonstração integral da solução, a instalação definitiva dos equipamentos nas dependências da Câmara Municipal ou a reprodução integral de seu ambiente tecnológico.

7.18.7. A Administração especificará previamente quais requisitos serão objeto da demonstração, dentre aqueles apresentados no anexo II, vedada a exigência de funcionalidades, testes ou critérios de avaliação não previstos nos documentos da contratação.

7.18.7.1. A licitante convocada para a demonstração técnica deverá apresentá-la no prazo de até **03 (três) dias úteis**, contado do recebimento da convocação pela Administração.

7.18.8. A Demonstração Técnica poderá ser realizada presencialmente, por videoconferência, mediante compartilhamento de tela, acesso supervisionado a equipamento ou ambiente contendo a solução ofertada, apresentação prática de funcionalidade ou por outro meio tecnicamente adequado, desde que permita à Administração verificar, de maneira objetiva, o atendimento do requisito questionado.

7.18.9. A realização da Demonstração Técnica não implicará qualquer obrigação de fornecimento definitivo da solução, nem constituirá etapa de homologação, aceitação definitiva ou operação assistida, destinando-se exclusivamente à verificação do atendimento dos requisitos previamente estabelecidos.

Critério de avaliação da solução

7.18.10. A avaliação da documentação técnica, da eventual diligência técnica e da demonstração técnica, quando realizada, limitar-se-á à verificação objetiva do atendimento aos requisitos técnicos e funcionais previamente estabelecidos, conforme anexo II, do Termo de Referência, incluindo, conforme aplicável, as características, funcionalidades, capacidades, desempenho, compatibilidade, integração, segurança e mais especificações exigidas para a solução. A análise terá caráter exclusivamente verificatório, não havendo atribuição de pontuação, classificação técnica, comparação de mérito entre fabricantes ou soluções.

7.18.10.1. O resultado da avaliação será registrado, para cada requisito analisado, apenas como: () Atendeu; ou () Não atendeu;

7.18.11. A cada etapa de avaliação técnica realizada, a equipe técnica elaborará relatório devidamente fundamentado, no qual serão registrados os procedimentos adotados e os respectivos resultados. O relatório deverá consignar, quando cabível, a necessidade de realização de diligência técnica e, se necessário a demonstração técnica, bem como as conclusões quanto ao atendimento dos requisitos estabelecidos no Anexo II.

7.18.12. Caso a proponente não atenda aos requisitos estabelecidos nesta contratação para a solução de segurança a ser ofertada o pregoeiro convocará a licitante classificada em seguida para, se considerada habilitada, submeter-se à mesma avaliação técnica. O procedimento será repetido



sucessivamente, respeitando-se a ordem de classificação, até que se identifique a solução de Firewall que atenda integralmente às exigências previstas no Termo de Referência.

Qualificação técnica dos profissionais – Equipe técnica para suporte

7.18.13. A contratada deverá disponibilizar, durante toda a execução contratual, profissional ou equipe tecnicamente qualificada para prestar o suporte técnico relacionado ao appliance, firmwares, softwares, licenças, subscrições, atualizações e demais componentes da solução fornecida.

7.18.14. O profissional ou a equipe disponibilizada deverá possuir qualificação compatível com a tecnologia ofertada e capacidade técnica para realizar, no mínimo:

7.18.14.1. A interlocução técnica com a Câmara e com a empresa responsável pela implantação e administração da solução, quando necessário;

7.18.14.2. O diagnóstico inicial de falhas, indisponibilidades ou comportamentos anômalos relacionados aos componentes da solução contratada;

7.18.14.3. A análise e orientação quanto a problemas relacionados ao appliance, softwares, firmwares, licenças, subscrições e atualizações;

7.18.14.4. A abertura, acompanhamento e escalonamento de chamados junto ao fabricante, desenvolvedor ou estrutura oficial de suporte, quando necessária a atuação especializada; e

7.18.14.5. Acompanhamento das providências necessárias à solução das ocorrências relacionadas ao objeto contratado.

7.18.15. A disponibilização do profissional ou da equipe técnica constitui obrigação da Contratada para a adequada execução do objeto e não será exigida como requisito de habilitação, devendo ser comprovada pela Contratada no momento da assinatura do contrato, mediante certificação emitida pelo fabricante ou desenvolvedor da solução ofertada, por instituição por ele reconhecida, ou por outro meio de comprovação técnica equivalente, desde que demonstre conhecimento e competência compatíveis com as atividades de suporte previstas no Termo de Referência.

7.18.15.1. Serão admitidas certificações com diferentes denominações, níveis ou estruturas, desde que sua abrangência demonstre qualificação compatível com a tecnologia efetivamente ofertada. Não serão consideradas, isoladamente, suficientes as certificações de natureza exclusivamente comercial, de vendas ou meramente introdutória, que não demonstrem capacitação técnica para as atividades de suporte exigidas.

7.18.15.2. Na hipótese de o fabricante ou desenvolvedor da solução não possuir programa formal de certificação individual aplicável à tecnologia ofertada, será admitida comprovação equivalente de capacitação técnica, acompanhada, quando necessário, de comprovação de experiência profissional compatível com as atividades de suporte previstas no Termo de Referência.

7.18.15.3. A qualificação exigida deverá guardar relação direta com o objeto da contratação, não sendo exigida certificação específica de determinado fabricante, modelo ou tecnologia quando houver outras formas objetivamente equivalentes de comprovação da capacidade técnica necessária à prestação do suporte.

Qualificação técnica dos profissionais – Instrutor do Treinamento



7.18.16. A qualificação do instrutor poderá ser comprovada mediante certificação técnica emitida pelo fabricante ou desenvolvedor da solução, por instituição por ele reconhecida, ou por outro meio de comprovação técnica equivalente, desde que demonstre conhecimento compatível com o conteúdo e as atividades de capacitação previstas.

7.18.16.1. A comprovação da qualificação do instrutor deverá ser apresentada pela contratada previamente à execução contratual, no ato da assinatura do contrato, mediante a documentação pertinente, ficando sua apresentação condicionada à verificação pela Administração quanto à compatibilidade da qualificação apresentada com o conteúdo e as atividades de treinamento previstas no termo de referência.

7.18.17. Não será exigida denominação específica de certificação, nível de certificação, categoria de parceria ou vínculo com centro oficial de treinamento do fabricante, desde que a documentação apresentada demonstre, de forma objetiva, a qualificação técnica necessária para a realização do treinamento.

7.18.17.1. Certificações de natureza exclusivamente comercial, de vendas ou meramente introdutória não serão consideradas, isoladamente, suficientes para comprovar a qualificação técnica exigida.

7.18.18. Os documentos apresentados para comprovação da qualificação técnica do instrutor deverão possuir mecanismo de validação ou verificação de autenticidade, mediante código, número de registro, endereço eletrônico, QR Code, sistema de consulta ou outro meio idôneo disponibilizado pelo fabricante, desenvolvedor, instituição certificadora ou entidade responsável pela emissão do documento, de forma a possibilitar à Administração a conferência de sua veracidade.

7.18.19. Quando o documento apresentado não dispuser de mecanismo próprio de validação, a contratada deverá fornecer, juntamente com o documento, os elementos necessários à sua comprovação, tais como declaração da entidade emissora, endereço eletrônico para consulta, identificação do responsável pela emissão ou outro meio documental idôneo que permita à Administração verificar sua autenticidade.

7.19. Qualificação Econômica-Financeira

7.19.1. Certidão negativa de falência expedida pelo distribuidor da sede do licitante (Lei Federal nº 14.133/21, art. 69, caput, II).

8. DOS RECURSOS

8.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133/21.

8.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.



8.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

8.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

8.3.2. o prazo para a manifestação da intenção de recorrer será de 10 (dez) minutos.

8.3.3. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

8.4. Os recursos deverão ser encaminhados em campo próprio do sistema.

8.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

8.6. Os recursos interpostos fora do prazo não serão conhecidos.

8.7. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

8.8. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

8.9. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

8.10. Os autos do processo permanecerão com vista franqueada aos interessados no sítio eletrônico da Câmara Municipal.



9. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

9.1. Comete **infração administrativa**, nos termos deste Edital e de seus anexos, da lei e da Portaria CM nº 060/2025 desta Câmara Municipal, o Licitante que, com **dolo ou culpa**:

9.1.1. Dar causa à inexecução parcial do contrato;

9.1.2. Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

9.1.3. Dar causa à inexecução total do contrato;

9.1.4. Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado.

9.1.5. Deixar de entregar toda a documentação exigida para o certame ou solicitado pela Pregoeira para análise complementar ou entregar documentação em manifesta desconformidade com as exigências do instrumento convocatório;

9.1.6. Salvo em decorrência de fato superveniente devidamente justificado, não manter a proposta, em especial quando:

9.1.6.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

9.1.6.2. recusar-se a enviar o detalhamento da proposta quando exigível;

9.1.6.3. pedir para ser desclassificado quando encerrada a etapa competitiva; ou

9.1.6.4. deixar de apresentar amostra; ou vídeo demonstrativo, quando for o caso;

9.1.6.5. apresentar proposta ou amostra ou vídeo demonstrativo em desacordo com as



especificações do edital;

9.1.6.6. deixar de encaminhar, ou encaminhar em manifesta desconformidade com o instrumento convocatório, as amostras ou vídeos demonstrativos solicitados pela Pregoeira;

9.1.6.7. deixar de atender a convocações da Pregoeira durante o trâmite do certame ou atendê-las de forma insatisfatória;

9.1.6.8. abandonar o certame;

9.1.7. Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

9.1.7.1. recusar-se, sem justificativa, a assinar o contrato, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

9.1.8. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação.

9.1.9. Fraudar a licitação.

9.1.10. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

9.1.10.1. agir em conluio ou em desconformidade com a lei;

9.1.10.2. induzir deliberadamente a erro no julgamento;

9.1.10.3. apresentar amostra falsificada ou deteriorada, quando exigida;

9.1.10.4. apresentar vídeo demonstrativo manipulado, com o objetivo de falsear a verdade, quando exigido;



9.1.11. Praticar atos ilícitos com vistas a frustrar os objetivos da licitação.

9.1.12. Praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

9.2. Com fulcro na Lei nº 14.133/21, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

9.2.1. Advertência;

9.2.2. Multa;

9.2.3. Impedimento de licitar e contratar e

9.2.4. Declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

9.3. Na aplicação das sanções serão considerados:

9.3.1. A natureza e a gravidade da infração cometida.

9.3.2. As peculiaridades do caso concreto

9.3.3. As circunstâncias agravantes ou atenuantes

9.3.4. Os danos que dela provierem para a Administração Pública

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



9.4. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado, recolhida no prazo máximo de 15 (quinze) dias úteis, a contar da comunicação oficial.

9.4.1. Para as infrações previstas nos itens 9.1.5, 9.1.6 e 9.1.7, a multa será de 0,5% a 15% do valor do contrato licitado.

9.4.2. Para as infrações previstas nos itens 9.1.1, 9.1.2, 9.1.3, 9.1.8, 9.1.9, 9.1.10, 9.1.11 e 9.1.12 a multa será de 15% a 30% do valor do contrato licitado.

9.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

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

9.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6 e 9.1.7 quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do Município de Divinópolis/MG, pelos prazos fixados na Portaria CM nº 60/25.

9.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 9.1.8, 9.1.9, 9.1.10, 9.1.11 e 9.1.12, bem como pelas infrações administrativas previstas nos itens 9.1.5, 9.1.6 e 9.1.7 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

9.9. A recusa injustificada do adjudicatário em assinar o contrato, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 9.1.7, caracterizará o **descumprimento total** da obrigação assumida e o sujeitará às penalidades e à **imediata perda da garantia** de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, §4º da IN SEGES/ME n.º 73, de 2022.

9.10. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de



responsabilização a ser conduzido por comissão composta por 3 (três) ou mais servidores estáveis, conforme Portaria CM nº60/2025, que avaliará fatos e circunstâncias conhecidos e intimará o Licitante ou o Adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

9.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

9.12. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

9.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

9.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

10. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

10.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, devendo protocolar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

10.2. A resposta à impugnação ou ao pedido de esclarecimento será divulgado em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

10.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, no e-mail licitacao@divinopolis.mg.leg.br.

10.4. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.



10.4.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo agente de contratação, nos autos do processo de licitação.

10.5. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

11. DAS DISPOSIÇÕES GERAIS

11.1. Será divulgada ata da sessão pública no sistema eletrônico.

11.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

11.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília - DF.

11.4. A homologação do resultado desta licitação não implicará direito à contratação.

11.5. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

11.6. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

11.7. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

11.8. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.



11.9. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

11.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico da Câmara Municipal de Divinópolis (<https://www.divinopolis.mg.leg.br/>).

11.11. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

11.11.1. ANEXO I - Termo de Referência

11.11.1.1. Detalhamento das especificações técnicas da solução;

11.11.1.2. Lista de verificação dos requisitos técnicos para avaliação;

11.11.1.3. Instrumento de medição de resultados (IMR);

11.11.1.4. Modelo para formação de propostas;

11.11.1.5. Declaração de enquadramento no limite de faturamento ME/EPP

11.11.1.6. Apêndice I – Estudo técnico preliminar (ETP)

11.11.2. ANEXO II – Minuta do Contrato.

Divinópolis, 22 de outubro de 2026.

Vereador Israel Mendonça

Presidente da Câmara Municipal de Divinópolis

Assinantes



Presidente da Camara Municipal de Divinópolis

Assinou em 22/10/2026 às 14:47:41 com Certificado Digital Qualificado, emitido em nome de ISRAEL MENDONCA com o CPF *****.119.356-****, nos termos do § 1º do art. 10 da Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

Eu, Presidente da Camara Municipal de Divinópolis, 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.betha.cloud** e insira o código abaixo:

Y75-678-Z66-RJ1

**TERMO DE REFERÊNCIA****Contratação de Solução integrada de Firewall NGFW**

Processo Administrativo nº ____/2026

1 CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1 A presente licitação tem por objetivo a contratação de solução integrada de segurança de rede do tipo Firewall de Próxima Geração (NGFW/UTM), em regime de locação com cessão de uso/comodato do appliance, incluindo fornecimento do appliance, subscrição/licenciamento durante toda a vigência contratual, suporte técnico oficial da solução, atualização tecnológica e garantia de continuidade operacional e treinamento técnico para transferência de conhecimento à equipe de Tecnologia da Informação da Câmara Municipal, de acordo com as quantidades, especificações e condições descritas neste Termo de Referência e em seus anexos.

Item	Descrição da Solução	Catmat/ Catser	Quant	Unidade	Valor unitário	Valor Total
01	Fornecimento de solução integrada de segurança de rede do tipo Firewall de próxima geração (NGFW), em regime de locação com cessão de uso/comodato do appliance Conforme quantitativos e especificações constantes na tabela item 1.2 e anexo I deste documento.	27090	12	Mês	R\$ 8.514,83	R\$ 102.177,96
TOTAL MENSAL ESTIMADO						R\$ 8.514,83
TOTAL ANUAL ESTIMADO						R\$ 102.177,96

1.2 O objeto constitui solução única e integrada, correspondente ao Item 01 desta contratação, sendo os componentes descritos na tabela abaixo partes indissociáveis da solução, não constituindo itens autônomos para fins de disputa, julgamento, adjudicação ou contratação. A proposta deverá contemplar integralmente todos os componentes e respectivos quantitativos, licenças, subscrições, funcionalidades, suporte, atualizações e demais recursos necessários ao atendimento dos requisitos e especificações técnicas estabelecidos neste Termo de Referência e em seus anexos.



Tabela de composição do Item 01 – Solução Integrada de Firewall NGFW			
Componente	Descrição	Quant	Unid.
Appliance NGFW	Appliance dedicado de Firewall de Próxima Geração – NGFW, novo, em linha de produção atual, disponibilizado em regime de locação com cessão de uso/comodato. O equipamento deverá atender integralmente às especificações mínimas de hardware, capacidade, suficiente para suportar toda a demanda prevista da rede institucional, incluindo sistema operacional/firmware nativo ou homologado, kit de instalação em rack e demais componentes e acessórios necessários ao funcionamento da solução, conforme especificações do Anexo I.	1	Unidade
Licenciamento/ Subscrição de Segurança	Licenciamento, subscrição ou disponibilização integral de todos os recursos de segurança necessários ao appliance NGFW durante toda a vigência contratual, com capacidade técnica e de licenciamento para suportar no mínimo 500 dispositivos, abrangendo, quando aplicável à arquitetura ofertada, IPS, antivírus, antimalware, filtragem de conteúdo, controle de aplicações, inspeção de tráfego, análise comportamental, Inteligência Artificial – IA e/ou Machine Learning, inteligência de ameaças e demais funcionalidades de segurança, conforme especificações anexo I.	1	Conjunto
Conectividade segura/VPN	Licenciamento, habilitação ou disponibilização dos recursos necessários à conectividade segura via VPN IPsec, SSL VPN, VPN baseada em TLS/SSL ou tecnologia equivalente, abrangendo a solução durante toda a vigência contratual. Quando tais funcionalidades forem nativas ou já estiverem abrangidas pelo licenciamento principal da plataforma, não será exigido licenciamento específico adicional, desde que permaneçam integralmente disponíveis.	1	Conjunto
Plataforma de gerenciamento centralizado	Licenciamento, subscrição ou disponibilização da plataforma de gerenciamento centralizado do appliance NGFW, recurso tecnológico integrante da solução ofertada, disponibilizado em nuvem, ambiente local, híbrido ou tecnologia equivalente, válido durante toda a vigência contratual, permitindo o gerenciamento centralizado do appliance, visualização das informações operacionais, geração de alertas e relatórios, backup automático das configurações com retenção mínima de 5 (cinco) versões válidas, gerenciamento de políticas e acompanhamento dos indicadores de saúde operacional da solução.	1	Plataforma
Garantia, suporte oficial e atualização tecnológica	Disponibilização, durante toda a vigência contratual, da documentação técnica oficial, acesso aos recursos e portais oficiais aplicáveis, imagens e atualizações oficiais de firmware/software, licenças e subscrições, garantia, suporte técnico oficial da solução, atendimento aos níveis de serviço previstos neste documento e seus anexos, substituição de hardware quando necessária e mecanismos de atualização tecnológica/Hardware Refresh, inclusive nas hipóteses de descontinuidade, perda de suporte ou incapacidade de atendimento aos requisitos contratados.	1	Serviço
Treinamento e transferência de conhecimento	Treinamento técnico destinado à equipe de Tecnologia da Informação da Câmara Municipal, com carga horária mínima de 8 (oito) horas, abrangendo as funcionalidades efetivamente contratadas e observando os requisitos estabelecidos no anexo I deste documento.	1	Serviço



- 1.3** Todos os equipamentos e componentes físicos fornecidos para composição da solução deverão ser entregues em estado de novo e sem uso anterior, sendo vedado o fornecimento de equipamentos ou componentes reconicionados, remanufaturados ou refurbished. O appliance de Firewall NGFW deverá, adicionalmente, corresponder a modelos integrantes da linha atual do fabricante e regularmente comercializados na data da entrega, observadas as condições de conformidade e ciclo de vida estabelecidas no item 1.4 deste Termo de Referência.
- 1.4** Não serão aceitos softwares ou firmwares em versões beta, experimentais ou não oficiais, nem appliance que, na data da entrega, tenha atingido os marcos de End-of-Life (EOL), End-of-Sale (EOS) ou End-of-Support (EOSP), conforme as definições e informações oficiais do fabricante, devendo o equipamento permanecer em linha de comercialização regular, com suporte técnico e atualizações oficiais disponíveis, observadas as exigências de continuidade tecnológica estabelecidas neste Termo de Referência.
- 1.5** Independentemente da origem da solução ofertada, é indispensável que esta disponha de suporte técnico em território nacional, mecanismos compatíveis com políticas de soberania de dados, conformidade com a LGPD e recursos adequados de auditoria, rastreabilidade de acessos e gestão da segurança da informação.
- 1.6** A contratada deverá garantir a modernização contínua da plataforma sempre que o appliance, sistema operacional, licenciamento ou componente integrante da solução fornecida entrar em processo de descontinuidade, fim de suporte, fim de venda ou fim de vida útil e essa condição comprometer o suporte, a atualização, a segurança, a compatibilidade ou o atendimento aos requisitos contratados, bem como nos casos de incompatibilidade técnica ou incapacidade comprovada de atendimento aos requisitos contratados sem ônus adicional para a Câmara Municipal de Divinópolis.
- 1.7** As características, funcionalidades, capacidades e especificações técnicas mínimas a serem atendidas pela solução de Firewall de Próxima Geração (NGFW) estão estabelecidas no Anexo I deste documento.
- 1.8** Havendo divergência entre a descrição do item constante neste Termo de Referência e a descrição do item correspondente no CATMAT/CATSER apresentado no portal COMPRASNET, deverá prevalecer a descrição constante neste Termo de Referência e no Edital.
- 1.9** A presente contratação caracteriza-se como solução de Tecnologia da Informação e Comunicação – TIC de natureza composta, integrada e comum, compreendendo a disponibilização de 01 (um) appliance de Firewall NGFW em regime de locação com cessão de uso/comodato, licenciamentos e subscrições, suporte técnico, atualização tecnológica e demais recursos e serviços associados previstos neste Termo de Referência e em seus anexos. Seus padrões de desempenho e qualidade podem ser objetivamente definidos por meio de especificações usuais de mercado.



- 1.10** A contratação possui natureza continuada, sem dedicação exclusiva de mão de obra, considerando a necessidade permanente de disponibilidade da solução, dos licenciamentos, subscrições, atualizações e suporte técnico durante toda a vigência contratual, indispensáveis à manutenção da segurança e da continuidade operacional da rede institucional.
- 1.11** O objeto desta contratação não se enquadra como sendo bem de luxo, conforme art. 42, II, da Portaria nº 188/23 desta Câmara Municipal.
- 1.12** Na elaboração da proposta, a licitante deverá identificar e considerar todos os dispositivos, componentes e acessórios específicos da solução ofertada que, conforme as especificações e recomendações do fabricante, sejam necessários à sua adequada instalação e funcionamento, incluindo, quando aplicável, cabos de alimentação, adaptadores, acessórios de montagem, componentes para acesso administrativo local ou recuperação e demais itens necessários. Todos esses componentes deverão estar incluídos na proposta e no preço ofertado, sem ônus adicional para a Contratante, não abrangendo adequações ou ampliações da infraestrutura elétrica predial, cuja disponibilização observará o disposto no item 1.13 deste Termo de Referência.
- 1.13** A Câmara Municipal de Divinópolis disponibilizará a infraestrutura física e elétrica predial necessária à implantação da solução, compatível com as condições do ambiente previamente informadas e com os requisitos desta contratação. Caberá à Contratada fornecer, juntamente com a solução e sem custo adicional posterior, os dispositivos, componentes e acessórios complementares de proteção elétrica que sejam necessários ao perfeito funcionamento dos equipamentos ofertados, conforme previsto no item 1.12 deste Termo de Referência.
- 1.14** A responsabilidade por eventual dano aos equipamentos será apurada de acordo com sua causa e com as obrigações atribuídas a cada parte, observada a existência de nexo entre o fato ocorrido e o dano verificado. A Administração responderá pelas ocorrências comprovadamente decorrentes de falha ou inadequação da infraestrutura física ou elétrica predial sob sua responsabilidade, enquanto a Contratada responderá pelos danos decorrentes de vício, defeito, inadequação ou ausência dos equipamentos, dispositivos de proteção, componentes ou acessórios cujo fornecimento lhe seja atribuído nos termos desta contratação.

Detalhamento básico da solução

- 1.15** A solução a ser contratada compreenderá uma infraestrutura integrada de proteção, composta pelos seguintes pilares:
- 1.15.1 Capacidade Operacional e Continuidade da Solução:** A solução deverá ser composta por 01 (um) appliance dedicado de Firewall NGFW, dimensionado para atender integralmente, de forma individual, à demanda institucional e aos parâmetros mínimos de desempenho estabelecidos neste Termo de Referência e em seus



anexos. A continuidade operacional da solução será assegurada pela capacidade do equipamento, pelos mecanismos de monitoramento, suporte técnico, contingência, restauração, substituição de hardware e atualização tecnológica previstos na contratação, não sendo exigida redundância física mediante cluster de appliances em Alta Disponibilidade (HA).

1.15.2 Inteligência de Segurança e Análise Comportamental: A solução deverá possuir recursos avançados de inspeção profunda de pacotes, análise comportamental, correlação automatizada de eventos e mecanismos de detecção de ameaças, podendo utilizar inteligência artificial (IA), Machine Learning (ML) ou tecnologias funcionalmente equivalentes, permitindo identificar atividades suspeitas, tentativas de exploração, ransomwares e outras ameaças cibernéticas modernas.

1.15.3 Conectividade Inteligente e SD-WAN: O sistema deverá atuar como elemento central de gerenciamento das comunicações da instituição, gerenciando de forma inteligente os links de internet. Através da tecnologia SD-WAN, a solução deverá monitorar constantemente a qualidade das conexões (latência e perda de pacotes), direcionando o tráfego crítico para o melhor link disponível e reduzindo o risco de paralisação dos serviços quando houver enlace alternativo disponível.

1.15.4 Gestão Unificada e Soberania de Dados: Todo o ecossistema de segurança deverá ser gerenciado por meio de painel centralizado, em nuvem, local, híbrido ou solução equivalente, permitindo à equipe de TI monitorar ameaças, usuários, aplicações, VPNs, links de internet, políticas de segurança, alertas e relatórios gerenciais. O ambiente prioriza a conformidade com a LGPD, mantendo trilhas de auditoria e logs detalhados de todas as conexões, assegurando a rastreabilidade necessária à segurança da informação, à auditoria e à governança institucional.

1.15.5 Sustentabilidade Tecnológica (Hardware Refresh): A plataforma de segurança como um todo será amparada por um modelo de contratação que garanta que, durante toda a vigência contratual, o equipamento e os demais componentes da solução estarão atualizados, com suporte técnico do fabricante ou fornecedor autorizado, e com substituição proativa de hardware em caso de descontinuidade de modelos (End-of-Life).

Informações sobre o ambiente atual da Câmara Municipal

1.16 A infraestrutura tecnológica da Câmara Municipal compreende rede corporativa interna, conectividade com a Internet, rede sem fio corporativa composta por 24 (vinte e quatro) pontos de acesso (APs) e interligação corporativa entre a sede, localizada na Rua São Paulo, nº 277, Centro, Divinópolis/MG, e o prédio anexo, localizado na Rua Antônio Olímpio de Moraes, nº 545, Centro, Divinópolis/MG.

A solução de Firewall NGFW deverá ser compatível com esse ambiente, permitindo o



gerenciamento dos links de Internet, a redundância operacional dos links, o balanceamento de tráfego, o controle e a aplicação de políticas de segurança sobre o tráfego da rede interna e da rede Wi-Fi, bem como a integração com a interligação corporativa entre a sede e o prédio anexo. Quando tecnicamente aplicável à arquitetura adotada, deverá permitir a utilização de VPN ou mecanismo equivalente para proteção da comunicação.

Os elementos descritos neste item possuem caráter informativo quanto ao ambiente tecnológico no qual a solução será utilizada, devendo os requisitos funcionais, capacidades e especificações técnicas mínimas da solução observar o disposto no item 1.15 e no Anexo I deste Termo de Referência.

1.17 O ambiente atual possui aproximadamente:

1.17.1 Rede interna cabeada com capacidade operacional estimada em 300 Mbps Full Duplex;

1.17.2 Infraestrutura de rede sem fio (Wi-Fi) com utilização aproximada de 100 Mbps Full Duplex;

1.17.3 Ambiente de acesso remoto e VPN com consumo estimado em 70 Mbps Full Duplex.

1.18 Atualmente, a infraestrutura de conectividade da Câmara Municipal opera com 3 (três) links de internet ativos. Está prevista, no âmbito de contratação correlata específica de conectividade, a substituição dessa infraestrutura por 2 (dois) links dedicados com capacidade mínima de 1 Gbps Full Duplex, destinados a proporcionar redundância operacional e balanceamento de tráfego, bem como interligação corporativa dedicada entre a sede e o prédio anexo. A solução de Firewall NGFW objeto deste Termo de Referência deverá ser compatível com essa arquitetura de conectividade, permitindo o gerenciamento dos links e a aplicação das políticas de segurança pertinentes, sem que o fornecimento dos links de internet ou da interligação corporativa Sede-Anexo integre o objeto desta contratação.

1.19 O suporte a DNS Dinâmico (DDNS) constitui funcionalidade técnica integrante da solução de Firewall NGFW, não caracterizando componente ou item autônomo para fins de disputa ou adjudicação. A solução deverá disponibilizar suporte à atualização automática de registros DNS associados a interfaces ou serviços cujos endereços IP possam sofrer alterações, quando aplicável à arquitetura de conectividade implantada, de forma a preservar a resolução de nomes e a continuidade de acesso aos serviços dependentes dessa funcionalidade. A utilização efetiva do recurso ficará condicionada às necessidades operacionais e às características dos enlaces de comunicação utilizados pela Câmara Municipal.



2 FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1 A presente contratação mostra-se indispensável para garantir a segurança, a continuidade e a modernização da camada de segurança perimetral da rede de dados utilizada pela Câmara Municipal de Divinópolis, mediante a adoção de uma solução integrada de segurança de rede do tipo Firewall de Próxima Geração (NGFW).

2.1.1 Ressalta-se que a consulta aos Catálogos de Soluções de Tecnologia da Informação e Comunicação (TIC) com condições padronizadas não foi realizada, considerando que os referidos instrumentos apresentam soluções vinculadas a fabricantes, marcas e produtos específicos, enquanto a presente contratação foi estruturada com base em requisitos técnicos e funcionais, sem indicação ou preferência por marca ou fabricante. Dessa forma, considerando a possibilidade de participação de diferentes soluções tecnológicas que atendam às especificações estabelecidas, entendeu-se que os preços constantes dos referidos catálogos não constituiriam, necessariamente, parâmetros equivalentes ao objeto pretendido, razão pela qual a estimativa de preços foi fundamentada em pesquisa de mercado, com referências compatíveis com as características e exigências da contratação.

2.2 A fundamentação completa da contratação, bem como a descrição detalhada da necessidade que a justifica, encontra-se pormenorizada em tópico específico do Estudo Técnico Preliminar, apêndice deste termo de referência.

Plano de Contratações Anual

2.3 O Plano de Contratações Anual (PCA) é um documento de planejamento que deve ser elaborado e publicado consolidando as contratações a serem efetuadas ou prorrogadas no exercício subsequente. A presente contratação encontra-se prevista no Plano Anual de Contratações da Câmara Municipal de Divinópolis, disponível no PNCP através do endereço eletrônico <https://pncp.gov.br/app/pca/23774227000190/2026> conforme detalhamento a seguir:

Número do item no PCA: 16

Classificação: 70 Informática – Equipamentos, peças, acessórios e suprimentos de TIC

Documentos de Formalização de Demanda de Origem: DFD nº 005/2026 da Diretoria de Informática e tecnologia da informação, assinados com o certificado avançado da Betha Sistemas

Adequação da solução proposta: Em relação à solução inicialmente prevista no DFD original supracitado, registra-se que, em decorrência de aprofundamentos dos estudos técnicos realizados no âmbito do ETP, verificou-se a necessidade de adequação da solução inicialmente delineada, uma vez que esta não contemplava integralmente os requisitos técnicos e operacionais necessários à integral segurança da rede institucional. Dessa forma, procedeu-se à adequação da solução proposta, com vistas a assegurar maior aderência às necessidades do Órgão, preservando-se, contudo, a natureza e a finalidade originalmente pretendidas, sem que a alteração represente desvio de objeto.



Ressalta-se que a fase de planejamento da contratação, especialmente por meio do Estudo Técnico Preliminar, constitui instrumento destinado à análise e à definição da solução mais adequada à necessidade da Administração, nos termos da Lei nº 14.133/2021, permitindo o aprimoramento das informações inicialmente levantadas no DFD, com vista à seleção da alternativa mais vantajosa, eficiente e aderente ao interesse público.

3 DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERANDO O CICLO DE VIDA DO OBJETO

3.1 A solução a ser contratada compreende o fornecimento integrado e continuado de solução de segurança de rede do tipo Firewall de Próxima Geração (NGFW/UTM), em regime de locação com cessão de uso/comodato, composta por 01 (um) appliance dedicado de segurança, dimensionado para atender integralmente à demanda institucional e aos parâmetros mínimos de desempenho estabelecidos neste Termo de Referência, respectivos licenciamentos e subscrições de segurança, recursos de conectividade segura, plataforma de gerenciamento centralizado, documentação técnica oficial, atualizações de firmware e software, suporte técnico oficial, atualização tecnológica e treinamento técnico da equipe de Tecnologia da Informação da Câmara Municipal, observados os requisitos estabelecidos neste Termo de Referência e em seus anexos.

3.1.1 A implantação física, a configuração lógica, a migração, a integração com o ambiente existente, os testes, a homologação e a sustentação operacional continuada da solução não estão compreendidos no objeto dessa contratação.

3.2 Os componentes da solução deverão ser fornecidos de forma integrada e permanecer licenciados, atualizados, suportados e plenamente funcionais durante toda a vigência contratual, cabendo à Contratada assegurar a continuidade tecnológica da solução, inclusive mediante atualização, substituição ou modernização dos componentes quando ocorrer descontinuidade, fim de suporte, fim de venda, fim de vida útil, incompatibilidade técnica ou incapacidade comprovada de atendimento aos requisitos contratados, nos termos previstos neste documento e seus anexos.

4 REQUISITOS DA CONTRATAÇÃO

Requisitos básicos

4.1 A seleção do fornecedor será efetuada por meio da realização de processo licitatório, na modalidade PREGÃO, sob a forma ELETRÔNICA, por meio do critério de menor preço, nos termos do art. 33, inciso I, da Lei nº 14.133/2021.

4.2 Para a habilitação do fornecedor serão exigidas, exclusivamente, as condições de que dispõe a Lei 14.133/2021, conforme regulamentação dada pelo art. 36 da Instrução Normativa SEGES/ME nº 73, de 30 de Setembro de 2022, recepcionada pelo Município



de Divinópolis por meio do Decreto 15.980/2023. Tais requisitos serão oportunamente apresentados em tópico específico deste documento.

4.3 Não será admitida a participação de pessoas jurídicas em regime de consórcio, qualquer que seja sua forma de constituição, por não se tratar de execução contratual de alta complexidade ou de grande vulto financeiro.

4.4 Este processo será preferencial para microempresas (ME) e empresas de pequeno porte (EPP), por força da LC 123/2006 e 14.133/2021. Resta afastado o critério de exclusividade uma vez que o valor estimado para esta contratação extrapola o limite previsto no art 48, inciso I, da LC 123/2006.

4.4.1 Para a obtenção dos benefícios constantes na Lei Complementar 123/2006 e 14.133/2021, as microempresas e empresas de pequeno porte deverão apresentar declaração de que, no ano-calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte, conforme previsão no Art. 4º, § 2º da Lei 14.133/2021.

4.5 Durante a execução contratual, a Contratada deverá atender às solicitações e aos chamados técnicos nos prazos e condições estabelecidos, observados os níveis de criticidade e os tempos máximos de resposta e restabelecimento previstos no item 5.8, bem como as regras de contagem dos prazos estabelecidas no item 5.9.

Parâmetros de sustentabilidade da Contratação

4.6 A contratada deverá observar, durante a execução contratual, práticas que promovam a sustentabilidade ambiental, a eficiência energética, o consumo responsável de recursos e a adequada gestão dos resíduos gerados, em conformidade com a Lei nº 14.133/2021, Lei nº 12.305/2010 (Política Nacional de Resíduos Sólidos), bem como com as diretrizes do Guia Nacional de Contratações Sustentáveis da Advocacia-Geral da União, em especial:

4.6.1 Os equipamentos fornecidos deverão possuir projeto voltado para o uso eficiente de energia elétrica, de forma a minimizar o consumo durante sua operação, compatível com sua categoria e capacidade de processamento.

4.6.2 Só será admitida a oferta de bens de informática que não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenil polibromados (PBBs), éteres difenilpolibromados (PBDEs).

4.6.3 Ao término da vida útil dos equipamentos fornecidos, ou quando houver necessidade de substituição definitiva decorrente da garantia, a contratada deverá assegurar a destinação ambientalmente adequada dos equipamentos eletroeletrônicos, componentes e baterias eventualmente substituídos, observando os



princípios da logística reversa previstos na Lei nº 12.305/2010.

- 4.6.4** A solução deverá possuir ciclo de vida compatível com a vigência da contratação, permitindo atualizações de software, assinaturas de segurança e suporte técnico oficial durante todo o período contratual, evitando substituições prematuras de equipamentos e contribuindo para a redução da geração de resíduos eletroeletrônicos.
- 4.6.5** As atualizações de firmware e software deverão ocorrer preferencialmente por meio eletrônico, dispensando o fornecimento de mídias físicas, salvo quando tecnicamente indispensável.
- 4.6.6** Sempre que possível, deverão ser adotadas medidas que reduzam o uso de papel e de outros materiais físicos, sem prejuízo da disponibilização de documentos em meio físico quando exigido pela legislação ou por norma técnica. Nesse sentido, a documentação técnica, os manuais, as licenças, os certificados, os relatórios e os demais documentos relacionados à solução deverão ser disponibilizados, preferencialmente, em meio eletrônico.
- 4.6.7** Embora a responsabilidade pelo descarte dos resíduos gerados recaia sobre a empresa contratada, a Administração poderá exigir a comprovação da destinação ambientalmente adequada desses materiais, de modo a assegurar o atendimento à legislação ambiental vigente e a preservação do meio ambiente. Tal medida reforça o compromisso institucional com práticas sustentáveis e com a adoção de mecanismos de controle que garantam a efetividade das ações ambientais associadas à contratação.

Vistoria

- 4.7** Para o correto dimensionamento e elaboração de sua proposta, o licitante poderá realizar, se necessário, vistoria nas instalações da Câmara, acompanhado por servidor designado para esse fim, de segunda a sexta-feira, das 12h às 18h, devendo o agendamento ser previamente realizado pelo e-mail: compras@divinopolis.mg.leg.br;
- 4.8** O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até o dia útil anterior à data prevista para a abertura da sessão pública;
- 4.9** Para a vistoria, o licitante, ou o seu representante legal, deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria;
- 4.10** A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo a licitante vencedora assumir os ônus das situações decorrentes da ausência de verificação;
- 4.11** A licitante deverá declarar que realizou a vistoria e tomou conhecimento de todas as informações e condições locais para o cumprimento das obrigações objeto da licitação ou



declaração de que não realizou a vistoria e entende conhecer todos os elementos suficientes para o correto dimensionamento dos serviços a serem prestados.

Subcontratação

- 4.12** É vedada a subcontratação integral do objeto, bem como a transferência a terceiros da responsabilidade pelas obrigações principais assumidas pela Contratada, especialmente quanto ao fornecimento e à disponibilização da solução e de seus componentes, incluindo o appliance de Firewall NGFW, licenciamentos, subscrições, plataforma de gerenciamento, garantia, atualização tecnológica, continuidade da solução e suporte técnico oficial

Garantia para contratação

- 4.13** Não haverá exigência de garantia contratual, nos termos dos arts. 96 e seguintes da Lei nº 14.133/2021, considerando a avaliação dos riscos da contratação e a existência de mecanismos contratuais de fiscalização, recebimento, garantia, substituição e suporte técnico.

Proteção de dados

- 4.14** A partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa, a empresa passa a ser obrigada a cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenha acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado.
- 4.15** 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, vedado seu compartilhamento com terceiros, ressalvados contratos específicos para tratamento de dados firmados de acordo com os ditames dessa Lei.
- 4.16** A transferência internacional de dados somente será admitida nas hipóteses do art. 33 da LGPD e a empresa responderá legalmente caso desrespeite as disposições desta Lei.
- 4.17** Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever da empresa eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações
- 4.18** É dever da empresa orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da Lei nº 13.709, de 14 de agosto de 2018.
- 4.19** Caso seja admitida subcontratação, o instrumento de subcontratação deverá estabelecer para a subcontratada os deveres da presente cláusula expressamente.
- 4.20** A Administração poderá realizar diligência para aferir o cumprimento dessa cláusula,



devendo a contratada atender os pedidos de comprovação eventualmente efetuados.

4.20.1 O acesso da Contratada, de seus profissionais ou de terceiros autorizados aos recursos da solução e ao ambiente tecnológico da Câmara deverá ocorrer exclusivamente quando necessário à execução das atividades contratadas, mediante credenciais individualizadas, observando-se o princípio do menor privilégio e a limitação do acesso aos recursos estritamente necessários à atividade realizada.

4.20.2 Sempre que tecnicamente disponível, os acessos administrativos realizados pela Contratada ou por terceiros autorizados deverão ser passíveis de identificação e rastreabilidade, mediante registros que permitam identificar o usuário, a data, o horário e a atividade executada.

4.20.3 A Contratada deverá comunicar imediatamente à Câmara Municipal qualquer incidente de segurança da informação de que tenha conhecimento e que possa afetar dados, credenciais, configurações, logs, disponibilidade, integridade ou confidencialidade da solução ou do ambiente institucional, fornecendo as informações disponíveis para análise da ocorrência e adotando as medidas necessárias à preservação de registros e evidências técnicas relacionadas ao incidente.

4.20.4 As obrigações de segurança previstas nesta seção aplicam-se não apenas aos dados pessoais, mas também às informações técnicas e institucionais acessadas em razão da execução contratual, incluindo configurações, topologia de rede, regras de firewall, credenciais, endereçamento, logs, registros de eventos, vulnerabilidades identificadas e demais informações cuja divulgação, alteração ou indisponibilidade possa comprometer a segurança ou a continuidade das atividades da Câmara Municipal.

4.21 Caso a Contratada receba solicitação de titular de dados pessoais relacionada a dados tratados em razão desta contratação, deverá encaminhá-la imediatamente à Câmara Municipal de Divinópolis, abstendo-se de fornecer informações, realizar alterações, excluir dados ou adotar qualquer outra providência diretamente perante o titular sem prévia orientação ou autorização da Administração, ressalvadas as hipóteses em que esteja sujeita a obrigação legal própria e diretamente aplicável.

4.21.1 Quando solicitado pela Administração, a Contratada deverá prestar o apoio técnico necessário à identificação, localização, preservação, disponibilização ou eliminação dos dados relacionados à solicitação do titular, limitado às informações e recursos sob sua responsabilidade e observadas as orientações da Câmara Municipal.

4.22 Caso, em razão da prestação do suporte técnico ou da utilização de recursos da solução sob responsabilidade da Contratada, haja acesso, coleta, armazenamento ou tratamento de logs, registros de eventos, configurações, telemetria, registros de chamados ou outras informações técnicas relacionadas à infraestrutura tecnológica da Câmara Municipal, tais informações deverão ser utilizadas exclusivamente para as finalidades necessárias à execução desta contratação, observadas as regras de



segurança da informação, confidencialidade, controle de acesso, rastreabilidade e proteção de dados estabelecidas neste Termo de Referência.

4.22.1 As informações previstas no item anterior deverão permanecer protegidas contra acesso, utilização, alteração, divulgação ou eliminação não autorizados, sendo vedada sua utilização para finalidade diversa da execução contratual, ressalvadas as hipóteses legalmente exigidas.

4.22.2 O disposto neste item não implica autorização para formação, pela Contratada, de banco de dados próprio contendo informações da Câmara Municipal, nem para reutilização, compartilhamento ou aproveitamento dos dados e informações técnicas obtidos em razão do contrato para finalidade diversa daquela necessária ao cumprimento das obrigações contratuais.

5 MODELO DE EXECUÇÃO DO OBJETO

Dos prazos e local de entrega dos equipamentos

5.1 A Contratada deverá entregar o equipamento na sede da Câmara Municipal de Divinópolis/MG, situada à Rua São Paulo, 277, Centro, Divinópolis/MG, devidamente acompanhado dos componentes, acessórios e documentação técnica previstos neste Termo de Referência, bem como disponibilizar as respectivas licenças, subscrições e demais recursos necessários à posterior implantação da solução. A obrigação da Contratada deste Termo de Referência, nesta etapa, limita-se ao fornecimento e à disponibilização dos elementos integrantes da solução sob sua responsabilidade. A instalação física, configuração lógica, migração, integração, testes e homologação serão executados pela empresa responsável pela contratação correlata de serviços especializados, conforme disposto no item 5.2.

5.1.1 Após a entrega, o equipamento será inspecionado por servidor designado da Diretoria de Informática e T.I. para conferência com as especificações estabelecidas neste Termo de Referência. Em caso de desconformidade atribuível ao fornecimento, a Contratada será notificada para efetuar a substituição no prazo máximo de 03 (três) dias úteis, contado da respectiva notificação.

5.1.2 O equipamento deverá ser entregue exclusivamente durante o horário de funcionamento da Câmara Municipal de Divinópolis, em dias úteis e das 12 h às 18:00 h.

5.1.3 O prazo para entrega do appliance, disponibilização das licenças e subscrições, documentação técnica e demais componentes necessários à posterior implantação da solução será de até 20 (vinte) dias úteis, contado da notificação da Contratada pela Contratante, mediante emissão da respectiva Solicitação de Serviço.

Da transferência de conhecimento e realização de treinamento

5.1.4 O treinamento técnico será destinado à equipe de Tecnologia da Informação da Câmara Municipal, com o objetivo de proporcionar conhecimento prévio da



ferramenta, promover o nivelamento técnico e desenvolver a capacidade de acompanhamento e interlocução sobre a solução fornecida.

5.1.5 O treinamento deverá possuir carga horária mínima de 8 (oito) horas, podendo ser estendida, caso necessário, para assegurar a abordagem integral do conteúdo programático previsto no Anexo I deste Termo de Referência. O treinamento poderá ser realizado de forma presencial, remota ou híbrida, ou por meio de cursos em videoaulas, desde que sejam asseguradas condições adequadas para a efetiva transferência de conhecimento.

5.1.5.1 O conteúdo programático possui caráter de capacitação técnica e transferência de conhecimento, não implicando transferência à equipe da Câmara Municipal das responsabilidades de administração, configuração, monitoramento ou sustentação operacional continuada da solução, atribuídas à empresa responsável pela contratação específica dos serviços especializados correlatos.

5.1.6 O treinamento poderá ser ministrado pelo fabricante, parceiro autorizado ou fornecedor da solução, desde que o instrutor possua conhecimento técnico compatível com a solução ofertada, comprovado por certificação emitida pelo fabricante, habilitação técnica equivalente ou experiência profissional compatível na solução ofertada.

5.1.7 Ao término do treinamento, deverá ser disponibilizado material didático, documentação técnica ou conteúdo equivalente utilizado durante a capacitação, em formato digital, bem como emitido certificado, declaração ou documento equivalente que comprove sua realização.

Da implantação e configuração inicial da solução de Firewall NGFW

5.2 A implantação física, a configuração lógica, a migração, a integração com os ambientes existentes, a orientação operacional relacionada ao ambiente implantado, os testes, a homologação e os demais serviços especializados necessários à implantação e configuração da solução **não fazem parte do objeto desta contratação**, sendo de responsabilidade de empresa contratada especificamente para a prestação desses serviços.

5.2.1 A atuação dessa empresa não eximirá a Contratada de suas responsabilidades contratuais, nem impedirá o seu acionamento direto pela Administração, permanecendo integralmente responsável pelo atendimento, pelo suporte técnico e pelo cumprimento dos níveis de serviço estabelecidos nesta contratação, no que se refere às obrigações que lhe competem.

5.3 À empresa fornecedora do appliance e dos demais componentes da solução caberá, no âmbito desta contratação, a disponibilização da documentação técnica oficial da solução ofertada, o acesso aos portais do fabricante, quando aplicável, o fornecimento dos licenciamentos, imagens oficiais de firmware e respectivas atualizações, o suporte



técnico do fabricante ou de parceiro autorizado, bem como a prestação das informações técnicas necessárias à implantação da solução e o apoio técnico à empresa responsável pela implantação e configuração, sempre que necessário.

Do suporte técnico e Acordo de Nível de Serviço (SLA)

- 5.4** A Contratada deverá disponibilizar suporte técnico sem custo adicional para a Contratante, com a finalidade de esclarecimento de dúvidas acerca da solução ofertada ou abertura de chamados técnicos.
- 5.4.1** Para os incidentes classificados como Críticos, o atendimento deverá estar disponível em regime 24x7, com contagem ininterrupta dos respectivos prazos de resposta e restabelecimento.
- 5.4.2** O suporte técnico deverá ser prestado por meio de chat, telefone, e-mail ou canais equivalentes, com atendimento por profissional humano especializado, em língua portuguesa.
- 5.4.3** O suporte deverá possibilitar escalonamento e atendimento por profissionais especializados em áreas específicas sempre que necessário à resolução de incidentes críticos ou complexos.
- 5.5** A Contratada deverá disponibilizar, adicionalmente, canal ou ferramenta para abertura, registro, acompanhamento e consulta dos chamados, podendo ser utilizado sistema WEB, e-mail, software específico ou outra solução tecnológica adequada, de forma a permitir à Contratante o adequado acompanhamento das solicitações e de seu respectivo andamento.
- 5.6** Os chamados deverão ser recebidos e tratados por equipe técnica especializada da Contratada, que deverá adotar postura proativa e iniciar imediatamente as providências necessárias para identificação, diagnóstico e correção das falhas, mediante atendimento remoto ou, quando tecnicamente necessário, mediante o envio de equipe técnica presencial à Sede da Câmara.
- 5.6.1** A Contratada deverá assegurar, durante toda a vigência contratual, capacidade de atendimento técnico presencial no Município de Divinópolis/MG, sempre que a natureza da ocorrência exigir intervenção física relacionada às obrigações do fornecimento da solução, especialmente em situações envolvendo falha de hardware, necessidade de substituição de equipamento ou outra providência que não possa ser solucionada exclusivamente por atendimento remoto.
- 5.6.2** A capacidade de atendimento presencial poderá ser disponibilizada por equipe própria da Contratada ou por empresa, parceiro técnico ou prestador de serviços formalmente vinculado à Contratada, desde que possua qualificação compatível com a solução ofertada e condições de atendimento que permitam o cumprimento dos prazos estabelecidos nos Acordos de Nível de Serviço – SLA.



5.6.3 A Contratada deverá comprovar essa capacidade antes do início da execução contratual, mediante contrato, instrumento de parceria, declaração de disponibilidade, acordo de prestação de serviços ou documento equivalente que demonstre a efetiva disponibilidade da estrutura de atendimento.

5.6.4 Não será exigida sede, filial ou estabelecimento da Contratada no Município de Divinópolis, sendo suficiente a demonstração de estrutura própria ou de terceiro que permita o atendimento presencial dentro dos prazos contratuais.

5.7 A Contratada deverá manter sistema de controle e registro de chamados, acessível à Contratante, que permita a abertura, o acompanhamento e a consulta das solicitações, mantendo histórico das ocorrências, respectivas datas, providências adotadas e soluções apresentadas.

5.8 O suporte técnico deverá ser prestado conforme a criticidade dos incidentes ou solicitações, observando os tempos máximos de resposta e restabelecimento definidos na tabela abaixo, sendo aplicável aos incidentes classificados como Críticos o regime de atendimento contínuo previsto no item 5.4.1.

Criticidade	Descrição	Tempo Máximo de Resposta	Tempo Máximo para Restabelecimento
Crítica	Indisponibilidade total do appliance NGFW ou da solução decorrente de falha de hardware, firmware, licenciamento, subscrição ou funcionalidade nativa da plataforma, bem como comprometimento grave de segurança decorrente de falha nativa da solução.	30 minutos	24 horas corridas
Alta	Degradação severa de desempenho ou falha parcial de serviços essenciais do appliance NGFW ou da solução, decorrente de falha de hardware, firmware, licenciamento, subscrição ou funcionalidade nativa da plataforma, ou comprometimento relevante de segurança atribuível ao produto, sem caracterizar indisponibilidade total.	1 hora	16 horas úteis
Média	Falhas em funcionalidades nativas da plataforma, firmware, relatórios, licenciamento ou subscrições, ou degradação moderada atribuível ao produto sem interrupção total dos serviços.	4 horas	24 horas úteis
Baixa	Solicitações administrativas relacionadas a licenciamento, subscrições, garantia ou suporte oficial, dúvidas técnicas sobre funcionalidades nativas ou demandas vinculadas ao produto sem impacto significativo na continuidade operacional.	8 horas	48 horas úteis

5.9 Os prazos de resposta e restabelecimento previstos no item 5.8 serão contados a partir da abertura formal do chamado junto à Contratada, realizada diretamente pela Administração ou, mediante sua autorização, pela empresa responsável pelos serviços especializados correlatos, observadas as condições de registro e acompanhamento previstas no item 5.7.

5.10 A Contratada deverá estar pronta para atuar com agilidade, mantendo equipe técnica habilitada e qualificada para os serviços, bem como todos os equipamentos, ferramentas e peças de reposição eventualmente necessárias aos atendimentos.



5.11 Nos casos em que for identificada falha física de hardware que comprometa total ou parcialmente a operação da solução, a Contratada deverá adotar imediatamente todas as medidas tecnicamente necessárias ao restabelecimento da solução dentro do SLA definido para a criticidade do incidente, empregando, conforme tecnicamente adequado à ocorrência, contingência temporária, appliance substituto, equipamento reserva ou solução técnica equivalente. Quando necessária a substituição física definitiva do equipamento, esta deverá ocorrer no prazo máximo de 2 (dois) dias úteis, por equipamento de capacidade igual ou superior, sem comprometer os tempos máximos de restabelecimento previstos no item 5.8.

Dos dados armazenados e segurança da informação

5.12 A Contratada e seus profissionais deverão respeitar a Política de Segurança da Informação da Câmara Municipal de Divinópolis, bem como as demais normas aplicáveis a tratamento de dados e segurança da informação.

5.13 Todas as informações obtidas pela Contratada em razão da execução contratual deverão ser tratadas como confidenciais, incluindo, entre outras, dados, documentos, topologia de rede, configurações, regras de firewall, vulnerabilidades identificadas, credenciais, informações de endereçamento, registros de eventos, logs e demais informações técnicas ou institucionais relacionadas à infraestrutura da Câmara Municipal. É vedada sua reprodução, utilização, compartilhamento ou divulgação para finalidade diversa da execução do contrato, salvo mediante autorização expressa da Administração ou quando decorrente de obrigação legal, devendo ser observadas as disposições da Constituição Federal, da Lei nº 14.133/2021, da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) e das demais normas aplicáveis.

5.13.1 A obrigação de sigilo e confidencialidade prevista no item anterior aplica-se à Contratada, a seus representantes, empregados, parceiros, prestadores de serviços e demais terceiros por ela utilizados, permanecendo vigente mesmo após o encerramento ou término da contratação.

5.14 Ao término da vigência contratual, em caso de não renovação, substituição da solução ou encerramento do contrato, a contratada deverá providenciar a retirada do equipamento fornecido em até 15 (quinze) dias úteis, responsabilizando-se pela destinação ambientalmente adequada, descarte ecológico quando aplicável e sanitização segura de dados eventualmente armazenados no equipamento.

Do Backup das Configurações da Solução

5.15 A solução contratada deverá disponibilizar funcionalidade de backup periódico e automatizado das configurações do appliance de firewall, configurável para execução com periodicidade mínima diária, bem como permitir a geração de cópias adicionais sob demanda e a restauração das configurações quando necessária.

5.16 A funcionalidade de backup deverá permitir a retenção de, no mínimo, 5 (cinco) versões válidas das configurações, com identificação das versões existentes e possibilidade de



restauração em caso de falha, erro operacional, substituição de equipamento, atualização malsucedida, desastre ou necessidade de reversão.

5.17 A configuração, administração, acompanhamento e validação das rotinas de backup, incluindo a verificação de sua execução, integridade, disponibilidade e retenção, bem como a geração de cópia extraordinária antes de alterações relevantes em regras, VPNs, NAT, SD-WAN, integrações, atualizações de firmware ou outras mudanças com potencial impacto operacional, serão realizadas pela empresa contratada para a prestação dos serviços especializados correlatos, responsável pela administração e sustentação operacional da solução.

5.17.1 A responsabilidade operacional atribuída à empresa contratada para a prestação dos serviços especializados correlatos não afasta a obrigação da Contratada de manter disponíveis, licenciados e plenamente funcionais, durante toda a vigência contratual, os recursos tecnológicos de backup, versionamento e restauração exigidos para a solução.

6 DAS OBRIGAÇÕES:

6.1 Obrigações da Contratante:

6.1.1 A Câmara Municipal de Divinópolis deve cumprir todas as obrigações constantes neste instrumento e em seus anexos, observando, ainda, as obrigações a seguir dispostas:

6.1.1.1 Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com o Instrumento contratual, com o Termo de Referência e seus anexos;

6.1.1.2 Receber o objeto no prazo e condições estabelecidas este Termo de Referência;

6.1.1.3 Propiciar todas as facilidades para que a Contratada possa executar os serviços dentro das normas e condições deste Termo de Referência.

6.1.1.4 Notificar a Contratada, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, ou na prestação de serviços, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

6.1.1.5 Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pela Contratada;

6.1.1.6 Efetuar o pagamento à Contratada do valor correspondente ao fornecimento do objeto, no prazo, forma e condições estabelecidos no presente Contrato;



6.1.1.7 Aplicar à Contratada as sanções motivadas pela inexecução total ou parcial do Contrato;

6.1.1.8 Cientificar o órgão de representação judicial da Procuradoria da Câmara para adoção das medidas cabíveis quando do descumprimento de obrigações pela Contratada;

6.1.1.9 Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

6.1.1.10 Concluída a instrução do requerimento, a Administração terá o prazo de 15 (quinze) dias úteis para decidir, admitida a prorrogação motivada por igual período.

6.1.2 A Administração não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução de eventual contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

6.2 Obrigações da Contratada

6.2.1 A contratada deve cumprir todas as obrigações constantes neste instrumento e em seus anexos, assumindo exclusivamente como seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

6.2.1.1 Responsabilizar-se integralmente, nos termos do contrato, pelo fornecimento, licenciamento e garantia da solução de firewall, bem como pela segurança dos dados que tratar, acessar ou armazenar em decorrência do suporte ou dos recursos sob sua responsabilidade, nos termos da legislação vigente;

6.2.1.2 Fornecer suporte técnico especializado relacionado ao appliance NGFW e aos demais componentes da solução fornecida, incluindo hardware, firmware, licenciamentos, subscrições e funcionalidades nativas, observadas as responsabilidades e os níveis de serviço estabelecidos neste Termo de Referência, durante toda a vigência contratual e sem ônus adicional para a Contratante;

6.2.1.3 Manter canal de atendimento apto ao recebimento de qualquer chamado para atendimentos técnicos;

6.2.1.4 Atender aos chamados de manutenção nos prazos previstos no item 5.8, observadas as regras de contagem estabelecidas no item 5.9 deste Termo de



Referência;

- 6.2.1.5** Prestar os serviços de suporte técnico na forma e dia solicitados pela Contratante, bem como executá-los na forma estatuída neste documento e dentro das normas técnicas vigentes;
- 6.2.1.6** Disponibilizar a seus técnicos, todos os equipamentos, ferramentas e EPIs necessários para a prestação dos serviços;
- 6.2.1.7** Manter mão de obra suficiente para garantir a execução dos serviços, durante o prazo de vigência do contrato;
- 6.2.1.8** Prestar apoio técnico necessário à implantação, configuração, integração e operação da solução, observadas as responsabilidades e os limites estabelecidos na contratação específica dos serviços especializados;
- 6.2.1.9** Garantir a atualização da plataforma de segurança sempre que o equipamento fornecido entrar em processo de descontinuidade, fim de suporte, fim de vida útil, incompatibilidade com licenças vigentes ou incapacidade comprovada de atendimento aos requisitos mínimos de desempenho e segurança contratados, quando tais condições comprometerem o suporte, a atualização, a segurança ou a continuidade operacional da solução, mediante substituição por equipamento equivalente ou superior, regularmente suportado pelo fabricante e plenamente compatível com os requisitos contratados, sujeita à prévia aprovação da Administração, sem ônus adicional para a Contratante;
- 6.2.1.10** Adotar medidas corretivas, contingenciais ou substitutivas necessárias ao restabelecimento do serviço, em caso de falha de hardware que comprometa a operação da solução, dentro dos prazos de SLA definidos neste documento;
- 6.2.1.11** Realizar a substituição definitiva do appliance NGFW, por equipamento de capacidade igual ou superior, quando forem registradas 04 (quatro) ou mais ocorrências de falhas recorrentes atribuíveis ao hardware ou aos componentes da solução sob responsabilidade da Contratada, no período de 60 (sessenta) dias corridos, devidamente comprovadas por registros de chamados técnicos, observados os prazos e as condições de substituição estabelecidos no item 5.11 deste Termo de Referência, sem ônus adicional para a Contratante;
- 6.2.1.12** A contratada deverá fornecer acesso a especialistas, preferencialmente do fabricante da solução fornecida, com atendimento humano especializado em língua portuguesa via chat, telefone ou e-mail;
- 6.2.1.13** Responsabilizar-se pela retirada e destinação ambientalmente correta de todas as peças e materiais eventualmente substituídos nos equipamentos, obedecendo à legislação vigente;
- 6.2.1.14** Providenciar a retirada do equipamento fornecido ao término ou



encerramento da contratação, observados o prazo, as condições e as responsabilidades estabelecidas no item 5.14 deste Termo de Referência;

6.2.1.15 Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior (art. 137, II) e prestar todo esclarecimento ou informação por eles solicitados;

6.2.1.16 Substituir, reparar, corrigir, remover ou refazer, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

6.2.1.17 Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou a terceiros, não reduzindo essa responsabilidade à fiscalização ou ao acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos;

6.2.1.18 Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas, bens ou dados de terceiros;

6.2.1.19 Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;

6.2.1.20 Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

6.2.1.21 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 do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021;

6.2.1.22 Orientar e treinar seus empregados sobre os deveres previstos na Lei nº 13.709, de 14 de agosto de 2018, adotando medidas eficazes para proteção de dados pessoais a que tenha acesso por força da execução deste contrato;

6.2.1.23 Não permitir a utilização de qualquer trabalho de menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

7 GESTÃO E FISCALIZAÇÃO DO CONTRATO

7.1 A contratação será formalizada por meio de instrumento contratual, conforme o art. 95 da



Lei nº 14.133, de 2021.

- 7.2** O contrato terá vigência de 12 (doze) meses, contados a partir da assinatura do contrato, podendo ser prorrogado sucessivamente, até a vigência máxima de 10 (dez) anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.
- 7.3** O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133/2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.
- 7.4** As comunicações entre a Contratante e a Contratada deverão ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.
- 7.5** A fiscalização do contrato será exercida por servidor(res) designado(s) pela Administração, ao qual competirá acompanhar, fiscalizar, conferir e avaliar a execução do objeto, bem como dirimir e desembaraçar quaisquer dúvidas e pendências que surgirem, determinando o que for necessário à regularização das faltas, falhas, problemas ou defeitos observados, e os quais de tudo darão ciência à contratada, conforme determina o art. 117 da Lei nº 14.133/21 e arts. 82 e seguintes da Portaria nº 188, de 20 de dezembro de 2023, desta Câmara Municipal.
- 7.5.1** As funções de fiscalização do contrato serão subdivididas em técnica e administrativa, e poderão ser exercidas por um ou dois fiscais, a critério da Administração.

Da fiscalização técnica e administrativa

- 7.6** Caberá ao fiscal do contrato e, nos seus afastamentos e impedimentos legais, ao seu substituto, o apoio técnico e operacional ao gestor do contrato, em especial:
- 7.6.1** Atestar a conformidade dos serviços prestados em relação aos termos estabelecidos neste Termo de Referência e seus anexos;
- 7.6.2** Zelar pelo cumprimento das normas técnicas aplicáveis ao objeto desta contratação;
- 7.6.3** Fiscalizar toda a execução do contrato para que sejam cumpridas as condições estabelecidas no ato da contratação, de modo a assegurar os resultados almejados pela administração;
- 7.6.4** Notificar o fornecedor contratado sempre que se observarem irregularidades nos serviços prestados, solicitando a correção nos termos e prazos estabelecidos no instrumento contratual;
- 7.6.5** Comunicar ao gestor do contrato sempre que se verificarem inconsistências que inviabilizem a continuidade da prestação dos serviços;



7.6.6 Auxiliar o gestor do contrato na avaliação da qualidade dos serviços prestados pela contratada, apresentando sempre que possível dados técnicos e relatórios de quaisquer eventos ocorridos durante todo o período contratual, de forma a se analisar a viabilidade de eventuais prorrogações contratuais;

7.7 No desempenho das funções administrativas, caberá ao fiscal do contrato:

7.7.1 Prestar apoio administrativo ao gestor do contrato, com a realização das tarefas relacionadas ao controle dos prazos do contrato e à formalização de apostilamentos e de termos aditivos, ao acompanhamento do empenho e do pagamento;

7.7.2 Verificar a manutenção das condições de habilitação da Contratada, examinar a regularidade no recolhimento das contribuições fiscais, trabalhistas e previdenciárias e quanto ao cumprimento das obrigações trabalhistas e sociais, com a solicitação dos documentos comprobatórios pertinentes;

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

7.8 A contratada declara, antecipadamente, aceitar todas as condições, métodos e processos de inspeção, verificação e controle adotados pela fiscalização, obrigando-se a fornecer todos os dados, elementos e esclarecimentos solicitados.

7.9 A fiscalização não exclui ou reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, nem a exime de manter fiscalização própria.

7.10 A existência e a atuação da gestão e da fiscalização não diminuem a responsabilidade exclusiva da contratada em relação ao objeto e suas consequências, tanto para a Contratante quanto para terceiros. Da mesma forma, se ocorrerem irregularidades durante a execução do contrato, tais fatos não implicarão qualquer responsabilidade compartilhada por parte da Contratante ou de seus representantes.

7.11 A contratada deve, sem prejuízo das penalidades previstas, ressarcir imediatamente a Contratante por quaisquer danos causados devido a falhas em suas atividades.

8 CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

8.1 Para avaliar a qualidade na execução dos serviços, a Contratante utilizará o Instrumento de Medição de Resultados (IMR), conforme modelo previsto no Anexo III deste Termo de Referência.

8.2 O IMR verificará a conformidade da execução dos serviços com as exigências estabelecidas neste Termo de Referência e a obtenção dos resultados esperados, com base em critérios objetivos previamente definidos pela Câmara.

8.3 Os critérios estabelecidos no IMR servirão como base para a mensuração dos resultados alcançados pela Contratada, impactando diretamente no valor dos pagamentos devidos,



bem como podendo fundamentar a aplicação de penalidades, inclusive multas e eventual rescisão contratual, em caso de descumprimento.

Do recebimento

- 8.4** O recebimento provisório se dará no ato da entrega dos equipamentos e licenças mediante conferência, pela equipe de T.I e fiscal do Contrato, da conformidade dos equipamentos fornecidos às especificações constantes neste termo de referência e na proposta realinhada.
- 8.5** Constatada qualquer irregularidade, desconformidade ou pendência, a Contratada será formalmente comunicada para que proceda à respectiva correção ou substituição, sem prejuízo da aplicação das medidas e sanções cabíveis.
- 8.6** O recebimento definitivo ficará condicionado à verificação da conformidade do appliance NGFW e dos demais componentes da solução fornecida, incluindo licenciamentos, subscrições, documentação técnica, acessos oficiais, garantia, suporte técnico e funcionalidades exigidas neste Termo de Referência e em seus anexos, mediante conferência documental e verificações técnicas pertinentes às obrigações da Contratada. A conclusão dos serviços de implantação física, configuração lógica, migração, integração, testes e homologação operacional, atribuídos à contratação correlata de serviços especializados, não constituirá condição para o recebimento definitivo deste fornecimento, sem prejuízo da responsabilidade da Contratada por eventuais falhas ou desconformidades dos componentes da solução sob sua responsabilidade.
- 8.7** Constatadas pendências, falhas ou desconformidades, a Contratada deverá providenciar sua correção no prazo estabelecido pela Contratante, contado da respectiva comunicação, ficando o recebimento definitivo condicionado à comprovação da regularização.
- 8.8** O recebimento definitivo não afasta a responsabilidade da Contratada pela qualidade, adequação e funcionamento da solução durante toda a vigência contratual.

Dos pagamentos

- 8.9** O pagamento será efetuado em moeda corrente nacional, no prazo de até 10 (dez) dias úteis após o recebimento da nota fiscal, através de ordem bancária, para crédito em banco, agência e conta-corrente indicada pela contratada, ou por meio de boleto bancário.
- 8.10** Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, quando couber.
- 8.11** A empresa regularmente optante pelo Simples Nacional, nos termos da Lei Complementar 123/2006, 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.

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

8.13 A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhada 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 14.133/2021.

9 FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

9.1 O fornecedor será selecionado por meio da realização de procedimento licitatório, na modalidade PREGÃO, sob a forma eletrônica, a ser realizado através da plataforma de compras do Governo Federal – compras.gov.br – mediante seleção da melhor proposta pelo critério de MENOR PREÇO GLOBAL, nos termos da Lei 14.133/2021.

9.2 Na apresentação das propostas, os fornecedores deverão atentar-se quanto às especificações do objeto que se encontram neste Termo de Referência. Nos preços ofertados deverão estar inclusos todos os custos diretos e indiretos inerentes ao objeto desta contratação, inclusive custos logísticos e de suporte técnico.

9.3 Não será admitido a nenhum licitante ofertar lance que não englobe a totalidade do serviço demandado, estando os licitantes sujeitos às penalidades cabíveis, em caso de descumprimento.

9.4 As empresas interessadas em participar da disputa serão integralmente responsáveis pela avaliação e levantamento dos custos relativos à execução do objeto, sendo inteiramente responsáveis por eventuais prejuízos decorrentes de avaliação equivocada ou da sua ausência.

9.5 O licitante provisoriamente classificado em primeiro lugar deverá apresentar, quando convocado pela Administração, na fase de julgamento da proposta, a documentação técnica oficial do fabricante relativa à solução de Firewall NGFW ofertada, incluindo catálogos, folders, datasheets, fichas técnicas ou outros documentos técnicos oficiais ou equivalentes, conforme previsto no item 9.31 deste Termo de Referência, que permitam a verificação objetiva do atendimento às especificações e aos requisitos técnicos exigidos neste Termo de Referência e em seus anexos. A documentação será utilizada para análise da conformidade técnica da proposta, não se confundindo com os documentos de habilitação técnico-operacional da licitante, observados os procedimentos de diligência e eventual demonstração técnica previstos neste instrumento. O não atendimento aos requisitos técnicos mínimos exigidos, após a análise da documentação apresentada e, quando cabíveis, os procedimentos de diligência e demonstração técnica, implicará a



desclassificação da proposta, observadas as disposições do Edital e da legislação aplicável.

Exigências de habilitação

9.6 Previamente à formalização da contratação, a Administração verificará o eventual descumprimento das condições para fornecimento à Administração Pública, especialmente quanto à existência de sanção que a impeça, mediante a consulta a cadastros informativos oficiais, tais como:

9.6.1 SICAF;

9.6.2 Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS, mantido pela Controladoria-Geral da União (www.portaldatransparencia.gov.br/ceis);

9.6.3 Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/cnep>).

9.7 A consulta aos cadastros será realizada em nome da empresa interessada e de seu sócio majoritário, por força do artigo 12 da Lei 8.429/1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

9.8 Caso atendidas as condições para fornecimento, a habilitação do interessado será verificada por meio do SICAF, nos documentos por ele abrangidos.

9.9 É dever do interessado manter atualizada a respectiva documentação constante do SICAF, ou encaminhar, quando solicitado pela Administração, a respectiva documentação atualizada.

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

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

9.12 Para fins de habilitação, deverá o interessado comprovar os requisitos de habilitação, que serão exigidos conforme sua natureza jurídica.

Habilitação jurídica

9.13 Para sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada – EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a



cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores.

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

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

9.16 Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

9.17 Prova de inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ);

9.18 Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria Geral da Fazenda Nacional (PGFN) referente a todos os créditos tributários federais e à dívida ativa da União;

9.19 Prova de regularidade com Fundo de Garantia do Tempo de serviço (FGTS);

9.20 Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante apresentação de certidão negativa ou positiva com efeito de negativa.

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

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

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

9.24 Declaração de que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do art. 7º. XXXIII da Constituição Federal.

9.25 Para ME e EPP, declaração de que, no ano-calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

Qualificação Econômica-Financeira



9.26 Certidão negativa de falência expedida pelo distribuidor da sede do licitante (Lei Federal nº 14.133/21, art. 69, caput, II).

Habilitação técnica da empresa

9.27 Para fins de habilitação técnica, a licitante deverá comprovar aptidão para a execução do objeto desta contratação, mediante apresentação de Atestado de Capacidade Técnica Operacional, expedido por pessoa jurídica de direito público ou privado para a qual tenha fornecido ou disponibilizado solução de segurança de borda do tipo NGFW/UTM ou tecnologia equivalente, contemplando equipamentos ou appliances, licenciamento ou subscrições, garantia, atualização tecnológica e suporte técnico em ambiente corporativo ou institucional de complexidade compatível.

9.27.1 Para fins de comprovação da aptidão operacional, os atestados deverão demonstrar experiência na execução dos serviços pelo período mínimo de **1 (um) ano**, não havendo obrigatoriedade de serem ininterruptos.

9.27.2 Serão admitidos atestados relativos a soluções de fabricantes distintos daquele ofertado, desde que comprovem experiência em tecnologias e atividades de natureza e complexidade compatíveis com o objeto, não sendo exigida identidade de marca ou fabricante.

9.27.3 Será admitida a apresentação de um ou mais atestados complementares, desde que, em conjunto, comprovem a experiência operacional da empresa, as características compatíveis com o objeto da contratação, bem como atendam ao período mínimo de execução estabelecido no item 9.27.4.

9.27.4 Somente serão aceitos atestados de capacidade técnica expedidos após a conclusão do contrato ou, caso o contrato ainda esteja em execução, desde que tenha decorrido, no mínimo, 1 (um) ano do início de sua execução, salvo se firmado para ser executado em prazo inferior.

9.27.5 Os atestados de capacidade técnica deverão conter, no mínimo, a identificação da pessoa jurídica emitente, CNPJ, endereço, identificação do responsável pela emissão, descrição dos serviços prestados, período de execução, local de prestação dos serviços, bem como demais informações necessárias à verificação da compatibilidade com o objeto da contratação.

9.27.6 Os atestados deverão ser emitidos em documento formal da contratante, preferencialmente em papel timbrado, ou outro meio idôneo e identificação do emitente, devendo conter assinatura do responsável legal ou de pessoa com poderes para atestar a execução dos serviços.

9.27.7 Serão admitidos atestados assinados física ou eletronicamente, desde que seja possível verificar a autoria e a integridade do documento, mediante certificação



digital, código de validação, sistema eletrônico de verificação ou outro meio idôneo de conferência.

9.27.8 Quando a comprovação da experiência mínima exigida decorrer da apresentação de mais de um atestado, os documentos devem ser apresentados em ordem cronológica, acompanhados, quando necessário, de quadro-resumo indicativo dos períodos, quantitativos e contratantes, a fim de facilitar a análise pela Administração.

9.27.9 Sempre que necessário para a adequada verificação da capacidade técnica da licitante, a Administração poderá solicitar a apresentação de outros documentos idôneos relacionados aos atestados apresentados, com a finalidade de complementar ou esclarecer as informações neles constantes.

9.27.10 Certificações, credenciamentos ou reconhecimentos emitidos por fabricantes ou desenvolvedores poderão ser apresentados como elementos complementares, não substituindo os atestados de capacidade técnica exigidos para comprovação da capacidade técnico-operacional.

9.27.11 Caso haja necessidade, a Administração reserva-se o direito de solicitar a apresentação de cópia da(s) Nota(s) Fiscal(is) correspondentes ao(s) contratos ou Atestado(s) de Capacidade Técnica apresentados.

9.28 A licitante deverá comprovar que a solução ofertada é proveniente de cadeia legítima de fornecimento e que dispõe dos meios necessários para assegurar os licenciamentos, subscrições, atualizações, garantia e suporte técnico exigidos durante a vigência contratual. Essa comprovação possui finalidade distinta da qualificação técnico-operacional prevista no item 9.27 e não substitui os respectivos atestados de capacidade técnica.

9.28.1 A comprovação prevista no item 9.28 poderá ser realizada, conforme o modelo comercial, de distribuição ou de suporte adotado pelo fabricante ou desenvolvedor da solução, mediante um ou mais dos seguintes meios:

9.28.1.1 Declaração de parceria, certificado de distribuidor, revendedor, integrador, parceiro autorizado ou documento equivalente emitido pelo fabricante, desenvolvedor ou distribuidor oficial da solução;

9.28.1.2 Registro ou credenciamento em programa oficial de parceiros, canais, integradores, revendedores, prestadores de serviços ou equivalente;

9.28.1.3 Documento emitido pelo fabricante, desenvolvedor, distribuidor oficial ou representante autorizado;

9.28.1.4 Consulta a portal, diretório ou sistema oficial do fabricante ou desenvolvedor;

9.28.1.5 Documentação de licenciamento, subscrição, garantia, suporte, números



de série, direitos de suporte ou instrumentos equivalentes;

9.28.1.6 Comprovação de suporte prestado diretamente pelo fabricante ou desenvolvedor; ou

9.28.1.7 Outro documento ou mecanismo idôneo e equivalente que demonstre objetivamente a legitimidade do fornecimento e a disponibilidade dos recursos e serviços exigidos.

9.29 O licitante deverá disponibilizar as informações necessárias à verificação da legitimidade dos atestados apresentados, mediante código de validação, sistema eletrônico de verificação, consulta junto ao emitente ou outro meio idôneo que possibilite à Administração confirmar a autenticidade, a validade e a correspondência das informações constantes do documento.

Da validação técnica da solução ofertada

9.30 A validação técnica da solução ofertada terá por finalidade verificar o atendimento aos requisitos mínimos estabelecidos neste Termo de Referência, conforme os critérios detalhados no anexo II deste documento.

9.31 A comprovação do atendimento aos requisitos e às especificações técnicas exigidos para a solução ocorrerá, prioritariamente, mediante a apresentação e análise de documentação técnica oficial do fabricante, a ser apresentada pelo licitante provisoriamente classificado em primeiro lugar, quando convocado pela Administração, na fase de julgamento da proposta, conforme previsto no item 9.5 deste Termo de Referência, podendo ser utilizados, isoladamente ou em conjunto, os seguintes documentos, conforme aplicável, desde que permitam a verificação objetiva dos requisitos exigidos:

- a) Datasheets oficiais;
- b) Manuais técnicos;
- c) Guias de administração (Administration Guide);
- d) Guias de instalação;
- e) Guias de arquitetura;
- f) Matrizes oficiais de funcionalidades (Feature Matrix);
- g) Notas técnicas;
- h) Release Notes;
- i) White Papers;
- j) Documentação disponibilizada oficialmente pelo fabricante;
- k) Certificações técnicas;
- l) Declarações oficiais emitidas pelo fabricante ou representante autorizado;
- m) Outros documentos técnicos oficiais ou equivalentes que permitam comprovar objetivamente o atendimento aos requisitos deste Termo de Referência e de seus anexos.



9.32 Quando a documentação apresentada não permitir comprovação objetiva de determinado requisito técnico exigido ou houver dúvida quanto ao seu atendimento, a Administração realizará diligência destinada exclusivamente ao esclarecimento da informação. A diligência poderá consistir na apresentação de documentação complementar, esclarecimentos técnicos ou demonstração técnica da ferramenta ofertada.

Demonstração técnica da solução apresentada

9.33 A demonstração técnica dos requisitos será realizada de forma complementar, somente quando a análise da documentação técnica apresentada pela licitante e a realização de diligência técnica forem insuficientes para comprovar, de forma objetiva, o atendimento de determinado requisito técnico da solução ofertada.

9.33.1 A demonstração será limitada às funcionalidades ou requisitos específicos objeto de dúvida, não sendo necessária a demonstração integral da solução, a instalação definitiva dos equipamentos nas dependências da Câmara Municipal ou a reprodução integral de seu ambiente tecnológico.

9.34 A Administração especificará previamente quais requisitos serão objeto da demonstração, dentre aqueles apresentados no anexo II, vedada a exigência de funcionalidades, testes ou critérios de avaliação não previstos nos documentos da contratação.

9.34.1 A licitante convocada para a demonstração técnica deverá apresentá-la no prazo de até **03 (três) dias úteis**, contado do recebimento da convocação pela Administração.

9.35 A Demonstração Técnica poderá ser realizada presencialmente, por videoconferência, mediante compartilhamento de tela, acesso supervisionado a equipamento ou ambiente contendo a solução ofertada, apresentação prática de funcionalidade ou por outro meio tecnicamente adequado, desde que permita à Administração verificar, de maneira objetiva, o atendimento do requisito questionado.

9.36 A realização da Demonstração Técnica não implicará qualquer obrigação de fornecimento definitivo da solução, nem constituirá etapa de homologação, aceitação definitiva ou operação assistida, destinando-se exclusivamente à verificação do atendimento dos requisitos previamente estabelecidos.

Critério de avaliação da solução

9.37 A avaliação da documentação técnica, da eventual diligência técnica e da demonstração técnica, quando realizada, limitar-se-á à verificação objetiva do atendimento aos requisitos técnicos e funcionais previamente estabelecidos, conforme anexo II, deste Termo de Referência, incluindo, conforme aplicável, as características, funcionalidades, capacidades, desempenho, compatibilidade, integração, segurança e



mais especificações exigidas para a solução. A análise terá caráter exclusivamente verificatório, não havendo atribuição de pontuação, classificação técnica, comparação de mérito entre fabricantes ou soluções.

9.37.1 O resultado da avaliação será registrado, para cada requisito analisado, apenas como: () Atendeu; ou () Não atendeu;

9.38 A cada etapa de avaliação técnica realizada, a equipe técnica elaborará relatório devidamente fundamentado, no qual serão registrados os procedimentos adotados e os respectivos resultados. O relatório deverá consignar, quando cabível, a necessidade de realização de diligência técnica e, se necessário a demonstração técnica, bem como as conclusões quanto ao atendimento dos requisitos estabelecidos no Anexo II.

9.39 Caso a proponente não atenda aos requisitos estabelecidos nesta contratação para a solução de segurança a ser ofertada o pregoeiro convocará a licitante classificada em seguida para, se considerada habilitada, submeter-se à mesma avaliação técnica. O procedimento será repetido sucessivamente, respeitando-se a ordem de classificação, até que se identifique a solução de Firewall que atenda integralmente às exigências previstas neste Termo de Referência.

Qualificação técnica dos profissionais – Equipe técnica para suporte

9.40 A contratada deverá disponibilizar, durante toda a execução contratual, profissional ou equipe tecnicamente qualificada para prestar o suporte técnico relacionado ao appliance, firmwares, softwares, licenças, subscrições, atualizações e demais componentes da solução fornecida.

9.41 O profissional ou a equipe disponibilizada deverá possuir qualificação compatível com a tecnologia ofertada e capacidade técnica para realizar, no mínimo:

9.41.1 A interlocução técnica com a Câmara e com a empresa responsável pela implantação e administração da solução, quando necessário;

9.41.2 O diagnóstico inicial de falhas, indisponibilidades ou comportamentos anômalos relacionados aos componentes da solução contratada;

9.41.3 A análise e orientação quanto a problemas relacionados ao appliance, softwares, firmwares, licenças, subscrições e atualizações;

9.41.4 A abertura, acompanhamento e escalonamento de chamados junto ao fabricante, desenvolvedor ou estrutura oficial de suporte, quando necessária a atuação especializada; e

9.41.5 Acompanhamento das providências necessárias à solução das ocorrências relacionadas ao objeto contratado.

9.42 A disponibilização do profissional ou da equipe técnica constitui obrigação da Contratada para a adequada execução do objeto e não será exigida como requisito de



habilitação, devendo ser comprovada pela Contratada no momento da assinatura do contrato, mediante certificação emitida pelo fabricante ou desenvolvedor da solução ofertada, por instituição por ele reconhecida, ou por outro meio de comprovação técnica equivalente, desde que demonstre conhecimento e competência compatíveis com as atividades de suporte previstas neste Termo de Referência.

9.42.1 Serão admitidas certificações com diferentes denominações, níveis ou estruturas, desde que sua abrangência demonstre qualificação compatível com a tecnologia efetivamente ofertada. Não serão consideradas, isoladamente, suficientes as certificações de natureza exclusivamente comercial, de vendas ou meramente introdutória, que não demonstrem capacitação técnica para as atividades de suporte exigidas.

9.42.2 Na hipótese de o fabricante ou desenvolvedor da solução não possuir programa formal de certificação individual aplicável à tecnologia ofertada, será admitida comprovação equivalente de capacitação técnica, acompanhada, quando necessário, de comprovação de experiência profissional compatível com as atividades de suporte previstas neste Termo de Referência.

9.42.3 A qualificação exigida deverá guardar relação direta com o objeto da contratação, não sendo exigida certificação específica de determinado fabricante, modelo ou tecnologia quando houver outras formas objetivamente equivalentes de comprovação da capacidade técnica necessária à prestação do suporte.

Qualificação técnica dos profissionais – Instrutor do Treinamento

9.43 A qualificação do instrutor poderá ser comprovada mediante certificação técnica emitida pelo fabricante ou desenvolvedor da solução, por instituição por ele reconhecida, ou por outro meio de comprovação técnica equivalente, desde que demonstre conhecimento compatível com o conteúdo e as atividades de capacitação previstas.

9.43.1 A comprovação da qualificação do instrutor deverá ser apresentada pela contratada previamente à execução contratual, no ato da assinatura do contrato, mediante a documentação pertinente, ficando sua apresentação condicionada à verificação pela Administração quanto à compatibilidade da qualificação apresentada com o conteúdo e as atividades de treinamento previstas neste termo de referência.

9.44 Não será exigida denominação específica de certificação, nível de certificação, categoria de parceria ou vínculo com centro oficial de treinamento do fabricante, desde que a documentação apresentada demonstre, de forma objetiva, a qualificação técnica necessária para a realização do treinamento.

9.44.1 Certificações de natureza exclusivamente comercial, de vendas ou meramente introdutória não serão consideradas, isoladamente, suficientes para comprovar a qualificação técnica exigida.

9.45 Os documentos apresentados para comprovação da qualificação técnica do instrutor



deverão possuir mecanismo de validação ou verificação de autenticidade, mediante código, número de registro, endereço eletrônico, QR Code, sistema de consulta ou outro meio idôneo disponibilizado pelo fabricante, desenvolvedor, instituição certificadora ou entidade responsável pela emissão do documento, de forma a possibilitar à Administração a conferência de sua veracidade.

9.46 Quando o documento apresentado não dispuser de mecanismo próprio de validação, a contratada deverá fornecer, juntamente com o documento, os elementos necessários à sua comprovação, tais como declaração da entidade emissora, endereço eletrônico para consulta, identificação do responsável pela emissão ou outro meio documental idôneo que permita à Administração verificar sua autenticidade.

Da exequibilidade da proposta apresentada

9.47 Conforme disposto no art 34 da IN SEGES/ME nº 73 de 30 de setembro de 2022, será considerado indício de inexecução as propostas apresentadas com valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

9.47.1 A inexecução da proposta apresentada só será considerada após diligência do agente de contratação ou da comissão de contratação, quando o substituir, que comprove:

I – que o custo do licitante ultrapassa o valor da proposta;

II – que inexistirem custos de oportunidade capazes de justificar o vulto da oferta;

10 ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

10.1 O valor médio estimado para a contratação é de **R\$ 102.177,96 (cento e dois mil, cento e setenta e sete reais e noventa e seis centavos)** com base no valor médio encontrado no Mapa Comparativo de Preços resultante das pesquisas de mercado conforme cotações e metodologia apresentada em documento específico anexado ao processo.

11 ADEQUAÇÃO ORÇAMENTÁRIA

11.1 As despesas decorrentes da presente contratação estão programadas em dotações orçamentárias própria do exercício de 2026, prevista no orçamento da Câmara Municipal nas seguintes classificações:

11.1.1 Função programática: 01.001.001.01.122.1010.2003 – Gestão das atividades operacionais.

11.1.2 Natureza da despesa: Ficha 1199 – 3.3.90.40.00.00.00.00 Serviços de Tecnologia da Informação.



12 DISPOSIÇÕES GERAIS

12.1 As normas disciplinadoras deste Termo de Referência serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

12.2 Integram este Termo de Referência, para todos os fins e efeitos, os seguintes anexos e apêndices:

- 12.2.1** Anexo I – Detalhamento das especificações técnicas da solução;
- 12.2.2** Anexo II – Lista de verificação dos requisitos técnicos para avaliação;
- 12.2.3** Anexo III – Instrumento de medição de resultados (IMR);
- 12.2.4** Anexo IV – Modelo para formação de propostas;
- 12.2.5** Anexo V – Declaração de Limite de Faturamento ME/EPP.
- 12.2.6** Apêndice I – Estudo técnico preliminar (ETP).

Divinópolis, 20 de outubro de 2026.

Samuel Carlos da Silva Marques
Diretor de Administração e Suprimentos (em substituição)

De acordo.

Flávio Ramos
Secretário-Geral

Ciente da necessidade da contratação em tela e das informações prestadas, aprovo o termo de referência.

Israel da Farmácia
Presidente da Câmara Municipal de Divinópolis



ANEXO I - DETALHAMENTO DAS ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

1 - Arquitetura e Performance (Hardware) para suportar o tráfego crescente e a inspeção profunda de pacotes (DPI).

Arquitetura e Performance (Hardware) para suportar o tráfego crescente e a inspeção profunda de pacotes (DPI) deverá apresentar capacidade de processamento adequada ao ambiente da Câmara Municipal de Divinópolis, comprovada por documentação oficial do fabricante, considerando operação simultânea de firewall, mecanismos de prevenção de intrusão, antivírus/antimalware, controle de aplicações, conectividade segura, gerenciamento inteligente de links, filtragem de conteúdo e inspeção avançada de tráfego, sem degradação incompatível com os níveis mínimos de serviço definidos neste Termo de Referência e em seus anexos, devendo observar, no mínimo, os seguintes requisitos técnicos:

1.1. Conformidade Appliance

A solução deverá ser composta por appliance dedicado de segurança, com integração nativa ou homologada entre hardware, sistema operacional e licenciamento da plataforma ofertada, sendo vedado o uso de servidores genéricos, soluções improvisadas ou não homologadas pelo fabricante da plataforma de segurança.

1.2. Processamento e Memória

A solução deverá possuir recursos de processamento, memória e arquitetura adequada à operação simultânea dos serviços de firewall, prevenção de intrusões, antivírus/antimalware, conectividade segura, gerenciamento inteligente de links, controle de aplicações, filtragem de conteúdo e inspeção avançada de tráfego, devendo o desempenho ser comprovado por documentação oficial do fabricante.

1.3. Conectividade

O appliance deverá possuir interfaces de rede em quantidade suficiente para permitir a conexão simultânea de links WAN, redes LAN, DMZ, segmentação de redes internas, redes de visitantes e futuras expansões da infraestrutura, conforme dimensionamento da solução.

As interfaces deverão suportar velocidades compatíveis com os requisitos mínimos de desempenho estabelecidos neste Termo de Referência e em seus anexos.

1.4. Expansibilidade

A solução deverá possuir recursos que permitam futura evolução da conectividade para 10GbE ou superior, mediante interfaces nativas, portas SFP/SFP+, módulos de expansão ou tecnologia equivalente compatível com a arquitetura ofertada, sem necessidade de substituição integral da plataforma.



1.5. Especificações mínimas do appliance NGFW

Especificação	Mínimo Exigido
Quantidade de appliances	01 (um)
Número mínimo de dispositivos suportados, sem limitação técnica ou de licenciamento inferior a esse quantitativo	500
Interfaces de rede	10 interfaces Ethernet 10/100/1000 Mbps
Velocidade de cada interface	1 Gbps
Interface de console ou mecanismo equivalente	01 (uma) interface de console ou mecanismo equivalente de acesso administrativo local e recuperação, homologado pelo fabricante.
Instalação	Rack padrão 19" com kit de fixação
Throughput de Firewall	10 Gbps
Throughput de VPN	8,2 Gbps
NGFW / Threat Protection	1,5 Gbps
Throughput de Antivírus HTTP (HTTP AV Throughput)	7,3 Gbps
Throughput de IPS	5,3 Gbps
SSL/TLS Inspection	1 Gbps
Conexões simultâneas	1250000
Novas conexões por segundo	25000
Alimentação elétrica	Fonte Full Range (100~240 VCA, 50/60 Hz ou equivalente de acordo com o equipamento)

O appliance deverá atender integralmente às especificações mínimas estabelecidas, possuindo capacidade suficiente para suportar toda a demanda da rede institucional e a utilização simultânea das funcionalidades e mecanismos de segurança exigidos neste Termo de Referência e em seus anexos.

2 – Inteligência e Segurança (Software)

2.1. Controle de Aplicações e Análise Comportamental

Identificação e controle de aplicações independentemente da porta ou protocolo utilizado, incluindo redes sociais, aplicativos de comunicação, VPNs, proxies, serviços de acesso remoto, aplicações de streaming e demais serviços de camada 7, permitindo aplicação de políticas baseadas em comportamento, categoria, risco, usuário, grupo ou perfil de utilização.

2.2. Prevenção de Intrusão (IPS)

Inspeção de tráfego e análise de ameaças para identificação, bloqueio e mitigação de tentativas de invasão, exploração de vulnerabilidades, tráfego malicioso, malwares, ransomwares, trojans, worms, comunicações suspeitas e comportamentos maliciosos, utilizando, quando disponível na solução



ofertada, mecanismos de inteligência de ameaças (Threat Intelligence), reputação de IPs, domínios, URLs, arquivos ou tecnologias equivalentes.

2.3. Controle de Conteúdo

Filtro Web corporativo com categorização dinâmica de conteúdo, atualização contínua de categorias, criação de listas de permissão e bloqueio, políticas distintas por rede, usuário ou grupo, geração de relatórios de navegação e possibilidade de diagnóstico de bloqueios ou liberações de URLs.

2.4. Gestão de Certificados

Criação e revogação de certificados SSL/TLS via interface gráfica para inspeção de tráfego criptografado.

3. Conectividade e Redes Avançadas

3.1. Roteamento Dinâmico

Suporte a protocolos de roteamento dinâmicos aderentes a ambientes corporativos e integração com múltiplos links e redes, permitindo integração com múltiplas unidades administrativas ou ambientes de nuvem pública

3.2. VPN (Virtual Private Network)

Suporte a túneis VPN Site-to-Site e Client-to-Site, incluindo IPsec, SSL VPN, VPN baseada em TLS/SSL ou tecnologias equivalentes, com possibilidade de autenticação integrada a bases corporativas, geração de logs de conexão, autenticação e desconexão, com identificação dos eventos e das sessões conforme a modalidade de VPN utilizada, bem como disponibilização de relatórios de uso e alertas de conexão ou desconexão, quando suportados pela solução ofertada.

3.3. Serviços Críticos e Priorização de Tráfego

Suporte a DNS Dinâmico, NetFlow ou tecnologia equivalente, SNMP, NTP, DHCP Relay, recursos de análise de tráfego, QoS e demais funcionalidades de conectividade corporativa aderentes à arquitetura ofertada

4 – Gestão Centralizada, Monitoramento e Continuidade Operacional

A solução deverá oferecer mecanismo de gerenciamento centralizado, preferencialmente por meio de painel em nuvem, admitindo-se ambiente local, híbrido ou tecnologia equivalente, desde que permita administração unificada, monitoramento contínuo, gerenciamento centralizado do appliance, visualização, em tempo real, das informações operacionais e acompanhamento da saúde da solução. A plataforma deverá disponibilizar, no mínimo, os seguintes recursos:

4.1. Backup Automático das Configurações:

Realização de backup periódico e automatizado das configurações da solução, com retenção mínima de 5 (cinco) versões válidas para fins de restauração, contingência e manutenção da operação.



4.2. Visibilidade Operacional e Eventos de Segurança

Disponibilização de painéis, relatórios, gráficos e recursos de visualização operacional que permitam acompanhamento em tempo real dos eventos de segurança, podendo incluir representações estatísticas, históricas, geográficas ou equivalentes, quando suportadas pela solução ofertada.

4.3. Monitoramento e Alertas

Disponibilização de recursos de monitoramento contínuo com geração de alertas operacionais, podendo incluir aplicativo móvel, painel web, e-mail, integração com plataformas de monitoramento ou mecanismos equivalentes para notificação de indisponibilidade, degradação de links, perda de pacotes, latência elevada, falhas operacionais, eventos críticos de segurança ou indisponibilidade de serviços monitorados

4.4. Gerenciamento Inteligente de Links (SD-WAN)

Suporte a balanceamento de carga, failover automático e priorização de tráfego com base em critérios técnicos como latência, perda de pacotes, disponibilidade e desempenho dos links de comunicação.

4.5. Gerenciamento Centralizado de Políticas

Possibilidade de gerenciamento centralizado de regras, políticas de segurança, objetos de rede, VPNs, perfis de inspeção, relatórios e demais configurações relevantes da solução

4.6. Acompanhamento da Saúde Operacional

Disponibilização de informações relativas ao estado operacional do appliance, utilização de CPU, memória, armazenamento, interfaces, throughput, links, VPNs, qualidade dos links e demais indicadores relevantes para gestão da infraestrutura de segurança, possibilitando o acompanhamento contínuo da saúde operacional da solução, a identificação preventiva de degradações de desempenho, indisponibilidades, falhas operacionais e eventuais inconsistências de configuração que possam comprometer a segurança, a disponibilidade ou o desempenho do ambiente

4.7. Análise de Risco, Postura de Segurança e Recomendações:

A plataforma deverá disponibilizar recursos de avaliação contínua da postura de segurança (Security Posture Assessment), análise de risco da configuração, recomendações de boas práticas, alertas operacionais e histórico de eventos, permitindo acompanhar a conformidade das regras de firewall, NAT, VPN, usuários administrativos, senhas, objetos de rede, políticas de segurança, links e demais componentes críticos da solução, emitindo recomendações técnicas de melhoria sempre que aplicável.

4.8. Inteligência de Ameaças:

A solução deverá utilizar mecanismos de inteligência de ameaças (Threat Intelligence), quando disponíveis na plataforma ofertada, com atualização contínua de indicadores de comprometimento (IoCs), reputação de endereços IP, domínios, URLs, arquivos e demais informações relevantes para



prevenção, identificação e resposta a ameaças cibernéticas emergentes, podendo utilizar bases próprias do fabricante ou serviços equivalentes integrados.

5. - Requisitos de suporte e SLA (Nível de Serviço)

5.1. Substituição Proativa

A Contratada deverá assegurar a atualização tecnológica e a substituição do appliance NGFW, quando necessárias, observadas as condições, responsabilidades e exigências estabelecidas nos itens 1.6 e 6.2.1.9 do Termo de Referência, sem ônus adicional para a Contratante.

5.2. Suporte Direto

Acesso a atendimento humano especializado, prestado pelo fabricante, desenvolvedor da solução, representante autorizado, parceiro certificado ou equipe técnica formalmente habilitada para a solução ofertada, em língua portuguesa, por meio de chat, telefone, e-mail ou canais equivalentes.

5.3. Intervenção Remota

Possibilidade de suporte remoto especializado pelo fabricante, desenvolvedor da solução, parceiro autorizado ou equipe técnica formalmente habilitada, mediante autorização prévia da Contratante e observadas as políticas de segurança, auditoria e controle de acesso.

6. Aspectos Complementares da contratação

6.1. Treinamento e transferência de conhecimento

O treinamento técnico destinado à equipe de Tecnologia da Informação da Câmara Municipal deverá observar as condições de realização, carga horária, qualificação do instrutor, transferência de conhecimento e disponibilização de materiais estabelecidas nos itens 5.1.4 a 5.1.7 do Termo de Referência. O conteúdo programático deverá contemplar, no mínimo, quando aplicável às funcionalidades efetivamente contratadas:

- a) Arquitetura e funcionamento geral da solução;
- b) Administração das políticas de segurança;
- c) Criação, alteração e revisão de regras de firewall;
- d) Administração de objetos, grupos e serviços;
- e) Configuração e administração de VPNs;
- f) Administração de regras de NAT;
- g) Administração das funcionalidades de segurança disponibilizadas pela solução;
- h) Monitoramento operacional, análise de eventos e interpretação de logs;
- i) Geração e interpretação de relatórios técnicos, quando aplicável;



- j) Administração dos mecanismos de autenticação integrados;
- k) Administração dos backups das configurações e procedimentos de restauração;
- l) Procedimentos para atualização da solução, observadas as responsabilidades previstas no contrato;
- m) Boas práticas de administração, segurança da informação e continuidade operacional;
- n) Procedimentos básicos para identificação, tratamento e escalonamento de incidentes;
- o) Esclarecimento de dúvidas e realização de atividades práticas, sempre que tecnicamente possível.

6.2. Conformidade com a LGPD

A solução deve permitir a exportação de logs de acesso de usuários para fins de auditoria, conforme princípios de segurança, prevenção e responsabilização. Também deverá possibilitar a guarda centralizada de logs pelo período definido na política institucional da Câmara Municipal de Divinópolis ou conforme legislação vigente e a exportação em formatos auditáveis (como CSV ou PDF). Também deverá possuir recursos que permitam identificar usuários, horários, origem dos acessos e ações executadas no ambiente de rede, quando tecnicamente aplicável à solução ofertada e à arquitetura implantada, em conformidade com o princípio da responsabilização (accountability) previsto na Lei Geral de Proteção de Dados (LGPD).

6.3. Suporte técnico

Independentemente da origem da solução ofertada, é indispensável que esta disponha de suporte técnico disponível em língua portuguesa e acessível à Administração nos níveis de serviço contratados, mecanismos compatíveis com políticas de soberania de dados e recursos adequados de auditoria, rastreabilidade de acessos e gestão da segurança da informação, contribuindo para o atendimento dos princípios e obrigações aplicáveis da LGPD, para a continuidade operacional, a segurança institucional e a adequada governança do ambiente tecnológico.



ANEXO II

LISTA DE VERIFICAÇÃO DOS REQUISITOS TÉCNICOS PARA AVALIAÇÃO

1. OBJETO

Este anexo estabelece as especificações técnicas mínimas para a contratação de solução integrada de segurança de rede do tipo Firewall de Próxima Geração (NGFW/UTM), em regime de locação com cessão de uso/comodato, incluindo 01 (um) appliance dedicado, subscrição e licenciamento durante toda a vigência contratual, garantia, suporte técnico do fabricante ou parceiro autorizado, gerenciamento centralizado, atualização tecnológica e demais componentes necessários ao pleno funcionamento da solução.

Os serviços especializados de implantação física, configuração lógica, migração de regras, integração, orientação operacional relacionada ao ambiente efetivamente implantado, testes, homologação, operação assistida e sustentação operacional serão executados em contratação correlata, cabendo à contratada deste objeto fornecer o equipamento, as licenças, documentação, acesso aos portais – quando aplicável, versões dos firmwares e suporte técnico necessário à implantação e à continuidade tecnológica da plataforma.

Da comprovação dos requisitos técnicos

A comprovação dos requisitos estabelecidos neste Anexo II será realizada mediante documentação técnica oficial do fabricante ou desenvolvedor da solução ofertada, conforme previsto no item 9.31 do Termo de Referência, admitidos documentos técnicos oficiais equivalentes que permitam a verificação objetiva do atendimento às especificações exigidas.

A ausência de indicação específica na coluna “Forma de comprovação” não dispensa a comprovação do respectivo requisito. Quando indicada, a forma de comprovação terá caráter orientativo, sendo admitida documentação oficial equivalente que demonstre objetivamente o atendimento à exigência.

Nos casos em que a documentação apresentada não permitir a comprovação objetiva de determinado requisito, poderão ser adotados os procedimentos de diligência ou demonstração técnica previstos neste Termo de Referência.

Da aplicabilidade e avaliação dos requisitos técnicos

Os requisitos técnicos mínimos estabelecidos neste Anexo II são de atendimento obrigatório, observadas as condições de aplicabilidade expressamente previstas e a compatibilidade com as especificações do Termo de Referência e do Estudo Técnico Preliminar.

As expressões “quando aplicável”, “quando tecnicamente aplicável” ou equivalentes, quando relacionadas à arquitetura ou ao ambiente institucional, condicionam a utilização ou ativação da funcionalidade, não dispensando a disponibilidade da capacidade técnica exigida, salvo disposição expressa em contrário.

As funcionalidades expressamente identificadas como complementares ou facultativas não



constituirão requisitos técnicos mínimos obrigatórios para fins de avaliação da conformidade da proposta, nem poderão fundamentar sua desclassificação pela simples ausência do recurso.

A avaliação deverá observar a natureza de cada requisito, verificando objetivamente o atendimento às capacidades técnicas obrigatórias da solução ofertada, independentemente de sua efetiva ativação ou configuração operacional, quando estas estiverem condicionadas às características do ambiente institucional. Quando necessário, deverá ser registrada a justificativa técnica da condição de aplicabilidade, vedada a criação de exigências adicionais não previstas no Termo de Referência e em seus anexos.

2. ESCOPO E COMPOSIÇÃO DA SOLUÇÃO

Item	Requisito técnico mínimo	Forma de comprovação	Resultado
2.1	Fornecimento de 01 (um) appliance físico dedicado de Firewall NGFW, novo, dimensionado para atender integralmente à demanda institucional e aos requisitos mínimos estabelecidos neste Termo de Referência e em seus anexos.		() Atendeu () Não atendeu
2.2	Subscrição ou licenciamento completo dos recursos de segurança necessários ao pleno funcionamento do appliance e da solução durante toda a vigência contratual.		() Atendeu () Não atendeu
2.3	Licenciamento, habilitação ou disponibilização de conectividade segura via VPN IPsec, SSL VPN, TLS/SSL ou tecnologia equivalente.		() Atendeu () Não atendeu
2.4	Gerenciamento centralizado em nuvem, local, híbrido ou solução equivalente, válido durante toda a vigência contratual.		() Atendeu () Não atendeu
2.5	Suporte técnico do fabricante, desenvolvedor, representante autorizado, parceiro certificado ou equipe formalmente habilitada, em língua portuguesa.		() Atendeu () Não atendeu
2.6	Atualizações de firmware, software, assinaturas, bases de reputação, mecanismos de inteligência de ameaças (Threat Intelligence) ou tecnologia funcionalmente equivalente e demais mecanismos de proteção durante toda a vigência contratual.		() Atendeu () Não atendeu

3. REQUISITOS GERAIS DOS APPLIANCES

Item	Requisito técnico mínimo	Forma de comprovação	Resultado
3.1	O appliance deverá ser novo, de primeiro uso, sem histórico de utilização, vedada a entrega de equipamentos reconicionados ou refurbished.		() Atendeu () Não atendeu



Item	Requisito técnico mínimo	Forma de comprovação	Resultado
3.2	O equipamento deverá estar em linha de produção e comercialização regular na data da proposta e da entrega.		() Atendeu () Não atendeu
3.3	O equipamento não poderá estar em condição de End-of-Life (EOL), End-of-Sale (EOS) ou End-of-Support (EOSP).		() Atendeu () Não atendeu
3.4	A plataforma deverá possuir suporte oficial vigente durante toda a execução contratual.		() Atendeu () Não atendeu
3.5	A solução deverá ser composta por appliance dedicado de segurança, com integração nativa ou homologada entre hardware, sistema operacional e licenciamento.		() Atendeu () Não atendeu
3.6	Será vedado o uso de servidor genérico, equipamento improvisado ou solução não homologada pelo fabricante da plataforma ofertada.		() Atendeu () Não atendeu
3.7	Não serão aceitos softwares, firmwares ou componentes integrantes da solução em versões beta, experimentais ou não oficiais.	Documentação oficial do fabricante, release notes, declaração oficial ou documentação equivalente.	() Atendeu () Não atendeu

4. DIMENSIONAMENTO E CAPACIDADE OPERACIONAL

Item	Requisito técnico mínimo	Forma de comprovação	Resultado
4.1	Capacidade operacional estimada para atendimento simultâneo de aproximadamente 350 dispositivos, devendo a solução possuir capacidade para suportar, no mínimo, 500 dispositivos, de forma a permitir a expansão prevista durante a vigência contratual.	Datasheet ou documentação técnica oficial do fabricante.	() Atendeu () Não atendeu
4.2	Suporte aos 2 (dois) links dedicados previstos, cada um com capacidade estimada de 1 Gbps Full Duplex, além de múltiplos links e futuras expansões.	Datasheet ou documentação técnica oficial do fabricante.	() Atendeu () Não atendeu
4.3	Capacidade para operação simultânea de firewall, IPS, antivírus/antimalware, controle de aplicações, filtragem de conteúdo, VPN, SD-WAN e inspeção avançada de tráfego.	Datasheet ou documentação técnica oficial do fabricante.	() Atendeu () Não atendeu



Item	Requisito técnico mínimo	Forma de comprovação	Resultado
4.4	Recursos de processamento, memória, armazenamento e arquitetura suficientes para a operação simultânea das funcionalidades licenciadas.	Datasheet ou documentação técnica oficial do fabricante.	() Atendeu () Não atendeu
4.5	Capacidade de expansão progressiva de processamento, interfaces, licenciamento, retenção de logs e recursos de segurança, sem substituição integral precoce da plataforma.	Datasheet ou documentação técnica oficial do fabricante.	() Atendeu () Não atendeu
4.6	Throughput de Firewall de, no mínimo, 10 Gbps do appliance.	Datasheet ou documentação técnica oficial do fabricante.	() Atendeu () Não atendeu
4.7	Throughput de VPN de, no mínimo, 8,2 Gbps do appliance.	Datasheet ou documentação técnica oficial do fabricante.	() Atendeu () Não atendeu
4.8	NGFW / Threat Protection de, no mínimo, 1,5 Gbps do appliance.	Datasheet ou documentação técnica oficial do fabricante.	() Atendeu () Não atendeu
4.9	Throughput de Antivírus HTTP (HTTP AV Throughput) de, no mínimo, 7,3 Gbps do appliance.	Datasheet ou documentação técnica oficial do fabricante.	() Atendeu () Não atendeu
4.10	Throughput de IPS de, no mínimo, 5,3 Gbps do appliance.	Datasheet ou documentação técnica oficial do fabricante.	() Atendeu () Não atendeu
4.11	SSL/TLS Inspection de, no mínimo, 1 Gbps do appliance.	Datasheet ou documentação técnica oficial do fabricante.	() Atendeu () Não atendeu
4.12	Capacidade de, no mínimo, 1.250.000 conexões simultâneas do appliance.	Datasheet ou documentação técnica oficial do fabricante.	() Atendeu () Não atendeu
4.13	Capacidade de, no mínimo, 25.000 novas conexões por segundo do appliance.	Datasheet ou documentação técnica oficial do fabricante.	() Atendeu () Não atendeu



5. INTERFACES, CONECTIVIDADE E EXPANSIBILIDADE

Item	Requisito técnico mínimo	Forma de comprovação	Resultado
5.1	O appliance deverá possuir, no mínimo, 10 (dez) interfaces Ethernet 10/100/1000 Mbps, ou interfaces de tecnologia superior compatível, em quantidade suficiente para suportar WAN, LAN, DMZ, segmentação de rede, rede de visitantes e futuras expansões.		() Atendeu () Não atendeu
5.2	Suporte a interfaces 1GbE e, nativamente ou por módulos de expansão, interfaces 10GbE, SFP/SFP+ ou tecnologia superior/equivalente.		() Atendeu () Não atendeu
5.3	O appliance deverá possuir suporte à agregação de interfaces de rede e à segmentação lógica por VLAN, ficando a utilização e a configuração dessas funcionalidades condicionadas às necessidades e à arquitetura de rede efetivamente implantada.		() Atendeu () Não atendeu
5.4	Compatibilidade com conexões em cobre e fibra óptica, conforme os módulos e transceptores ofertados.		() Atendeu () Não atendeu
5.5	Todos os cabos, adaptadores, transceptores, módulos, fontes, acessórios e elementos necessários à operação do appliance deverão ser fornecidos pela contratada.		() Atendeu () Não atendeu
5.6	A solução deverá possuir interface de console ou mecanismo equivalente de acesso administrativo local e recuperação, homologado pelo fabricante.		() Atendeu () Não atendeu
5.7	O appliance deverá ser compatível com instalação em rack padrão 19", com fornecimento do respectivo kit de fixação.	Datasheet, guia de instalação ou documentação técnica oficial do fabricante.	() Atendeu () Não atendeu
5.8	O appliance deverá possuir alimentação elétrica Full Range, compatível com 100~240 VCA, 50/60 Hz, ou tecnologia equivalente.	Datasheet, guia de instalação ou documentação técnica oficial do fabricante.	() Atendeu () Não atendeu



6. FUNCIONALIDADES DE FIREWALL E CONTROLE DE REDE

Item	Requisito técnico mínimo	Forma de comprovação	Resultado
6.1	Criação e administração de políticas de firewall baseadas em endereços, redes, zonas, serviços, aplicações, usuários, grupos, horários e outros atributos suportados.		() Atendeu () Não atendeu
6.2	Suporte a objetos de rede, grupos de objetos, serviços e agrupamentos para padronização das regras.		() Atendeu () Não atendeu
6.3	Suporte a tradução de endereços e portas, incluindo NAT e PAT, conforme a arquitetura implantada.		() Atendeu () Não atendeu
6.4	Suporte a roteamento estático, roteamento dinâmico corporativo e roteamento baseado em políticas ou tecnologia equivalente.		() Atendeu () Não atendeu
6.5	A solução deverá possuir suporte aos protocolos IPv4 e IPv6, ficando a utilização e a configuração de cada protocolo condicionadas às necessidades e à arquitetura de rede efetivamente implantada na Contratante.		() Atendeu () Não atendeu
6.6	Disponibilização de recursos de proteção contra falsificação de endereços (Anti-Spoofing), varreduras de rede, anomalias de tráfego e ataques de negação de serviço (DoS), por meio de funcionalidades nativas ou integradas e homologadas pelo fabricante, com os licenciamentos necessários incluídos na solução contratada.		() Atendeu () Não atendeu
6.7	Recursos de QoS e priorização de tráfego por usuário, grupo, aplicação, endereço, serviço, protocolo ou critérios equivalentes.		() Atendeu () Não atendeu
6.8	Disponibilização de suporte a DNS Dinâmico (DDNS), permitindo a atualização automática de registros DNS associados a interfaces ou serviços com endereçamento IP variável, quando aplicável à arquitetura de conectividade implantada, conforme previsto no item 1.19 deste Termo de Referência.		() Atendeu () Não atendeu



7. CONTROLE DE APLICAÇÕES E ANÁLISE COMPORTAMENTAL

Item	Requisito técnico mínimo	Forma de comprovação	Resultado
7.1	Identificação e controle de aplicações independentemente da porta ou protocolo utilizado.		() Atendeu () Não atendeu
7.2	Classificação de aplicações por categoria, risco, comportamento ou perfil de utilização.		() Atendeu () Não atendeu
7.3	Aplicação de políticas diferenciadas por aplicação, usuário, grupo, rede, horário ou perfil.		() Atendeu () Não atendeu
7.4	Identificação de redes sociais, aplicativos de comunicação, VPNs, proxies, acesso remoto, streaming e demais serviços de camada 7.		() Atendeu () Não atendeu
7.5	Disponibilização de mecanismos de análise comportamental e correlação automatizada de eventos para identificação de ameaças, utilizando, quando aplicável à arquitetura ofertada, inteligência artificial (IA), Machine Learning (ML) ou tecnologias funcionalmente equivalentes, com os recursos necessários devidamente licenciados e disponíveis durante toda a vigência contratual.		() Atendeu () Não atendeu

8. PREVENÇÃO DE INTRUSÃO, ANTIMALWARE E INTELIGÊNCIA DE AMEAÇAS

Item	Requisito técnico mínimo	Forma de comprovação	Resultado
8.1	Sistema de Prevenção de Intrusão (IPS) integrado ou homologado, com capacidade de identificar, bloquear e mitigar tentativas de exploração e tráfego malicioso.		() Atendeu () Não atendeu
8.2	Proteção contra malwares, ransomwares, trojans, worms, botnets, arquivos maliciosos e comunicações suspeitas.		() Atendeu () Não atendeu
8.3	Atualização contínua das assinaturas, regras de detecção e mecanismos de proteção durante a vigência contratual.		() Atendeu () Não atendeu
8.4	Disponibilização e utilização de mecanismos de inteligência de ameaças (Threat Intelligence) ou tecnologia funcionalmente equivalente, com atualização contínua de indicadores de comprometimento (IoCs) e recursos de reputação de IPs, domínios, URLs e arquivos.		() Atendeu () Não atendeu



Item	Requisito técnico mínimo	Forma de comprovação	Resultado
8.5	Capacidade de registrar eventos contendo, quando disponível, ameaça, assinatura, ação aplicada, origem, destino, aplicação, usuário e horário.		() Atendeu () Não atendeu

9. FILTRAGEM DE CONTEÚDO E CONTROLE WEB

Item	Requisito técnico mínimo	Forma de comprovação	Resultado
9.1	Filtro Web corporativo com categorização dinâmica de conteúdo e atualização contínua das categorias.		() Atendeu () Não atendeu
9.2	Criação de listas de permissão e bloqueio de URLs, domínios ou categorias.		() Atendeu () Não atendeu
9.3	Políticas diferenciadas por rede, usuário, grupo, horário ou outros atributos suportados.		() Atendeu () Não atendeu
9.4	Geração de relatórios de navegação e eventos de bloqueio ou liberação.		() Atendeu () Não atendeu
9.5	Disponibilização de recursos que permitam o diagnóstico de bloqueios ou liberações de URLs, conforme as políticas de filtragem de conteúdo aplicadas, admitidos mecanismos equivalentes disponibilizados pela solução ofertada.		() Atendeu () Não atendeu

10. INSPEÇÃO DE TRÁFEGO CRIPTOGRAFADO E CERTIFICADOS

Item	Requisito técnico mínimo	Forma de comprovação	Resultado
10.1	Disponibilização de capacidade de inspeção de tráfego criptografado SSL/TLS, com os recursos e licenciamentos necessários incluídos na solução contratada, observadas, para sua utilização, as condições técnicas, as políticas institucionais de segurança e a legislação aplicável.	Datasheet ou manual.	() Atendeu () Não atendeu
10.2	Criação, importação, administração e revogação de certificados utilizados pela plataforma, por interface gráfica ou mecanismo equivalente.	Manual de certificados.	() Atendeu () Não atendeu
10.3	Possibilidade de definição de exceções e políticas de inspeção conforme usuários, redes, aplicações, categorias ou destinos.	Documentação oficial.	() Atendeu () Não atendeu



Item	Requisito técnico mínimo	Forma de comprovação	Resultado
10.4	Registro dos eventos associados à inspeção criptografada, respeitadas as políticas institucionais e a legislação aplicável.	Manual de logs e auditoria.	() Atendeu () Não atendeu

11. VPN E ACESSO REMOTO SEGURO

Item	Requisito técnico mínimo	Forma de comprovação	Resultado
11.1	Suporte a VPN Site-to-Site e Client-to-Site.		() Atendeu () Não atendeu
11.2	Suporte a IPsec, SSL VPN, VPN baseada em TLS/SSL ou tecnologia equivalente disponibilizada pelo fabricante.		() Atendeu () Não atendeu
11.3	A solução deverá possuir capacidade de integração com bases corporativas de autenticação, por meio de Active Directory, LDAP, RADIUS ou tecnologias funcionalmente equivalentes, ficando a utilização e a configuração dessa integração condicionadas às necessidades institucionais e à arquitetura de rede efetivamente implantada, observadas as funcionalidades e os licenciamentos integrantes da solução contratada.		() Atendeu () Não atendeu
11.4	A solução deverá disponibilizar recursos de geração e consulta de logs das conexões VPN, abrangendo, conforme a modalidade de VPN utilizada, eventos de conexão, autenticação e desconexão, identificação da origem e do usuário ou da identidade associada à conexão, bem como registros de início e encerramento das sessões, de modo a assegurar a rastreabilidade dos acessos e apoiar as atividades de auditoria e segurança da informação.		() Atendeu () Não atendeu
11.5	Possibilidade de aplicação de políticas de segurança ao tráfego dos usuários remotos.		() Atendeu () Não atendeu
11.6	Suporte à integração com a interligação corporativa entre a sede e o prédio anexo da Câmara Municipal, permitindo aplicação de políticas de segurança e, quando tecnicamente aplicável à arquitetura adotada, utilização de VPN ou mecanismo equivalente de proteção da comunicação.		() Atendeu () Não atendeu



12. GERENCIAMENTO INTELIGENTE DE LINKS (SD-WAN)

Item	Requisito técnico mínimo	Forma de comprovação	Resultado
12.1	Gerenciamento simultâneo de múltiplos links de internet.		() Atendeu () Não atendeu
12.2	Balanceamento de carga, failover automático e priorização de tráfego.		() Atendeu () Não atendeu
12.3	Monitoramento de qualidade dos links com base em latência, perda de pacotes, disponibilidade e desempenho.		() Atendeu () Não atendeu
12.4	Seleção dinâmica do melhor link conforme critérios técnicos e políticas definidas.		() Atendeu () Não atendeu
12.5	Geração de registros e alertas sobre alteração de estado, degradação ou indisponibilidade dos links.		() Atendeu () Não atendeu

13. GERENCIAMENTO CENTRALIZADO

Item	Requisito técnico mínimo	Forma de comprovação	Resultado
13.1	Gerenciamento centralizado em nuvem, local, híbrido ou solução equivalente, com administração centralizada do appliance e dos recursos integrantes da solução.		() Atendeu () Não atendeu
13.2	Gerenciamento centralizado de regras, políticas, objetos, VPNs, perfis de inspeção, relatórios e configurações relevantes.		() Atendeu () Não atendeu
13.3	Controle de acesso administrativo por perfis, funções ou níveis de privilégio.		() Atendeu () Não atendeu
13.4	A solução deverá disponibilizar recursos de registro e histórico das alterações administrativas realizadas nas configurações do appliance NGFW e de sua plataforma de gerenciamento, permitindo a rastreabilidade das ações executadas, com identificação do usuário ou identidade administrativa responsável, data e horário da ocorrência, ação realizada e, quando tecnicamente disponível, origem do acesso administrativo, de modo a possibilitar atividades de auditoria, fiscalização e segurança da informação.		() Atendeu () Não atendeu



Item	Requisito técnico mínimo	Forma de comprovação	Resultado
13.5	Acesso seguro por HTTPS ou mecanismo equivalente, admitida autenticação multifator quando disponibilizada pela solução de forma complementar.		() Atendeu () Não atendeu
13.6	Possibilidade de exportação ou integração de logs e eventos com plataformas externas de monitoramento, SIEM ou tecnologia equivalente.		() Atendeu () Não atendeu

14. BACKUP, VERSIONAMENTO E RESTAURAÇÃO

Item	Requisito técnico mínimo	Forma de comprovação	Resultado
14.1	Disponibilização de recurso de backup periódico e automatizado das configurações do appliance, configurável para periodicidade mínima diária.		() Atendeu () Não atendeu
14.2	Retenção mínima de 5 (cinco) versões válidas das configurações.		() Atendeu () Não atendeu
14.3	Possibilidade de restauração das configurações e recuperação do ambiente em caso de contingência.		() Atendeu () Não atendeu
14.4	Histórico das versões de configuração e identificação das datas de geração.		() Atendeu () Não atendeu
14.5	Disponibilização de mecanismo de rollback ou restauração de versão anterior das configurações, em conformidade com os recursos de backup, versionamento e restauração exigidos neste Termo de Referência.		() Atendeu () Não atendeu

**15. MONITORAMENTO, ALERTAS E SAÚDE OPERACIONAL**

Item	Requisito técnico mínimo	Forma de comprovação	Resultado
15.1	Visualização do estado operacional do appliance, interfaces, links e serviços licenciados.		() Atendeu () Não atendeu
15.2	Monitoramento de CPU, memória, armazenamento, throughput, sessões, VPNs, qualidade dos links e demais indicadores relevantes.		() Atendeu () Não atendeu
15.3	Geração de alertas por painel web, e-mail, aplicativo móvel, integração externa ou mecanismo equivalente.		() Atendeu () Não atendeu
15.4	Alertas para indisponibilidade, degradação de links, perda de pacotes, latência elevada, falhas operacionais e eventos críticos de segurança.		() Atendeu () Não atendeu
15.5	Painéis, gráficos e relatórios com informações em tempo real e históricas.		() Atendeu () Não atendeu
15.6	Funcionalidade complementar de visualização geográfica de eventos de segurança, quando disponibilizada pela plataforma ofertada, não constituindo requisito mínimo obrigatório para fins de avaliação da conformidade técnica da proposta.		() Atendeu () Não atendeu



16. ANÁLISE DE RISCO E POSTURA DE SEGURANÇA

Item	Requisito técnico mínimo	Forma de comprovação	Resultado
16.1	Recurso de avaliação contínua da postura de segurança (Security Posture Assessment) ou tecnologia funcionalmente equivalente, devidamente disponibilizado e licenciado durante toda a vigência contratual.		() Atendeu () Não atendeu
16.2	Análise de risco das configurações e recomendações de boas práticas.		() Atendeu () Não atendeu
16.3	Avaliação de regras de firewall, NAT, VPN, usuários administrativos, senhas, objetos, políticas, links e componentes críticos.		() Atendeu () Não atendeu
16.4	Disponibilização de histórico de eventos, análises e recomendações relacionadas à postura de segurança da solução.		() Atendeu () Não atendeu
16.5	Mecanismo automatizado de verificação da configuração e da saúde operacional (Health Check ou tecnologia funcionalmente equivalente), com execução ou atualização contínua ou, no mínimo, diária.		() Atendeu () Não atendeu

17. LOGS, RELATÓRIOS, AUDITORIA E LGPD

Item	Requisito técnico mínimo	Forma de comprovação	Resultado
17.1	Geração, consulta e exportação de logs de segurança, administração, autenticação, VPN, aplicações, navegação e eventos operacionais, conforme funcionalidades licenciadas.		() Atendeu () Não atendeu
17.2	Exportação em formatos auditáveis, como CSV, PDF ou formatos equivalentes.		() Atendeu () Não atendeu
17.3	Identificação de usuários, horários, origem dos acessos, ações executadas e eventos correlacionados, quando tecnicamente aplicável.		() Atendeu () Não atendeu
17.4	Possibilidade de guarda centralizada de logs pelo período definido na política institucional da Câmara Municipal de Divinópolis, observada, quando aplicável, a legislação vigente.		() Atendeu () Não atendeu



Item	Requisito técnico mínimo	Forma de comprovação	Resultado
17.5	Relatórios gerenciais e técnicos sobre ameaças, aplicações, usuários, links, VPNs, utilização, disponibilidade e saúde operacional.		() Atendeu () Não atendeu
17.6	Recursos de rastreabilidade e responsabilização compatíveis com as exigências de auditoria e com a Lei Geral de Proteção de Dados.		() Atendeu () Não atendeu

18. DOCUMENTAÇÃO E APOIO À IMPLANTAÇÃO

Item	Requisito técnico mínimo	Forma de comprovação	Resultado
18.1	Disponibilização de datasheets, manuais, guias de instalação, administração, arquitetura, release notes e documentação oficial pertinente.		() Atendeu () Não atendeu
18.2	Acesso aos portais oficiais do fabricante, quando aplicável, para obtenção de firmwares, documentação e abertura de chamados.		() Atendeu () Não atendeu
18.3	Disponibilização de imagens oficiais de firmware, arquivos de licenciamento e informações técnicas necessárias à implantação.		() Atendeu () Não atendeu
18.4	Documentação em português do Brasil ou, quando inexistente, em inglês acompanhada de esclarecimentos suficientes para avaliação e utilização.		() Atendeu () Não atendeu

Assinantes

**Samuel Carlos Da Silva Marques**

Assinou em 20/10/2026 às 17:56:46 com o certificado avançado da Betha Sistemas e possui a identidade verificada com o CPF ***.009.066-**.

Eu, Samuel Carlos Da Silva Marques, 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.

**Flavio Ramos De Assis Pereira**

Assinou em 21/10/2026 às 14:32:21 com o certificado avançado da Betha Sistemas e possui a identidade verificada com o CPF ***.876.376-**.

Eu, Flavio Ramos De Assis Pereira, 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.

**Presidente da Camara Municipal de Divinópolis**

Assinou em 21/10/2026 às 15:40:56 com Certificado Digital Qualificado, emitido em nome de ISRAEL MENDONCA com o CPF ***.119.356-**, nos termos do § 1º do art. 10 da Medida Provisória nº 2.200-2, de 24 de agosto de 2001.

Eu, Presidente da Camara Municipal de Divinópolis, 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.betha.cloud** e insira o código abaixo:

XRV-ZEX-R1Z-6V2



ANEXO III

INSTRUMENTO DE MEDIÇÃO DE RESULTADOS – IMR

1. DO OBJETO DA CONTRATAÇÃO

- 1.1. Contratação de solução integrada de segurança de rede do tipo Firewall de Próxima Geração (NGFW/UTM), em regime de locação, incluindo appliances, licenciamento, suporte técnico especializado, atualização tecnológica e garantia de continuidade operacional.

2. DEFINIÇÃO

- 2.1. Este Instrumento de Medição de Resultados (IMR) estabelece critérios objetivos para aferição da qualidade dos serviços prestados, por meio de indicadores de desempenho vinculados aos níveis mínimos esperados de disponibilidade, atendimento, resolução de incidentes, atualização tecnológica e gestão contratual.
- 2.2. A medição será realizada mensalmente pelo Fiscal do Contrato e servirá de base para o cálculo do Índice Global de Desempenho (IGD), sem prejuízo das sanções previstas no contrato.
- 2.3. As situações abrangidas pelo presente instrumento se referem a fatos cotidianos da execução do contrato, não isentando a Contratada das demais responsabilidades ou sanções legalmente previstas.
- 2.4. A Contratante poderá alterar os procedimentos metodológicos de medição durante a execução contratual sempre que o novo sistema se mostrar mais eficiente que o anterior e não houver prejuízos para a Contratada.
- 2.5. Este anexo é parte indissociável do contrato e de seus demais anexos.

3. DA METODOLOGIA DE MEDIÇÃO DOS RESULTADOS

- 3.1. A avaliação será realizada por meio de indicadores de desempenho previamente definidos, aos quais serão atribuídas pontuações específicas, totalizando o máximo de 100 (cem) pontos por período de medição.
- 3.2. A medição será efetuada pelo Fiscal Técnico do Contrato, com apoio do Fiscal Administrativo, utilizando como base, dentre outros elementos:
 - I – relatórios extraídos da própria solução de firewall;
 - II – registros de indisponibilidade da infraestrutura;
 - III – registros de chamados técnicos;
 - IV – relatórios de atendimento emitidos pela CONTRATADA;



V – relatórios de monitoramento;

VI – registros de atualização de firmware, assinaturas de segurança e demais componentes da solução;

VII – registros produzidos pela fiscalização contratual.

- 3.3.** Os elementos estabelecidos no tópico anterior possuem natureza exemplificativa e não exaustiva, podendo a Contratada se utilizar de outros instrumentos aptos a conferir maior segurança à medição da prestação dos serviços.
- 3.4.** Os resultados obtidos em cada indicador serão convertidos em pontuação, conforme critérios definidos neste instrumento, cuja soma constituirá o Índice Global de Desempenho – IGD referente ao período avaliado.
- 3.5.** O período de medição corresponderá, em regra, a um mês de execução contratual, iniciando-se no primeiro dia e encerrando-se no último dia de cada competência.
- 3.5.1.** Durante os primeiros 30 (trinta) dias contados do recebimento definitivo da solução implantada, os indicadores de desempenho serão normalmente monitorados pela fiscalização, porém eventual descumprimento das metas estabelecidas não ensejará aplicação de glosas financeiras, desde que decorrente de atividades de estabilização, ajustes finos de configuração, otimização das políticas de segurança ou correção de inconsistências identificadas durante a fase inicial de operação, sem prejuízo da obrigação da Contratada de promover a imediata correção das falhas verificadas.
- 3.6.** Sempre que houver descumprimento dos níveis mínimos estabelecidos no acordo de nível de serviços (SLA), a fiscalização registrará a ocorrência, assegurando à Contratada o direito de apresentar justificativa técnica no prazo estabelecido contratualmente.
- 3.6.1.** As justificativas apresentadas pela Contratada serão analisadas pela fiscalização, podendo ser acolhidas quando demonstrado que a ocorrência decorreu exclusivamente de caso fortuito, de força maior, ou de fato alheio ao controle da Contratada.
- 3.6.2.** As ocorrências cujas justificativas forem aceitas não serão consideradas para fins de cálculo do Índice Global de Desempenho.
- 3.7.** Caso seja constatado comportamento reiterado de desempenho insatisfatório, ainda que os descontos financeiros decorrentes do IMR tenham sido aplicados, poderão ser adotadas as demais medidas administrativas previstas no Contrato



4. DOS INDICADORES, DAS METAS E DOS MECANISMOS DE CÁLCULO

- 4.1.** Os indicadores possuem natureza objetiva, mensurável e verificável, sendo destinados à avaliação da disponibilidade da solução, da eficiência dos serviços de suporte, da continuidade operacional, da atualização tecnológica e do cumprimento das obrigações técnicas assumidas pela Contratada.
- 4.2.** Os indicadores serão avaliados mensalmente e receberão pontuação individual, conforme critérios definidos na tabela abaixo, totalizando, no máximo, **100 (cem) pontos** por período de medição.

Indicador	Objetivo	Responsável	Peso
I – Disponibilidade da solução NGFW	Garantir a continuidade operacional da infraestrutura de segurança	Fiscal Técnico	35 pontos
II – Resposta aos chamados técnicos	Assegurar resposta tempestiva às solicitações	Fiscal Técnico	20 pontos
III – Resolução dos chamados técnicos	Garantir solução tempestiva das ocorrências	Fiscal Técnico	25 pontos
IV – Atualização tecnológica e continuidade operacional	Manter a solução permanentemente atualizada	Fiscal Técnico	10 pontos
V – Gestão contratual e qualidade da prestação dos serviços	Avaliar a qualidade técnica e administrativa da execução	Fiscal Técnico/ Fiscal Administrativo	10 pontos

- 4.3.** Os critérios de análise de cada indicador serão aqueles abaixo apresentados:

4.3.1. INDICADOR I: Disponibilidade da solução NGFW

Disponibilidade	Pontuação
≥ 99,00%	35
94,00% a 98,99%	30
90,00% a 93,99%	20
abaixo de 90,00%	10

- 4.3.1.1.** A medição da disponibilidade do sistema será aferida através de relatório da própria solução de firewall e/ou registros de ocorrências de indisponibilidade verificadas pela Contratante.
- 4.3.1.2.** Não serão computadas indisponibilidades decorrentes de manutenção programada autorizada pela Contratante, caso fortuito, força maior ou falhas de infraestrutura da Contratante.

**4.3.2. INDICADOR II: Atendimento aos chamados técnicos**

Atendimentos dentro do prazo do SLA	Pontuação
100%	20
80 - 99%	18
60 - 79%	15
Abaixo de 60%	5

4.3.2.1. Os prazos para atendimento será aqueles presentes no SLA descrito no tópico 4.4

4.3.3. INDICADOR III: Resolução dos chamados técnicos

Restabelecimento do sistema dentro prazo do SLA	Pontuação
100%	25
80 - 99%	20
60 - 79%	15
Abaixo de 60%	5

4.3.3.1. Os prazos para atendimento será aqueles presentes no SLA descrito no tópico 4.4

4.3.4. INDICADOR IV: Atualização tecnológica e continuidade operacional

4.3.4.1. Para a análise deste indicador será avaliada a proatividade da empresa na manutenção da atualização tecnológica do sistema implantado, especialmente nos pontos que se seguem:

- a) Assinaturas de IPS, Antivírus, Anti-Malware, Web Filter, Application Control e demais serviços de inteligência de ameaças mantidas permanentemente atualizadas, conforme disponibilização do fabricante.
- b) Atualizações críticas de segurança (patches) aplicadas.
- c) Atualizações de firmware ou sistema operacional do firewall realizadas conforme recomendação do fabricante, observadas análise de risco, testes e autorização da fiscalização.
- d) Ausência de incidentes decorrentes de falha na gestão de atualizações, como permanência injustificada em versões vulneráveis ou perda de funcionalidades por negligência da contratada.

4.3.4.2. A cada ocorrência de negligência no que se refere à manutenção dos requisitos de atualização do sistema será descontado 1 ponto da pontuação atribuída a este indicador.

Nível de atualização da solução	Pontuação
100%	10
<100%	- 1 ponto (por ocorrência)



4.3.4.3. As falhas de atualização verificadas pela equipe Técnica de fiscalização serão formalmente notificadas à Contratada.

4.3.5. INDICADOR V: Gestão contratual e qualidade da prestação dos serviços

4.3.5.1. Para a análise deste indicador será avaliada a eficiência da contratada na gestão operacional do contrato, considerando a qualidade da prestação dos serviços, o atendimento às solicitações da Contratante, a organização documental, a prevenção de reincidências e a observância das obrigações contratuais, especialmente os pontos que se seguem:

- a) Atendimento às solicitações da Contratante com qualidade técnica, tempestividade, clareza das informações prestadas e postura profissional da equipe técnica.
- b) Ausência de reincidência de falhas decorrentes de serviços anteriormente executados ou de problemas cuja correção já tenha sido realizada pela contratada.
- c) Atendimento às determinações e solicitações da fiscalização contratual dentro dos prazos estabelecidos.
- d) Emissão e entrega tempestiva dos documentos técnicos, relatórios, registros de atendimento, pareceres e demais documentos previstos contratualmente.
- e) Manutenção das condições necessárias à adequada prestação dos serviços durante toda a execução contratual, incluindo disponibilidade da equipe técnica, observância dos procedimentos definidos, cumprimento das obrigações contratuais e comunicação tempestiva de ocorrências relevantes.

4.3.5.2. A cada ocorrência verificada no que se refere à qualidade da prestação dos serviços será descontado 1 ponto da pontuação atribuída a este indicador.

Nível de Qualidade na execução contratual	Pontuação
100%	10
<100%	- 1 ponto (por ocorrência)

4.3.5.3. As falhas ou ineficiências verificadas pela equipe de fiscalização serão notificadas à contratante buscado a adequação de conduta e melhorias na qualidade da prestação dos serviços.

4.4. Acordo de nível de serviço (SLA) para atendimento a chamados técnicos

Criticidade	Descrição	Tempo Máximo de Resposta	Tempo Máximo para Restabelecimento
Crítica	Indisponibilidade total da solução, falha do cluster HA, perda completa de conectividade institucional, indisponibilidade simultânea de links ou comprometimento grave de segurança	30 minutos	24 horas corridas



Alta	Degradação severa de desempenho, falha parcial de serviços essenciais, indisponibilidade de VPN corporativa, falha de um dos links redundantes ou comprometimento relevante de segurança	1 hora	16 horas úteis
Média	Falhas em regras específicas, NAT, relatórios, autenticação, políticas de acesso, funcionalidades secundárias ou degradação moderada sem interrupção total dos serviços	4 horas	24 horas úteis
Baixa	Solicitações administrativas, ajustes operacionais, dúvidas técnicas, alterações programadas, otimizações ou demandas sem impacto significativo na continuidade operacional	8 horas	48 horas úteis

5. ÍNDICE GLOBAL DE DESEMPENHO

- 5.1.** Mensalmente, será aferido o Índice Global de Desempenho (IGD) dos serviços prestados pela contratada, obtido a partir da soma das pontuações alcançadas em todos os indicadores previstos neste Instrumento de Medição de Resultados.
- 5.2.** O IGD representa o nível de atendimento das obrigações contratuais no período avaliado e servirá como referência para a avaliação da qualidade dos serviços prestados, para a aplicação de eventuais ajustes na remuneração mensal e para subsidiar as ações de gestão e fiscalização do contrato.
- 5.3.** A pontuação aferida será utilizada para a classificação do nível de serviços prestados, conforme tabela abaixo:

Pontuação	Classificação da execução contratual	Desconto a ser aplicado no valor contratual
95-100	Excelente	0%
90-94	Muito Bom	2%
80-89	Adequado	4%
70-79	Regular	8%
<70	Insatisfatório	10%, sem prejuízo de penalidades

6. DISPOSIÇÕES FINAIS

- 6.1.** A aplicação do presente Instrumento de Medição de Resultados não substitui nem afasta a aplicação das sanções administrativas previstas na Lei nº 14.133/2021, no Contrato e nos demais documentos que regem a contratação.
- 6.2.** O Fiscal emitirá relatório mensal contendo os indicadores apurados, justificativas apresentadas pela Contratada e o IGD do período. O descumprimento reiterado dos indicadores poderá ensejar aplicação das penalidades previstas no contrato.

**MODELO DE PROPOSTA COMERCIAL**

À
CÂMARA MUNICIPAL DE DIVINÓPOLIS (MG)

Conforme solicitado, a empresa _____, CNPJ, _____-_____, vem por meio deste apresentar proposta comercial para o fornecimento da solução abaixo especificada.

OBJETO CONTRATUAL: Contratação de solução integrada de segurança de rede do tipo Firewall de Próxima Geração (NGFW/UTM), em regime de locação com cessão de uso/comodato do appliance, incluindo o fornecimento do appliance, subscrição/licenciamento durante toda a vigência contratual, suporte técnico oficial da solução, atualização tecnológica, garantia de continuidade operacional e treinamento técnico para transferência de conhecimento à equipe de Tecnologia da Informação da Câmara Municipal, de acordo com as quantidades, especificações e condições descritas..

Item	Descrição	Qtd.	Unidade	Valor Unitário	Valor Total
01	<i>Fornecimento de solução integrada de segurança de rede do tipo Firewall de Próxima Geração (NGFW/UTM), em regime de locação com cessão de uso/comodato do appliance, incluindo os componentes tecnológicos necessários ao atendimento integral dos requisitos da contratação</i>	12	Mês	R\$ _____	R\$ _____
TOTAL MENSAL PROPOSTO					R\$ _____
TOTAL ANUAL PROPOSTO					R\$ _____



Tabela de composição do Item 01 - Solução Integrada de Firewall NGFW			
Componente	Descrição	Quant	Unid.
Appliance NGFW	Appliance dedicado de Firewall de Próxima Geração – NGFW, novo, em linha de produção atual, disponibilizado em regime de locação com cessão de uso/comodato. O equipamento deverá atender integralmente às especificações mínimas de hardware, capacidade, suficiente para suportar toda a demanda prevista da rede institucional, incluindo sistema operacional/firmware nativo ou homologado, kit de instalação em rack e demais componentes e acessórios necessários ao funcionamento da solução, conforme especificações do Anexo I.	1	Unidade
Licenciamento/ Subscrição de Segurança	Licenciamento, subscrição ou disponibilização integral de todos os recursos de segurança necessários ao appliance NGFW durante toda a vigência contratual, com capacidade técnica e de licenciamento para suportar no mínimo 500 dispositivos, abrangendo, quando aplicável à arquitetura ofertada, IPS, antivírus, antimalware, filtragem de conteúdo, controle de aplicações, inspeção de tráfego, análise comportamental, Inteligência Artificial – IA e/ou Machine Learning, inteligência de ameaças e demais funcionalidades de segurança, conforme especificações anexo I.	1	Conjunto
Conectividade segura/VPN	Licenciamento, habilitação ou disponibilização dos recursos necessários à conectividade segura via VPN IPsec, SSL VPN, VPN baseada em TLS/SSL ou tecnologia equivalente, abrangendo a solução durante toda a vigência contratual. Quando tais funcionalidades forem nativas ou já estiverem abrangidas pelo licenciamento principal da plataforma, não será exigido licenciamento específico adicional, desde que permaneçam integralmente disponíveis.	1	Conjunto
Plataforma de gerenciamento centralizado	Licenciamento, subscrição ou disponibilização da plataforma de gerenciamento centralizado do appliance NGFW, recurso tecnológico integrante da solução ofertada, disponibilizado em nuvem, ambiente local, híbrido ou tecnologia equivalente, válido durante toda a vigência contratual, permitindo o gerenciamento centralizado do appliance, visualização das informações operacionais, geração de alertas e relatórios, backup automático das configurações com retenção mínima de 5 (cinco) versões válidas, gerenciamento de políticas e acompanhamento dos indicadores de saúde operacional da solução.	1	Plataforma
Garantia, suporte oficial e atualização tecnológica	Disponibilização, durante toda a vigência contratual, da documentação técnica oficial, acesso aos recursos e portais oficiais aplicáveis, imagens e atualizações oficiais de firmware/software, licenças e subscrições, garantia, suporte técnico oficial da solução, atendimento aos níveis de serviço previstos neste documento e seus anexos, substituição de hardware quando necessária e mecanismos de atualização tecnológica/Hardware Refresh, inclusive nas hipóteses de descontinuidade, perda de suporte ou incapacidade de atendimento aos requisitos contratados.	1	Serviço



Tabela de composição do Item 01 - Solução Integrada de Firewall NGFW			
Treinamento e transferência de conhecimento	Treinamento técnico destinado à equipe de Tecnologia da Informação da Câmara Municipal, com carga horária mínima de 8 (oito) horas, abrangendo as funcionalidades efetivamente contratadas e observando os requisitos estabelecidos no anexo I deste documento.	1	Serviço

Nos preços indicados nesta proposta estão incluídos todos os custos, benefícios, encargos, tributos e demais contribuições pertinentes.

Outras observações do fornecedor:

A proposta tem validade para 60 dias.

Divinópolis de de 2026.

Assinatura

Nome:

CNPJ/CPF

Endereço:

Email:

Telefone:

Responsável pelo contato:



DECLARAÇÃO DE LIMITE DE FATURAMENTO ME/EPP

(PAPEL TIMBRADO DA LICITANTE)

(Nome da Empresa), CNPJ Nº _____, sediada na Rua _____, nº _____, bairro _____, CEP _____, município/UF _____, por seu representante legal abaixo assinado, DECLARA, para fins de participação em licitação ou contratação direta com a CÂMARA MUNICIPAL DE DIVINÓPOLIS / MG, sob as penas da lei que:

I – Que é ME, EPP ou MEI e não se encontra em nenhuma das situações do § 4º, art. 3º, da Lei Complementar nº 123/2006 e está apta para usufruir do tratamento estabelecido nos artigos 42 a 49 da Lei Complementar nº 123/2006.

II – Que, no ano-calendário de realização desta licitação, os valores somados dos contratos celebrados com a Administração Pública não extrapolam a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte, nos termos do art. 4º, § 2º da Lei nº 14.133/2021.

(LOCAL E DATA).

ASSINATURA DO REPRESENTANTE LEGAL

(Nome, identidade, carimbo e assinatura do representante legal da empresa)



ESTUDO TÉCNICO PRELIMINAR (ETP)

Objeto: Contratação de solução integrada de segurança de rede do tipo Firewall de Próxima Geração (NGFW/UTM), em regime de locação com cessão de uso/comodato do appliance, incluindo fornecimento do appliance, subscrição/licenciamento durante toda a vigência contratual, suporte técnico oficial da solução, atualização tecnológica e garantia de continuidade operacional.

1. DESCRIÇÃO DA NECESSIDADE E DO CENÁRIO ATUAL

A Câmara Municipal de Divinópolis utiliza atualmente servidores de propósito geral executando soluções baseadas em software livre para funções de firewall e segurança de borda. Embora essa arquitetura tenha atendido às necessidades iniciais da Administração, o cenário atual apresenta limitações decorrentes da utilização de hardware genérico, sem integração nativa entre hardware, sistema operacional, licenciamento e mecanismos avançados de segurança, além de restrições relacionadas à inspeção avançada de tráfego, atualização tecnológica, disponibilidade, gerenciamento centralizado e suporte técnico especializado. Diante desse cenário, torna-se necessária a modernização da infraestrutura de segurança perimetral por meio da adoção de solução baseada em appliances dedicados do tipo Next-Generation Firewall (NGFW). A necessidade de modernização fundamenta-se em:

- a) **Segurança Adaptativa:** Necessidade de enfrentar ameaças modernas (ransomwares, ataques avançados e vulnerabilidades ainda não catalogadas – Zero-Day), por meio de mecanismos avançados de detecção, correlação de eventos de segurança e análise comportamental automatizada.
- b) **Gestão de Continuidade:** Reduzir os riscos de interrupção dos serviços institucionais decorrentes de falhas de hardware, indisponibilidade de links ou demais ocorrências que afetem a infraestrutura de segurança, mediante mecanismos de contingência, gerenciamento dos enlaces de comunicação, suporte técnico especializado, níveis de serviço, garantia e substituição do equipamento quando necessária.
- c) **Eficiência de Gestão:** Centralizar o monitoramento e a administração da solução, por meio de painel em nuvem, local, híbrido ou solução equivalente, reduzindo a carga de trabalho manual da equipe técnica.

No cenário atual, a infraestrutura de firewall é composta por dois servidores HP ProLiant



ML110 G7, que operam com soluções baseadas em software livre, como pfSense, OPNsense ou distribuições Linux. Trata-se de equipamentos que, embora funcionais, apresentam limitações decorrentes de sua obsolescência tecnológica e do avanço das demandas de segurança da informação.

1.1. Limitações de Processamento e Instruções Modernas

O ML110 G7 utiliza processadores da família **Intel Xeon E3-1200 (v1)** ou Core i3 de 2ª geração.

a) AES-NI: Embora a maioria dos Xeon E3 dessa linha suporte AES-NI (aceleração de hardware para criptografia), alguns modelos de entrada (como os Pentium ou Celeron que às vezes vinham neles) não suportam. A ausência ou limitação de recursos modernos de aceleração criptográfica pode comprometer o desempenho de VPNs, inspeção de tráfego criptografado e demais mecanismos de segurança, impactando diretamente a performance da rede institucional.

b) Eficiência Energética: Os servidores legados utilizam arquitetura de geração anterior e apresentam menor eficiência energética quando comparados a equipamentos modernos desenvolvidos especificamente para funções de segurança de rede. Considerando que a infraestrutura de firewall opera de forma contínua, em regime 24x7, o consumo energético constitui fator relevante na avaliação do custo operacional e do ciclo de vida da solução. A adoção de appliances dedicados permite, ainda, reduzir a utilização de componentes de propósito geral e buscar maior eficiência entre capacidade de processamento e consumo de energia.

1.2. Barramentos e Redes (I/O)

a) PCIe 2.0: O servidor utiliza barramentos PCI Express 2.0. Para firewalls de 1Gbps, isso é suficiente. No entanto, conforme necessidade de expansão para **10Gbps**, o barramento e a arquitetura interna se tornam um gargalo de latência e throughput, sendo a limitação da plataforma um ponto importante a ser considerado diante da demanda atual.

b) Placas de Rede Integradas: Ele vem com duas portas Intel 82574L. São excelentes placas (com suporte nativo estável em BSD/Linux), mas duas portas costumam ser o limite mínimo (WAN e LAN). Para criar uma DMZ ou implementar redundância física de enlaces, torna-se necessário o uso de placas de expansão, e atualmente isso é uma limitação para esta Casa Legislativa.



1.3. Confiabilidade e Manutenção (Hardware Legacy)

- a) Degradação de Componentes:** Atualmente, os capacitores da placa-mãe e as fontes de alimentação (PSU) desses servidores já ultrapassaram em muito sua vida útil estimada. O risco de falha de hardware é elevado e representa atualmente o principal fator de risco da infraestrutura.
- b) Peças de Reposição:** Encontrar fontes ou placas-mãe específicas para o ML110 G7 torna-se cada vez mais difícil e caro, muitas vezes dependendo de peças usadas de procedência nem sempre rastreável, sem mencionar a dificuldade de encontrar fornecedores confiáveis para suprir essas necessidades, uma vez que não é mais fabricado há anos.
- c) iLO 3:** O gerenciamento remoto disponível nos equipamentos atuais encontra-se tecnologicamente defasado, podendo exigir versões antigas de navegadores, plugins ou componentes de software, o que aumenta riscos de segurança, reduz a usabilidade e dificulta a manutenção remota.

1.4. Memória RAM (8GB)

- a) Capacidade:** 8GB é mais que suficiente para um firewall básico. No entanto, quando habilitados recursos avançados de Next-Generation Firewall (NGFW), como:
- IDS/IPS (Suricata ou Snort) com grande volume de regras;
 - Proxy e filtragem de conteúdo (Squid, Zenarmor ou equivalentes);

A capacidade de memória pode se tornar insuficiente rapidamente, especialmente diante de elevado número de conexões simultâneas e tabelas de estado extensas.

Além dos aspectos anteriormente mencionados, a solução atualmente utilizada ainda apresenta restrições de hardware em relação ao uso exclusivo de RAID por software, o que compromete a confiabilidade e a capacidade de processamento diante do aumento do tráfego de dados. Esse cenário é agravado pela crescente utilização de sistemas baseados em web e serviços em nuvem nesta Casa Legislativa.

A tabela a seguir apresenta um resumo do cenário atual da solução de segurança atualmente implementada.



RESUMO DE VIABILIDADE		
Componente	Status em 2026	Impacto
CPU	Ultrapassada	Alto consumo e falta de instruções AVX modernas.
RAM (8GB)	Adequada	Suficiente para roteamento, apertada para IDS/IPS pesado.
Rede	Limitada	Apenas 1Gbps; expansão limitada pelo PCIe 2.0.
Energia	Menor eficiência energética	Maior consumo relativo em comparação a arquiteturas modernas dedicadas, devendo o aspecto energético ser considerado no ciclo de vida da solução.
Ruído	Alto	Inviável para ambientes de escritório sem rack isolado.

Do ponto de vista de segurança, a solução atual não contempla, de forma integrada, mecanismos avançados de proteção, como prevenção de intrusões (IPS), inspeção de tráfego criptografado, controle de aplicações e análise automatizada de ameaças. Essa limitação reduz a capacidade de resposta a incidentes e amplia a exposição a riscos cibernéticos.

Além disso, a gestão da solução atual depende fortemente de configurações manuais e conhecimento técnico especializado, dificultando a padronização, o monitoramento contínuo e a geração de relatórios gerenciais, além da elevada dependência de intervenção humana para várias situações que atualmente são resolvidas via softwares especializados para a função de monitoramento e prevenção.

Considerando também a necessidade de promover a continuidade dos serviços, a escalabilidade do ambiente tecnológico e maior eficiência operacional, torna-se necessária a implementação de solução de segurança de rede do tipo NGFW, com capacidade adequada ao atendimento integral da demanda institucional, gerenciamento centralizado, mecanismos de monitoramento e contingência, suporte técnico especializado, garantia de substituição do equipamento e recursos avançados de segurança.

Conforme será apresentado ao longo deste ETP, a contratação de solução de segurança de rede do tipo NGFW, em regime de locação com cessão de uso/comodato, incluindo a subscrição/licenciamento durante toda a vigência contratual, suporte técnico oficial da solução e garantia de atualização tecnológica é uma estratégia necessária para a modernização da infraestrutura de segurança perimetral da Câmara Municipal de Divinópolis.



2. PREVISÃO NO PLANO DE CONTRATAÇÕES ANUAL

A presente contratação encontra-se prevista no Plano Anual de Contratações de 2026, da Câmara Municipal de Divinópolis, disponível no Portal Nacional de Contratações Públicas (PNCP) através do endereço eletrônico <https://pncp.gov.br/app/pca/23774227000190/2026>, conforme detalhamento a seguir:

Número do item no PCA: 16

Classificação: 70 – Informática – Equipamentos, peças, acessórios e suprimentos de TIC

Documentos de Formalização de Demanda de Origem: DFD nº 005/2026 da Diretoria de Informática e Tecnologia da Informação, assinados com o certificado avançado da Betha Sistemas

Adequação da solução proposta: Em relação à solução inicialmente prevista no DFD original supracitado, registra-se que, em decorrência de aprofundamentos dos estudos técnicos realizados no âmbito deste ETP, verificou-se a necessidade de adequação da solução inicialmente delineada, uma vez que esta não contemplava integralmente os requisitos técnicos e operacionais necessários à integral segurança da rede institucional. Dessa forma, procedeu-se à adequação da solução proposta, com vistas a assegurar maior aderência às necessidades do Órgão, preservando-se, contudo, a natureza e a finalidade originalmente pretendidas, sem que a alteração represente desvio de objeto.

Ressalta-se que a fase de planejamento da contratação, especialmente por meio do Estudo Técnico Preliminar, constitui instrumento destinado à análise e à definição da solução mais adequada à necessidade da Administração, nos termos da Lei nº 14.133/2021, permitindo o aprimoramento das informações inicialmente levantadas no DFD, com vistas à seleção da alternativa mais vantajosa, eficiente e aderente ao interesse público.

3. ÁREA REQUISITANTE

A presente demanda está sendo solicitada pela Diretoria de Informática e Tecnologia da Informação da Câmara Municipal de Divinópolis, atualmente sob responsabilidade do Senhor Alexsandro Alves Vasconcelos, Analista Legislativo Tecnologia da Informação.

4. LEVANTAMENTO DE MERCADO

O mercado atual de segurança é caracterizado pela evolução do firewall tradicional para plataformas integradas de segurança cibernética, capazes de reunir mecanismos de inspeção avançada de tráfego, prevenção de intrusões, controle de aplicações, gerenciamento centralizado, inteligência de ameaças, análise comportamental e recursos automatizados de detecção e resposta.



A análise de mercado para o presente ETP identificou diferentes alternativas tecnológicas capazes de atender, em maior ou menor grau, às necessidades de segurança de borda da Câmara Municipal de Divinópolis, incluindo soluções baseadas em servidores de propósito geral com software livre, appliances físicos dedicados e plataformas corporativas de Firewall de Próxima Geração – NGFW.

O cenário tecnológico atual apresenta diferentes modelos de fornecimento e arquitetura, os quais variam conforme o nível de maturidade tecnológica, forma de disponibilização da solução, complexidade de integração, modelo de suporte, responsabilidade sobre os equipamentos e estratégia de atualização adotada.

Para fins deste estudo técnico, as soluções identificadas podem ser agrupadas, de forma geral, nos seguintes modelos:

- a) **Solução baseada em servidores físicos com software livre:** composta por servidores corporativos adquiridos pela Administração, sobre os quais são instaladas plataformas como OPNsense, pfSense, distribuições Linux ou tecnologias equivalentes, sendo necessária a implantação, configuração, integração, atualização e sustentação do ambiente por equipe própria ou empresa especializada;
- b) **Solução baseada em appliances físicos dedicados:** composta por equipamentos desenvolvidos especificamente para funções de segurança de rede, integrando hardware, sistema operacional e recursos de segurança, podendo operar de forma isolada ou em Alta Disponibilidade;
- c) **Solução baseada em virtualização:** implementada em ambiente virtualizado, utilizando infraestrutura própria da Administração ou ambientes em nuvem, sem necessidade de hardware dedicado específico para a função de firewall;
- d) **Solução corporativa NGFW disponibilizada como solução integrada:** fornecida de forma contínua, podendo contemplar appliances dedicados em regime de locação com cessão de uso/comodato, licenciamento/subscrição, suporte técnico, gerenciamento tecnológico da plataforma e atualização permanente dos mecanismos de segurança.

4.1. Panorama dos Fabricantes e Soluções Disponíveis

O levantamento de mercado identificou fabricantes, desenvolvedores nacionais, integradores tecnológicos, representantes autorizados, parceiros comerciais oficialmente habilitados, distribuidores autorizados e fornecedores de soluções próprias ou homologadas, aptos ao fornecimento de soluções de segurança de rede.



Também foram identificadas empresas especializadas na implantação e sustentação de soluções baseadas em software livre executadas sobre servidores corporativos.

No segmento de plataformas NGFW, foram identificadas soluções capazes de disponibilizar, de forma integrada, recursos de: Inspeção profunda de pacotes; Prevenção de intrusão; Gerenciamento centralizado; Conectividade segura via VPN; Controle de aplicações; Alta Disponibilidade, quando adotada arquitetura com mais de um equipamento; Balanceamento inteligente de links; Integração com ambientes em nuvem; Integração com ambientes de redes sem fio corporativas; Inteligência de ameaças; Monitoramento e acompanhamento da saúde operacional da solução; Mecanismos de análise comportamental, Inteligência Artificial – IA e/ou Machine Learning, conforme a tecnologia ofertada; e Suporte técnico oficial da solução.

As soluções disponíveis no mercado apresentam diferentes níveis de integração e maturidade tecnológica, sendo necessário avaliar não apenas a possibilidade de execução das funções básicas de firewall, mas a aderência do conjunto da solução aos requisitos de segurança, disponibilidade, gerenciamento, atualização tecnológica e continuidade operacional definidos pela Administração.

O ETP atualmente exige, entre outros elementos, gerenciamento centralizado, monitoramento, backup automático das configurações, alertas, SD-WAN e acompanhamento da saúde operacional, além de recursos de avaliação da postura de segurança e inteligência de ameaças.

4.2. Tendências e Tecnologias Relevantes e Aplicáveis

As soluções modernas de segurança de rede ultrapassam o conceito tradicional de simples bloqueio de portas e endereços, incorporando mecanismos capazes de analisar o contexto, o comportamento e o conteúdo das comunicações.

4.2.1. Análise Comportamental e Correlação Automatizada

As soluções modernas de segurança de rede incorporam mecanismos avançados de análise comportamental, correlação de eventos, inteligência artificial – IA e/ou Machine Learning, possibilitando maior capacidade de identificação de comportamentos suspeitos, tentativas de exploração de vulnerabilidades e atividades compatíveis com ataques cibernéticos modernos.

Esses recursos representam evolução relevante em relação ao modelo tradicional de firewall baseado predominantemente em regras estáticas, portas, protocolos e listas de acesso.



4.2.2. SD-WAN Integrado

A capacidade de gerenciar múltiplos links de internet de forma inteligente, mediante balanceamento baseado na qualidade dos enlaces, disponibilidade, latência, perda de pacotes e failover automático, tornou-se funcionalidade presente em plataformas modernas de NGFW.

Esse recurso apresenta especial relevância para a Câmara Municipal, considerando a utilização de múltiplos links de internet, serviços institucionais em nuvem e a necessidade de continuidade operacional.

4.2.3. Integração dos mecanismos de segurança

Outra tendência observada é a consolidação de diferentes mecanismos de proteção em uma mesma plataforma tecnológica.

Nas plataformas corporativas NGFW, funcionalidades como firewall, IPS, controle de aplicações, VPN, filtragem, gerenciamento de links, monitoramento, inteligência de ameaças, análise de eventos e gerenciamento centralizado podem operar de forma integrada e sob arquitetura comum.

Essa integração reduz a necessidade de composição manual de diversas ferramentas independentes, facilita a correlação dos eventos de segurança e permite gerenciamento mais uniforme das políticas aplicadas à infraestrutura.

4.3. Análise Comparativa das Soluções Disponíveis no Mercado

O levantamento demonstra a existência de diferentes alternativas para proteção de borda, desde soluções baseadas em software livre e firewalls convencionais até plataformas corporativas de Firewall de Próxima Geração – NGFW.

Soluções baseadas em pfSense, OPNsense ou distribuições Linux são tecnicamente viáveis para diversos cenários e podem disponibilizar importantes funcionalidades de segurança.

Entretanto, sua utilização sobre servidores de propósito geral normalmente exige maior participação do integrador ou da equipe responsável na composição da solução, dimensionamento do hardware, instalação, configuração, integração dos componentes, atualização, monitoramento e sustentação do ambiente.

Essa característica já é observada no ambiente atual da Câmara, que utiliza servidores de propósito geral executando soluções baseadas em software livre e cuja modernização constitui justamente uma das necessidades identificadas neste estudo.



Para avaliar a possibilidade de continuidade desse modelo mediante renovação completa da infraestrutura, foram levantadas referências reais para aquisição de novos servidores e contratação dos respectivos serviços de implantação e manutenção.

4.3.1. Alternativa baseada em aquisição de servidores e software livre

Considerando as características da arquitetura baseada em servidores de propósito geral e software livre, bem como a necessidade de evitar que a indisponibilidade de um único servidor resulte na interrupção integral das funções de segurança de borda, a alternativa foi dimensionada com 02 (dois) servidores corporativos, permitindo a implementação de mecanismo de redundância ou contingência entre os equipamentos.

Esse dimensionamento decorre das características próprias da alternativa analisada, na qual hardware de propósito geral, sistema operacional, software de firewall, armazenamento, interfaces de rede, módulos adicionais e demais componentes são administrados como elementos distintos da solução, exigindo mecanismos específicos de redundância e maior coordenação técnica para diagnóstico, recuperação e continuidade do ambiente.

Foram obtidas as seguintes referências:

- Dell PowerEdge R360
- Valor unitário: R\$ 64.515,51
- Quantidade: 02 unidades
- Valor total: R\$ 129.031,02

Esses valores se referem essencialmente à infraestrutura física necessária para execução da solução, não abrangendo a implantação e a sustentação continuada do firewall.

4.3.2. Implantação e manutenção da solução baseada em software livre

Também foi obtida proposta comercial para implantação e manutenção da alternativa baseada em servidores.

A proposta contempla a instalação de 01 servidor com sistema operacional OPNsense, configuração de firewall, IPS/IDS e VPN, pelo valor de R\$ 6.500,00 para implantação, acrescido de R\$ 1.750,00 mensais de manutenção.

Considerando 12 meses, o custo de manutenção representa R\$ 21.000,00,



resultando em R\$ 27.500,00 para implantação e manutenção no primeiro ano.

Assim, considerando somente os elementos efetivamente orçados, obtêm-se as seguintes referências:

- Alternativa: 02 Dell PowerEdge R360 + OPNsense
- Aquisição dos servidores: R\$ 129.031,02
- Implantação: R\$ 6.500,00
- Manutenção – 12 meses: R\$ 21.000,00
- Total estimado do 1º ano: R\$ 156.531,02

Esses valores demonstram que a utilização de software livre reduz ou elimina determinados custos de licenciamento do sistema de firewall, mas não elimina a necessidade de investimento em infraestrutura física nem os custos de implantação, integração e sustentação especializada.

Além disso, os equipamentos são adquiridos pela Administração e passam a integrar sua infraestrutura patrimonial, permanecendo sob sua responsabilidade os riscos relacionados à evolução tecnológica, eventual insuficiência futura de capacidade, término da garantia, reposição e necessidade de substituição dos ativos.

4.3.3. Diferenças de escopo entre a alternativa baseada em software livre e uma plataforma NGFW

A comparação exclusivamente financeira entre as alternativas deve ser realizada com cautela, pois os respectivos escopos não são necessariamente equivalentes.

A proposta obtida para a solução OPNsense contempla expressamente a instalação dos servidores, configuração de firewall, IPS/IDS e VPN.

O conjunto de necessidades definido neste ETP é mais amplo e contempla, entre outros recursos: Inspeção profunda de pacotes; Prevenção de intrusão; Antivírus e antimalware; Controle de aplicações; Filtragem de conteúdo; Inspeção SSL/TLS; Conectividade segura via VPN; SD-WAN; Gerenciamento centralizado; Monitoramento e alertas; Backup automatizado das configurações; Acompanhamento da saúde operacional da solução; Análise da postura de segurança; Inteligência de ameaças; Mecanismos automatizados de análise comportamental, IA e/ou Machine Learning; Atualização contínua dos mecanismos de proteção; e Suporte técnico especializado.



Não se afirma que a utilização de software livre impossibilite a implementação de tais funcionalidades. Entretanto, seu atendimento poderá depender da integração de diferentes módulos, ferramentas, bases de inteligência, serviços de terceiros e atuação especializada da empresa responsável pela sustentação.

Nas plataformas corporativas NGFW, por outro lado, essas funcionalidades tendem a integrar um mesmo ecossistema de hardware, software, licenciamento, atualização e gerenciamento, reduzindo a quantidade de componentes independentes cuja compatibilidade e manutenção precisam ser administradas.

Outro diferencial relevante se refere à atualização contínua dos mecanismos de proteção. As plataformas corporativas NGFW podem integrar, mediante as respectivas subscrições, bases de inteligência de ameaças, reputação de endereços IP, domínios, URLs e arquivos, indicadores de comprometimento, assinaturas de detecção e demais mecanismos destinados à identificação de ameaças emergentes.

Nas soluções baseadas em software livre, recursos equivalentes podem ser tecnicamente implementados, porém sua disponibilidade, abrangência e atualização dependem dos módulos, ferramentas, bases externas e serviços efetivamente adotados e mantidos no ambiente. Dessa forma, a inexistência de custo de licenciamento do software principal não representa, por si só, equivalência funcional ao conjunto de recursos de inteligência, atualização e proteção integrado às plataformas corporativas NGFW.

4.3.4. Desempenho e dimensionamento

Outro aspecto relevante está relacionado ao dimensionamento da solução.

Neste ETP foram estabelecidos parâmetros quantitativos mínimos de desempenho, incluindo throughput de firewall, VPN, NGFW/Threat Protection, antivírus, IPS, inspeção SSL/TLS, conexões simultâneas e novas conexões por segundo, devendo o appliance NGFW ofertado atender integralmente às capacidades especificadas.

Na alternativa baseada em servidores de propósito geral, a especificação isolada de processador, memória, armazenamento e interfaces não é suficiente, por si só, para comprovar o desempenho efetivo do conjunto quando firewall, IPS/IDS, VPN, inspeção de tráfego e demais mecanismos estiverem operando simultaneamente.

O resultado dependerá da combinação entre hardware, sistema operacional, drivers, módulos utilizados, volume e complexidade das regras, quantidade de



conexões e demais serviços habilitados.

Nas plataformas NGFW dedicadas, os parâmetros de desempenho são normalmente associados à arquitetura integrada do produto e podem ser comprovados por documentação técnica oficial do fabricante, nos termos previstos neste próprio ETP.

Considerando que a solução pretendida será composta por 01 (um) appliance NGFW, o equipamento deverá possuir, isoladamente, capacidade suficiente para suportar integralmente a carga operacional prevista para o ambiente da Câmara Municipal de Divinópolis, inclusive com a utilização simultânea das funcionalidades de segurança, conectividade, inspeção de tráfego, VPN, gerenciamento de links e demais recursos exigidos neste ETP.

A adoção de 01 (um) appliance NGFW não representa fracionamento ou redução da capacidade originalmente necessária à solução. O equipamento deverá ser dimensionado para suportar, isoladamente, 100% da demanda institucional prevista, observados os parâmetros mínimos de desempenho estabelecidos neste ETP, sem dependência da soma de capacidade de equipamentos adicionais para atendimento dos requisitos contratados.

O dimensionamento deverá considerar não apenas os valores nominais de throughput, mas também a capacidade efetiva da solução de manter o desempenho compatível com os requisitos mínimos estabelecidos quando submetida à operação conjunta dos mecanismos de segurança previstos para o ambiente institucional.

Dessa forma, a comparação entre a alternativa baseada em servidores de propósito geral e a plataforma NGFW deverá considerar a capacidade efetiva de cada arquitetura para atender integralmente às necessidades da Administração, observando-se desempenho, integração entre hardware e software, funcionalidades de segurança, conectividade, gerenciamento, suporte técnico, atualização tecnológica e demais requisitos definidos neste ETP.

Para fins deste estudo, a caracterização da solução como plataforma NGFW de última geração não decorre exclusivamente da data de fabricação ou lançamento do equipamento, mas da capacidade de integrar, de forma nativa ou homologada, os mecanismos avançados de segurança, gerenciamento, inteligência de ameaças, análise comportamental, conectividade, monitoramento e atualização tecnológica exigidos neste ETP, devendo o produto estar em linha regular de comercialização e suporte, sem condição de End-of-Life (EOL), End-of-Sale (EOS) ou End-of-Support (EOSP) na data da entrega.



4.3.5. Suporte, responsabilização, níveis de serviço e tratamento de falhas

Na arquitetura baseada em servidor e software livre, eventual indisponibilidade pode envolver diferentes componentes e responsáveis: hardware, armazenamento, interface de rede, sistema operacional, software de firewall, módulos adicionais ou configuração realizada pela empresa de sustentação.

Isso pode exigir análise destinada inicialmente a identificar se a origem da falha está no equipamento, no sistema operacional, em algum componente de software ou na própria configuração.

Nas plataformas corporativas integradas, hardware, sistema operacional, firmware, licenciamento e mecanismos nativos de segurança pertencem a um mesmo ecossistema tecnológico, facilitando a identificação da responsabilidade relativa ao produto e o escalonamento junto ao fabricante, desenvolvedor ou estrutura oficial de suporte.

Outro diferencial considerado na análise é a possibilidade de vincular o fornecimento da solução NGFW a níveis objetivos de serviço relacionados ao próprio produto. Conforme definido neste ETP, ocorrências críticas atribuíveis ao hardware, firmware, licenciamento, subscrição ou funcionalidades nativas da plataforma estarão submetidas a atendimento em regime 24x7, com prazos máximos de resposta e restabelecimento previamente estabelecidos.

A arquitetura com 01 (um) appliance não elimina a possibilidade de indisponibilidade decorrente de falha física do próprio equipamento. Por essa razão, a continuidade operacional não está fundamentada em redundância física entre appliances, mas na combinação entre monitoramento, suporte técnico oficial, mecanismos de contingência, níveis de serviço para restabelecimento e obrigação de substituição do equipamento quando necessária.

Na alternativa baseada em servidores próprios e software livre, a obtenção de nível equivalente de continuidade dependeria da combinação entre garantia dos servidores, disponibilidade de peças e equipamentos substitutos, suporte ao hardware, sustentação do sistema operacional e atuação da empresa responsável pelo firewall. Na proposta analisada para a solução OPNsense não foi demonstrada equivalência específica aos níveis de serviço estabelecidos neste ETP para o fornecimento da solução NGFW.

Dessa forma, a vantagem da plataforma corporativa não decorre somente da tecnologia empregada, mas também da possibilidade de estabelecer responsabilidade objetiva sobre os componentes integrantes da solução, mecanismos formais de escalonamento e prazos contratuais de atendimento,



restabelecimento e substituição compatíveis com a criticidade da infraestrutura institucional.

4.3.6. Obsolescência, ciclo de vida e atualização tecnológica

Na aquisição de servidores, a Administração realiza investimento inicial e assume o ciclo tecnológico dos equipamentos.

A evolução do tráfego, do número de conexões, da inspeção criptografada, dos mecanismos de prevenção e da utilização crescente de técnicas de análise comportamental e inteligência artificial pode elevar progressivamente os requisitos de processamento, memória, armazenamento e conectividade.

Assim, um equipamento pode permanecer fisicamente operacional e, ainda assim, deixar de possuir capacidade adequada ao cenário tecnológico futuro.

Nessa hipótese, a Administração poderá necessitar de novas expansões ou de substituição dos servidores, mediante novo investimento.

Esse risco é reduzido no modelo de locação com cessão de uso/comodato previsto neste ETP, no qual a atualização tecnológica e a substituição da plataforma, nas hipóteses contratualmente definidas, permanecem sob responsabilidade da contratada.

No modelo de locação adotado neste ETP, o appliance deverá permanecer em condição regular de suporte e compatibilidade tecnológica. Não serão admitidos equipamentos que, na data da entrega, estejam em condição de End-of-Life – EOL, End-of-Sale – EOS ou End-of-Support – EOSP, e, caso tais condições ocorram durante a vigência e comprometam o suporte, a atualização, a segurança ou a continuidade operacional, estará prevista a substituição por equipamento equivalente ou superior.

Essa característica reduz o risco de a Administração permanecer vinculada a ativo patrimonial ainda fisicamente operacional, porém tecnologicamente insuficiente ou sem suporte adequado para as necessidades de segurança da rede.

4.3.7. Cadeia de fornecimento, suporte oficial e governança tecnológica

Nas plataformas corporativas NGFW, outro aspecto considerado no levantamento refere-se à existência de cadeia formal de fornecimento, licenciamento, atualização, garantia e suporte.

O modelo permite vincular equipamentos, firmware, licenças, subscrições,



direitos de atualização e suporte técnico à estrutura oficial do fabricante, desenvolvedor, distribuidor ou parceiro tecnicamente habilitado, proporcionando maior rastreabilidade sobre a origem e a manutenção dos componentes tecnológicos integrantes da solução.

Essa estrutura também amplia as possibilidades de escalonamento técnico quando a solução de determinado incidente ultrapassar a capacidade de atuação da empresa responsável pela sustentação operacional, permitindo o acionamento da estrutura oficial associada ao produto.

Em soluções montadas sobre servidores próprios e diferentes componentes de software, a governança tecnológica poderá ficar mais distribuída entre fabricante do servidor, sistema operacional, módulos adicionais, bases de segurança e empresa integradora, exigindo maior coordenação para identificação e resolução de problemas.

A existência de uma cadeia oficial de atualização e suporte não elimina a necessidade da contratação especializada de administração e sustentação do ambiente, porém reduz a dependência exclusiva do integrador para questões relacionadas ao produto, firmware, licenciamento, garantia e componentes nativos da plataforma.

4.3.8. Atualização controlada e gestão do ciclo de mudanças

Outro aspecto relevante das plataformas corporativas NGFW é a existência de ciclo estruturado de atualização associado ao próprio produto, envolvendo firmware, software, assinaturas, mecanismos de proteção, documentação técnica oficial, notas de versão, recomendações e suporte especializado.

A atualização de uma plataforma de segurança não deve ser analisada apenas sob a perspectiva da disponibilidade de novas versões. Alterações em firmware, mecanismos de inspeção ou componentes de segurança podem afetar disponibilidade, compatibilidade, desempenho e funcionamento do ambiente, tornando necessário procedimento controlado de avaliação, backup, atualização, validação e, quando necessário, rollback.

No modelo previsto neste ETP, a contratada responsável pelo fornecimento deverá disponibilizar os componentes e informações oficiais necessários às atualizações e prestar suporte técnico quando necessário, enquanto a execução operacional será realizada de forma coordenada com a empresa responsável pela sustentação.

Nas soluções baseadas em servidores e composição de diferentes componentes



de software, procedimentos equivalentes também podem ser implementados, porém sua coordenação depende da compatibilidade entre sistema operacional, drivers, módulos, pacotes, ferramentas complementares e demais elementos utilizados. A integração nativa ou homologada da plataforma corporativa reduz essa fragmentação e proporciona maior previsibilidade no gerenciamento das mudanças.

4.3.9. Eficiência energética, ciclo de vida e sustentabilidade

A avaliação das alternativas também deve considerar os custos e impactos associados à operação física da infraestrutura durante todo o ciclo de vida da solução.

Appliances dedicados de segurança são desenvolvidos especificamente para execução de funções de proteção e inspeção de tráfego, tendendo a apresentar maior eficiência operacional e energética e menor quantidade de componentes físicos quando comparados a arquiteturas equivalentes baseadas em servidores de propósito geral.

Na alternativa baseada em servidores próprios, além da aquisição inicial, permanecem com a Administração a operação dos equipamentos durante seu ciclo de utilização e, posteriormente, a gestão patrimonial e a destinação dos ativos quando se tornarem obsoletos ou inservíveis.

No modelo de locação com cessão de uso/comodato, a retirada dos equipamentos ao término da contratação e sua destinação, quando aplicável, permanecem sob responsabilidade da contratada, reduzindo a formação de estoque patrimonial de equipamentos tecnológicos obsoletos e contribuindo para a gestão sustentável do ciclo de vida da solução.

4.3.10. Governança, rastreabilidade e capacidade de auditoria

A análise das alternativas também deve considerar a capacidade de governança e fiscalização da infraestrutura de segurança.

A plataforma NGFW pretendida deverá disponibilizar mecanismos integrados de gerenciamento, registro de eventos, geração de logs, trilhas de auditoria, relatórios e identificação de informações relevantes sobre os acessos, permitindo maior rastreabilidade das ações executadas no ambiente e proporcionando suporte às atividades de fiscalização, auditoria e investigação de incidentes.

Embora mecanismos equivalentes possam ser implementados em soluções baseadas em software livre, sua abrangência dependerá das ferramentas,



módulos e integrações efetivamente implantados e mantidos. Em uma plataforma corporativa integrada, tais mecanismos podem fazer parte do próprio ecossistema tecnológico e compartilhar políticas, identidade, eventos e informações operacionais da solução.

Essa integração proporciona maior uniformidade das informações disponibilizadas à Administração e facilita as atividades de governança, fiscalização contratual, auditoria e apuração de incidentes de segurança.

4.4. Das formas de contratação da solução de segurança

A definição do modelo de contratação deve considerar não apenas os custos financeiros envolvidos, mas também a natureza crítica da segurança de rede, a necessidade de atualizações constantes frente a novas ameaças cibernéticas, a continuidade operacional, a responsabilidade sobre os ativos e os riscos associados à obsolescência tecnológica.

Nesse contexto, foram consideradas três modalidades principais.

a) Aquisição de servidores e utilização de software livre

Modelo em que a Administração adquire os servidores necessários e contrata, separadamente, empresa especializada para instalação, configuração, manutenção e sustentação da solução.

A alternativa é tecnicamente possível, porém exige desembolso inicial para aquisição dos equipamentos, mantém os ativos sob responsabilidade patrimonial da Administração e demanda contratação continuada para sustentação do ambiente.

Além disso, eventual necessidade futura de aumento de capacidade ou substituição tecnológica poderá exigir novas aquisições.

b) Aquisição definitiva de appliances NGFW e respectivos licenciamentos

Modelo em que a Administração adquire os appliances e contrata os licenciamentos, subscrições, garantias e demais serviços necessários.

Embora permita utilização de plataforma corporativa integrada, essa modalidade também demanda investimento inicial relevante, incorpora os equipamentos ao patrimônio público e mantém com a Administração parte do risco relacionado ao ciclo de vida dos ativos e futuras atualizações de hardware.

c) Contratação de solução integrada em regime de locação com cessão de uso/comodato



Modelo em que a solução é disponibilizada de forma contínua, incluindo 01 (um) appliance dedicado, licenciamento/subscrição durante toda a vigência contratual, suporte técnico oficial e atualização tecnológica nos termos estabelecidos contratualmente.

Essa alternativa reduz a necessidade de investimento inicial na aquisição do appliance e transfere à contratada responsabilidades relacionadas à propriedade, garantia, substituição e atualização tecnológica dos equipamentos durante a vigência.

O modelo também possibilita maior integração entre hardware, firmware, sistema operacional, licenciamento e mecanismos de segurança, proporcionando maior previsibilidade tecnológica e facilitando o gerenciamento da continuidade da solução.

Registra-se que a adoção do modelo de locação com cessão de uso/comodato não elimina a necessidade da contratação correlata dos serviços especializados de implantação, configuração, administração, monitoramento e sustentação operacional, já prevista neste ETP.

A vantagem comparativa desta modalidade concentra-se na camada tecnológica disponibilizada de forma integrada — appliance, sistema operacional, licenciamento, subscrições, garantia, suporte oficial e atualização tecnológica — e na transferência dos riscos relacionados a esses componentes para a contratada, permanecendo os serviços operacionais especializados sujeitos a contratação e responsabilidades próprias.

4.5. Referências preliminares de valores das alternativas

Para fins exclusivamente comparativos do levantamento de mercado, foram consideradas as seguintes referências preliminares:

Alternativa	Referência
02 PowerEdge R360 + implantação + 12 meses de manutenção	R\$ 156.531,02 no primeiro ano
Plataforma corporativa BluePex	aproximadamente R\$ 12.600,00/mês
Plataforma corporativa Fortinet	aproximadamente R\$ 20.000,00/mês

Em termos anualizados, as referências informadas para as plataformas corporativas correspondem aproximadamente a R\$ 151.200,00 e R\$ 240.000,00, respectivamente.

Os valores acima não permitem concluir, isoladamente, que determinada



arquitetura seja economicamente superior às demais, pois os escopos, responsabilidades, funcionalidades e riscos associados a cada modelo são distintos.

As referências de valores apresentadas possuem caráter exclusivamente indicativo para o levantamento de mercado e não pressupõem identidade quantitativa ou integral equivalência de configuração entre as soluções pesquisadas e a arquitetura definida neste ETP. Em especial, os valores relativos às plataformas corporativas pesquisadas não devem ser interpretados, isoladamente, como estimativa definitiva do custo da solução atualmente dimensionada para 01 (um) appliance NGFW.

Especialmente no caso da solução baseada em servidores e software livre, o valor apresentado para manutenção contempla o escopo constante da proposta recebida, não havendo demonstração, nessa cotação específica, de equivalência integral a todas as funcionalidades e condições exigidas para a solução NGFW pretendida.

A estimativa definitiva da contratação deverá considerar especificamente o fornecimento de 01 (um) appliance NGFW dimensionado para atendimento integral da demanda institucional, acompanhado dos licenciamentos, subscrições, gerenciamento, suporte técnico oficial, garantia, atualização tecnológica e demais componentes exigidos neste ETP.

A comparação econômica definitiva deverá, portanto, considerar o custo global de cada alternativa em condições equivalentes de atendimento, incluindo hardware, implantação, licenciamento quando aplicável, suporte, sustentação, atualização tecnológica, garantia, substituição, recursos avançados de segurança e demais componentes necessários.

4.6. Análise Comparativa da Aderência das Soluções

A utilização de servidores próprios com software livre permanece alternativa tecnicamente possível e pode apresentar custo nominal inferior em determinados períodos ou configurações.

Entretanto, para o cenário institucional analisado, essa alternativa apresenta maior dependência da integração realizada pelo prestador de serviços, da manutenção de múltiplos componentes e da capacidade dos servidores adquiridos de acompanhar a evolução das demandas de segurança durante seu ciclo de utilização.

As plataformas corporativas NGFW apresentam, por sua vez, maior integração



entre hardware, firmware, sistema operacional, mecanismos de proteção, gerenciamento, licenciamento, inteligência de ameaças e suporte técnico.

Essa integração se torna especialmente relevante para o cenário da Câmara Municipal, que demanda simultaneamente inspeção avançada, VPN, SD-WAN, monitoramento, gerenciamento centralizado, inteligência de ameaças, análise da postura de segurança, mecanismos automatizados de detecção e recursos voltados à continuidade operacional da solução.

Além disso, quando a plataforma NGFW é disponibilizada em regime de locação com cessão de uso/comodato:

- a) Não há necessidade de aquisição inicial do appliance pela Administração;
- b) Evita-se a incorporação de ativos tecnológicos sujeitos à rápida defasagem ao patrimônio da Câmara;
- c) Reduz-se a necessidade de novos investimentos exclusivamente para substituição tecnológica dos equipamentos;
- d) Transfere-se à contratada parte relevante dos riscos relacionados a defeitos, obsolescência, perda de suporte e substituição de hardware;
- e) Assegura-se a continuidade dos licenciamentos e subscrições durante a vigência contratual;
- f) Permite-se estabelecer contratualmente mecanismos de atualização tecnológica;
- g) Proporciona-se maior previsibilidade quanto à manutenção da capacidade e da compatibilidade tecnológica da solução ao longo da contratação;
- h) Reduz-se o risco de permanência, no patrimônio da Administração, de equipamentos de segurança tecnologicamente obsoletos, cuja utilização tenha deixado de ser recomendável apesar de ainda permanecerem fisicamente operacionais;
- i) Ao término da contratação, em caso de não renovação ou substituição da solução, a retirada do appliance e a destinação dos equipamentos disponibilizados permanecem sob responsabilidade da contratada, conforme as condições estabelecidas neste ETP;
- j) Favorece maior previsibilidade orçamentária da camada tecnológica da solução, ao concentrar no valor periódico contratado a disponibilização do appliance, licenciamento/subscrições, garantia, suporte oficial e as obrigações de



substituição e atualização tecnológica previstas contratualmente, reduzindo a exposição da Administração a desembolsos não planejados relacionados a esses componentes durante a vigência; e

k) Permite concentrar a capacidade de processamento e os recursos de segurança em 01 (um) appliance NGFW dimensionado para suportar integralmente a demanda institucional, reduzindo a quantidade de equipamentos físicos da camada de segurança perimetral sem reduzir os requisitos mínimos de desempenho, licenciamento e funcionalidades definidos para a solução.

Outro benefício operacional considerado é a redução da dependência de atividades manuais rotineiras pela equipe interna de TI. A centralização de políticas, alertas, informações de saúde dos equipamentos, eventos de segurança e mecanismos de diagnóstico proporciona maior capacidade de acompanhamento e fiscalização da solução, permitindo que a equipe da Administração concentre seus esforços na governança e na análise estratégica do ambiente, sem afastar as atribuições da empresa responsável pela sustentação operacional.

4.6.1. Síntese comparativa dos modelos analisados

Aspecto	Servidores próprios + software livre	NGFW adquirido	NGFW em locação/comodato
Aquisição inicial de hardware	Necessária	Necessária	Não necessária pela Administração
Propriedade dos equipamentos	Administração	Administração	Contratada
Integração hardware/software	Depende da composição e integração realizadas	Plataforma integrada	Plataforma integrada
Licenciamento/subscrições	Conforme ferramentas adotadas	Contratados pela Administração	Mantidos durante a vigência contratual
Inteligência de ameaças	Depende das bases, módulos e serviços adotados	Conforme licenciamento	Integrada conforme subscrição ofertada
Atualizações de segurança	Dependem dos componentes utilizados	Conforme contratos de suporte/licença	Previstas durante a vigência
Comprovação de desempenho	Depende da combinação entre hardware e software	Documentação oficial do produto	Documentação oficial do produto
Risco de obsolescência do hardware	Administração	Administração	Transferido à contratada nas hipóteses contratuais
EOL/EOS/EOSP	Exige providência e eventual novo investimento	Exige providência da Administração	Substituição prevista quando comprometer a solução
Garantia e substituição de hardware	Conforme garantia adquirida	Conforme contratação	Responsabilidade contratual do fornecedor



Aspecto	Servidores próprios + software livre	NGFW adquirido	NGFW em locação/comodato
SLA relacionado ao produto	Depende dos contratos contratados	Conforme contratação	Definido contratualmente
Cadeia oficial de suporte	Depende dos componentes utilizados	Existente	Integrada ao fornecimento
Destinação ao fim do ciclo	Administração	Administração	Retirada pela contratada
Administração e sustentação operacional	Contratação específica	Contratação específica	Contratação específica
Eficiência energética e gestão do fim do ciclo	Depende da configuração dos servidores; gestão e destinação dos ativos pela Administração	Gestão e destinação pela Administração	Appliance dedicado e retirada/destinação conforme responsabilidades contratuais da contratada
Governança e esforço operacional da equipe interna	Dependente das ferramentas e integrações implantadas	Gerenciamento integrado conforme solução/licenciamento	Gerenciamento integrado, monitoramento e recursos tecnológicos mantidos durante a vigência

4.7. Conclusão do Levantamento

O levantamento de mercado demonstra a existência de múltiplas alternativas capazes de executar funções de segurança de borda, incluindo soluções baseadas em software livre sobre servidores próprios e plataformas corporativas NGFW.

A alternativa baseada em servidores e software livre permanece tecnicamente possível, especialmente quando acompanhada de contratação especializada para implantação e sustentação. Entretanto, exige investimento inicial em hardware, contratação específica de implantação e manutenção, integração entre diferentes componentes e permanência dos riscos relacionados ao ciclo tecnológico dos equipamentos sob responsabilidade da Administração.

As plataformas corporativas de Firewall de Próxima Geração apresentam maior aderência ao conjunto de requisitos técnicos e operacionais identificados neste ETP, especialmente por integrarem em uma mesma arquitetura mecanismos avançados de proteção, gerenciamento centralizado, inteligência de ameaças, conectividade segura, monitoramento, suporte técnico especializado e atualização tecnológica.

Quando disponibilizadas em regime de locação com cessão de uso/comodato, acrescenta-se ainda a vantagem de reduzir o investimento inicial na aquisição de ativos e transferir à contratada parte relevante dos riscos de propriedade, garantia, obsolescência e atualização tecnológica.

Não se conclui, neste momento, que a modalidade de locação seja



necessariamente a alternativa de menor custo nominal quando comparada à aquisição de servidores com software livre. A vantagem identificada está principalmente na maior aderência técnica e operacional, na integração da solução, na redução da imobilização inicial de recursos e na transferência de riscos tecnológicos para a contratada.

A análise também evidencia diferenças relevantes quanto ao ciclo de vida da solução, continuidade dos licenciamentos e subscrições, disponibilidade de suporte oficial, níveis de serviço associados ao produto, atualização permanente dos mecanismos de segurança, substituição de equipamentos em situações de descontinuidade ou insuficiência tecnológica e definição mais objetiva das responsabilidades relacionadas aos componentes integrantes da plataforma.

Dessa forma, considerando a criticidade dos serviços institucionais, a evolução das ameaças cibernéticas, a necessidade de atualização contínua e os requisitos definidos pela Câmara Municipal de Divinópolis, o modelo baseado em plataforma corporativa NGFW de última geração, disponibilizada de forma integrada e em regime de locação com cessão de uso/comodato, apresenta maior aderência ao conjunto das necessidades técnicas, operacionais e de continuidade identificadas.

A solução será composta por 01 (um) appliance NGFW dedicado, dimensionado para atender isoladamente e de forma integral à demanda institucional e aos parâmetros mínimos de desempenho estabelecidos neste ETP, acompanhado dos licenciamentos, subscrições, gerenciamento, suporte técnico oficial, garantia e mecanismos de atualização tecnológica necessários durante toda a vigência contratual.

A adoção de equipamento único não se fundamenta na existência de redundância física entre appliances, mas na capacidade integral do equipamento, na integração tecnológica da plataforma e nos mecanismos contratuais de monitoramento, suporte, contingência, restabelecimento e substituição, permitindo reduzir a quantidade de componentes físicos sem reduzir os requisitos de segurança e desempenho exigidos pela Administração.

5. REQUISITOS DA SOLUÇÃO



5.1. Arquitetura e Performance (Hardware) para suportar o tráfego crescente e a inspeção profunda de pacotes (DPI) deverá apresentar capacidade de processamento adequada ao ambiente da Câmara Municipal de Divinópolis, comprovada por documentação oficial do fabricante, considerando operação simultânea de firewall, mecanismos de prevenção de intrusão, antivírus/antimalware, controle de aplicações, conectividade segura, gerenciamento inteligente de links, filtragem de conteúdo e inspeção avançada de tráfego, sem degradação incompatível com os níveis mínimos de serviço definidos neste ETP, devendo observar, no mínimo, os seguintes requisitos técnicos:

5.1.1. Conformidade Appliance

A solução deverá ser composta por appliance dedicado de segurança, com integração nativa ou homologada entre hardware, sistema operacional e licenciamento da plataforma ofertada, sendo vedado o uso de servidores genéricos, soluções improvisadas ou não homologadas pelo fabricante da plataforma de segurança.

5.1.2. Processamento e Memória

A solução deverá possuir recursos de processamento, memória e arquitetura adequada à operação simultânea dos serviços de firewall, prevenção de intrusões, antivírus/antimalware, conectividade segura, gerenciamento inteligente de links, controle de aplicações, filtragem de conteúdo e inspeção avançada de tráfego, devendo o desempenho ser comprovado por documentação oficial do fabricante.

5.1.3. Conectividade

O appliance deverá possuir interfaces de rede em quantidade suficiente para permitir a conexão simultânea de links WAN, redes LAN, DMZ, segmentação de redes internas, redes de visitantes e futuras expansões da infraestrutura, conforme dimensionamento da solução.

As interfaces deverão suportar velocidades compatíveis com os requisitos mínimos de desempenho estabelecidos neste ETP.

5.1.4. Expansibilidade

A solução deverá possuir recursos que permitam futura evolução da conectividade para 10GbE ou superior, mediante interfaces nativas, portas SFP/SFP+, módulos de expansão ou tecnologia equivalente compatível com a arquitetura ofertada, sem necessidade de substituição integral da plataforma.

5.1.5. Especificações mínimas do appliance NGFW



Para fins de dimensionamento objetivo da solução, a tabela abaixo consolida os parâmetros quantitativos mínimos de hardware, capacidade e desempenho exigidos para o appliance NGFW, sem prejuízo dos requisitos qualitativos, funcionais e de arquitetura estabelecidos nos itens 5.1.1 a 5.1.4. O appliance deverá atender integralmente aos requisitos aplicáveis, não sendo admitido atendimento parcial aos parâmetros mínimos de desempenho.

Especificação	Mínimo Exigido
Quantidade de appliances	01 (um)
Número mínimo de dispositivos suportados, sem limitação técnica ou de licenciamento inferior a esse quantitativo	500
Interfaces de rede	10 interfaces Ethernet 10/100/1000 Mbps
Velocidade de cada interface	1 Gbps
Interface de console	1
Instalação	Rack padrão 19" com kit de fixação
Throughput de Firewall	10 Gbps
Throughput de VPN	8,2 Gbps
NGFW / Threat Protection	1,5 Gbps
Throughput de Antivírus HTTP (HTTP AV Throughput)	7,3 Gbps
Throughput de IPS	5,3 Gbps
SSL/TLS Inspection	1 Gbps
Conexões simultâneas	1250000
Novas conexões por segundo	25000
Alimentação elétrica	Fonte Full Range (100~240 VCA, 50/60 Hz ou equivalente de acordo com o equipamento)

O appliance deverá atender integralmente às especificações mínimas estabelecidas, possuindo capacidade suficiente para suportar toda a demanda da rede institucional e a utilização simultânea das funcionalidades e mecanismos de segurança exigidos neste ETP.

5.2. Inteligência e Segurança (Software)

5.2.1. Controle de Aplicações e Análise Comportamental

Identificação e controle de aplicações independentemente da porta ou protocolo utilizado, incluindo redes sociais, aplicativos de comunicação, VPNs, proxies, serviços de acesso remoto, aplicações de streaming e demais serviços de camada 7, permitindo aplicação de políticas baseadas em comportamento, categoria, risco, usuário, grupo ou perfil de utilização.



5.2.2. Prevenção de Intrusão (IPS)

Inspeção de tráfego e análise de ameaças para identificação, bloqueio e mitigação de tentativas de invasão, exploração de vulnerabilidades, tráfego malicioso, malwares, ransomwares, trojans, worms, comunicações suspeitas e comportamentos maliciosos, utilizando, quando disponível na solução ofertada, mecanismos de inteligência de ameaças (Threat Intelligence), reputação de IPs, domínios, URLs, arquivos ou tecnologias equivalentes.

5.2.3. Controle de Conteúdo

Filtro Web corporativo com categorização dinâmica de conteúdo, atualização contínua de categorias, criação de listas de permissão e bloqueio, políticas distintas por rede, usuário ou grupo, geração de relatórios de navegação e possibilidade de diagnóstico de bloqueios ou liberações de URLs.

5.2.4. Gestão de Certificados

Criação e revogação de certificados SSL/TLS via interface gráfica para inspeção de tráfego criptografado.

5.3. Conectividade e Redes Avançadas

5.3.1. Roteamento Dinâmico

Suporte a protocolos de roteamento dinâmicos aderentes a ambientes corporativos e integração com múltiplos links e redes, permitindo integração com múltiplas unidades administrativas ou ambientes de nuvem pública.

5.3.2. VPN (Virtual Private Network)

Suporte a túneis VPN Site-to-Site e Client-to-Site, incluindo IPsec, SSL VPN, VPN baseada em TLS/SSL ou tecnologias equivalentes, com possibilidade de autenticação integrada a bases corporativas, geração de logs de conexão, relatórios de uso e alertas de conexão ou desconexão, quando tecnicamente disponível na solução ofertada.

5.3.3. Serviços Críticos e Priorização de Tráfego

Suporte a DNS Dinâmico, NetFlow ou tecnologia equivalente, SNMP, NTP, DHCP Relay, recursos de análise de tráfego, QoS e demais funcionalidades de conectividade corporativa aderentes à arquitetura ofertada.

5.4. Gestão Centralizada, Monitoramento e Continuidade Operacional



A solução deverá oferecer mecanismo de gerenciamento centralizado, preferencialmente por meio de painel em nuvem, admitindo-se ambiente local, híbrido ou tecnologia equivalente, desde que permita administração unificada, monitoramento contínuo, gerenciamento centralizado do appliance, visualização, em tempo real, das informações operacionais e acompanhamento da saúde da solução.

A plataforma deverá disponibilizar, no mínimo, os seguintes recursos:

5.4.1. Backup Automático das Configurações

Realização de backup periódico e automatizado das configurações da solução, com retenção mínima de 5 (cinco) versões válidas para fins de restauração, contingência e manutenção da operação.

5.4.2. Visibilidade Operacional e Eventos de Segurança

Disponibilização de painéis, relatórios, gráficos e recursos de visualização operacional que permitam acompanhamento em tempo real dos eventos de segurança, podendo incluir representações estatísticas, históricas, geográficas ou equivalentes, quando suportadas pela solução ofertada.

5.4.3. Monitoramento e Alertas

Disponibilização de recursos de monitoramento contínuo com geração de alertas operacionais, podendo incluir aplicativo móvel, painel web, e-mail, integração com plataformas de monitoramento ou mecanismos equivalentes para notificação de indisponibilidade, degradação de links, perda de pacotes, latência elevada, falhas operacionais, eventos críticos de segurança ou indisponibilidade de serviços monitorados.

5.4.4. Gerenciamento Inteligente de Links (SD-WAN)

Suporte a balanceamento de carga, failover automático e priorização de tráfego com base em critérios técnicos como latência, perda de pacotes, disponibilidade e desempenho dos links de comunicação.

5.4.5. Gerenciamento Centralizado de Políticas

Possibilidade de gerenciamento centralizado de regras, políticas de segurança, objetos de rede, VPNs, perfis de inspeção, relatórios e demais configurações relevantes da solução.

5.4.6. Acompanhamento da Saúde Operacional



Disponibilização de informações relativas ao estado operacional do appliance, utilização de CPU, memória, armazenamento, interfaces, throughput, links, VPNs, qualidade dos links e demais indicadores relevantes para gestão da infraestrutura de segurança, possibilitando o acompanhamento contínuo da saúde operacional da solução, a identificação preventiva de degradações de desempenho, indisponibilidades, falhas operacionais e eventuais inconsistências de configuração que possam comprometer a segurança, a disponibilidade ou o desempenho do ambiente.

5.4.7. Análise de Risco, Postura de Segurança e Recomendações

A plataforma deverá disponibilizar recursos de avaliação contínua da postura de segurança (Security Posture Assessment), análise de risco da configuração, recomendações de boas práticas, alertas operacionais e histórico de eventos, permitindo acompanhar a conformidade das regras de firewall, NAT, VPN, usuários administrativos, senhas, objetos de rede, políticas de segurança, links e demais componentes críticos da solução, emitindo recomendações técnicas de melhoria sempre que aplicável.

5.4.8 Inteligência de Ameaças

A solução deverá utilizar mecanismos de inteligência de ameaças (Threat Intelligence), quando disponíveis na plataforma ofertada, com atualização contínua de indicadores de comprometimento (IoCs), reputação de endereços IP, domínios, URLs, arquivos e demais informações relevantes para prevenção, identificação e resposta a ameaças cibernéticas emergentes, podendo utilizar bases próprias do fabricante ou serviços equivalentes integrados.

5.5. Requisitos de suporte e SLA (Nível de Serviço)

5.5.1. Substituição Proativa

A contratada deverá garantir atualização da plataforma de segurança sempre que o appliance fornecido entrar em processo de descontinuidade, fim de suporte, fim de vida útil, incompatibilidade com licenças vigentes ou incapacidade comprovada de atendimento aos requisitos mínimos de desempenho e segurança contratados, sem ônus adicional para a Contratante.

5.5.2. Suporte Direto

Acesso a atendimento humano especializado, prestado pelo fabricante, desenvolvedor da solução, representante autorizado, parceiro certificado ou



equipe técnica formalmente habilitada para a solução ofertada, em língua portuguesa, por meio de chat, telefone, e-mail ou canais equivalentes.

5.5.3. Intervenção Remota

Possibilidade de suporte remoto especializado pelo fabricante, desenvolvedor da solução, parceiro autorizado ou equipe técnica formalmente habilitada, mediante autorização prévia da Contratante e observadas as políticas de segurança, auditoria e controle de acesso.

5.6. Aspectos Complementares da Contratação

5.6.1. Treinamento e Transferência de Conhecimento

Como parte da solução fornecida, deverá ser realizado treinamento técnico destinado à equipe de Tecnologia da Informação da Câmara Municipal, com o objetivo de proporcionar conhecimento prévio da ferramenta, promover o nivelamento técnico e desenvolver a capacidade de acompanhamento e interlocução sobre a solução fornecida, bem como preparar a equipe técnica para acompanhar sua posterior implementação no âmbito da contratação dos serviços correspondentes.

O treinamento deverá possuir carga horária mínima de 8 (oito) horas, podendo ser realizado de forma presencial, remota ou híbrida, ou através de cursos em videoaulas, desde que sejam asseguradas condições adequadas para a efetiva transferência de conhecimento.

O treinamento poderá ser ministrado pelo fabricante, parceiro autorizado ou fornecedor da solução, desde que o instrutor possua conhecimento técnico compatível com a solução ofertada, comprovado por certificação conforme item 8.2.4. A realização deste treinamento possui caráter de capacitação técnica da equipe da Câmara Municipal e não se confunde com os serviços de implementação, configuração e demais atividades atribuídas à contratação específica dos serviços de implementação da solução.

O conteúdo programático deverá contemplar, no mínimo, quando aplicável às funcionalidades efetivamente contratadas:

- a)** Arquitetura e funcionamento geral da solução;
- b)** Administração das políticas de segurança;
- c)** Criação, alteração e revisão de regras de firewall;
- d)** Administração de objetos, grupos e serviços;
- e)** Configuração e administração de VPNs;



- f) Administração de regras de NAT;
- g) Administração das funcionalidades de segurança disponibilizadas pela solução;
- h) Monitoramento operacional, análise de eventos e interpretação de logs;
- i) Geração e interpretação de relatórios técnicos, quando aplicável;
- j) Administração dos mecanismos de autenticação integrados;
- k) Administração dos backups das configurações e procedimentos de restauração;
- l) Procedimentos para atualização da solução, observadas as responsabilidades previstas no contrato;
- m) Boas práticas de administração, segurança da informação e continuidade operacional;
- n) Procedimentos básicos para identificação, tratamento e escalonamento de incidentes;
- o) Esclarecimento de dúvidas e realização de atividades práticas, sempre que tecnicamente possível.

Ao término do treinamento, deverá ser disponibilizado material didático, documentação técnica ou conteúdo equivalente utilizado durante a capacitação, em formato digital, bem como emitido certificado, declaração ou documento equivalente que comprove sua realização.

5.6.2. Conformidade com a LGPD

A solução deve permitir a exportação de logs de acesso de usuários para fins de auditoria, conforme princípios de segurança, prevenção e responsabilização. Também deverá possibilitar a guarda centralizada de logs pelo período definido na política institucional da Câmara Municipal de Divinópolis ou conforme legislação vigente e a exportação em formatos auditáveis (como CSV ou PDF). Também deverá possuir recursos que permitam identificar usuários, horários, origem dos acessos e ações executadas no ambiente de rede, quando tecnicamente aplicável à solução ofertada e à arquitetura implantada, em conformidade com o princípio da responsabilização (accountability) previsto na Lei Geral de Proteção de Dados (LGPD).

5.6.3. Suporte técnico

Independentemente da origem da solução ofertada, é indispensável que esta disponha de suporte técnico disponível em língua portuguesa e acessível à Administração nos níveis de serviço contratados, mecanismos compatíveis com políticas de soberania de



dados e recursos adequados de auditoria, rastreabilidade de acessos e gestão da segurança da informação, contribuindo para o atendimento dos princípios e obrigações aplicáveis da LGPD, para a continuidade operacional, a segurança institucional e a adequada governança do ambiente tecnológico.

6. ESTIMATIVA DAS QUANTIDADES E ESPECIFICAÇÕES DA SOLUÇÃO PRETENDIDA

A presente contratação prevê o fornecimento de solução integrada de segurança de borda, composta por 1 (um) appliance dedicado, subscrição/licenciamento durante toda a vigência contratual, suporte técnico oficial da solução, garantia, atualização tecnológica e dA presente contratação prevê o fornecimento de solução integrada de segurança de borda, composta por 01 (um) appliance NGFW dedicado, subscrição/licenciamento durante toda a vigência contratual, suporte técnico oficial da solução, garantia, atualização tecnológica e demais componentes necessários ao pleno funcionamento da solução, dimensionada considerando atendimento simultâneo estimado de aproximadamente 350 dispositivos.

A solução fornecida deverá possuir, desde sua disponibilização inicial, capacidade técnica e de licenciamento para suportar no mínimo 500 dispositivos, conforme estabelecido no item 5.1.5, de modo a absorver o crescimento estimado do ambiente institucional.

A implantação física, configuração lógica, migração, integração com os ambientes existentes, transferência de conhecimento operacional relacionada ao ambiente implantado, testes, homologação, operação assistida e demais serviços especializados serão executados por empresa contratada especificamente para prestação desses serviços, conforme contratação correlata.

A transferência de conhecimento operacional prevista neste item não se confunde com o treinamento técnico da solução previsto no item 5.6.1, o qual integra a presente contratação de fornecimento e mais componentes necessários ao pleno funcionamento da solução, dimensionada considerando atendimento simultâneo estimado de aproximadamente 350 dispositivos. A solução fornecida deverá possuir, desde sua disponibilização inicial, capacidade técnica e de licenciamento para suportar no mínimo 500 dispositivos, conforme estabelecido no item 5.1.5, de modo a absorver o crescimento estimado do ambiente institucional.

A implantação física, configuração lógica, migração, integração com os ambientes existentes, transferência de conhecimento operacional relacionada ao ambiente implantado, testes, homologação, operação assistida e demais serviços especializados serão executados por empresa contratada especificamente para prestação desses



serviços, conforme contratação correlata.

6.1. Dimensionamento da Infraestrutura e Capacidade Operacional

O dimensionamento da solução proposta foi elaborado com base no cenário atual de utilização do ambiente tecnológico da Câmara Municipal de Divinópolis, considerando o ambiente operacional existente, a projeção de crescimento institucional e a necessidade de continuidade dos serviços legislativos e administrativos.

Atualmente, a infraestrutura de conectividade da Câmara opera com 3 (três) links de internet ativos, estando previsto novo processo licitatório para contratação de 2 (dois) links dedicados com capacidade mínima estimada de 1 Gbps Full Duplex, destinados à substituição da infraestrutura atual de conectividade, contemplando redundância operacional, balanceamento de tráfego e manutenção da VPN corporativa entre a sede e o prédio anexo.

A solução deverá suportar gerenciamento inteligente dos links, redundância operacional, balanceamento de tráfego e manutenção de conectividade segura via VPN corporativa entre a sede da Câmara Municipal, localizada na Rua São Paulo, nº 277, Centro, Divinópolis/MG, e o prédio anexo localizado na Rua Antônio Olímpio de Moraes, nº 545, Centro, Divinópolis/MG, assegurando comunicação segura, disponibilidade operacional e integração contínua entre os ambientes institucionais.

O ambiente atual possui aproximadamente:

- a)** Rede interna cabeada com capacidade operacional estimada em 300 Mbps Full Duplex;
- b)** Infraestrutura de rede sem fio (Wi-Fi) com utilização aproximada de 100 Mbps Full Duplex;
- c)** Ambiente de acesso remoto e VPN com consumo estimado em 70 Mbps Full Duplex.

A infraestrutura deverá suportar a evolução previsível da demanda institucional, considerando a ampliação do uso de sistemas baseados em nuvem, transmissão de sessões legislativas, acesso remoto seguro e utilização crescente de dispositivos móveis.

O quantitativo estimado foi definido com base na infraestrutura atualmente existente, nas condições normais de operação administrativa e legislativa, na projeção de crescimento institucional e na expansão dos serviços digitais, considerando o aumento do uso de sistemas em nuvem, acessos remotos, dispositivos móveis e demais necessidades futuras de conectividade e disponibilidade. Para fins de



dimensionamento, a solução deverá possuir capacidade operacional para atendimento simultâneo estimado de aproximadamente 350 dispositivos, devendo a solução fornecida possuir, desde sua disponibilização inicial, capacidade técnica e de licenciamento para suportar no mínimo 500 dispositivos, conforme estabelecido no item 5.1.5, durante a vigência da contratação, inclusive para absorver eventuais aumentos de utilização decorrentes de sessões extraordinárias, audiências públicas, eventos institucionais e transmissões realizadas nas dependências da Câmara Municipal. Os quantitativos constituem estimativa técnica para dimensionamento da solução, não representando garantia mínima de utilização contratual.

A estimativa contempla:

- a)** Estações de trabalho administrativas;
- b)** Equipamentos móveis institucionais;
- c)** Dispositivos de visitantes;
- d)** Equipamentos conectados via rede sem fio;
- e)** Túneis VPN simultâneos;
- f)** Serviços hospedados em nuvem e aplicações corporativas institucionais;

A infraestrutura proposta deverá possuir capacidade de escalabilidade horizontal e vertical, permitindo expansão futura sem necessidade de substituição integral.

Além da capacidade de conectividade, a solução deverá suportar adequadamente o tráfego gerado por:

- a)** Sistemas legislativos e administrativos;
- b)** Serviços de arquivos e autenticação;
- c)** Aplicações hospedadas em nuvem;
- d)** Transmissão de sessões legislativas;
- e)** Serviços corporativos, sistemas institucionais e tráfego de dados críticos;
- f)** Inspeção profunda de pacotes, antivírus, IPS, VPN e demais mecanismos de segurança habilitados simultaneamente.

Considerando o crescimento do tráfego de rede, da utilização de sistemas em nuvem, da retenção de logs, dos acessos remotos via VPN, da segmentação de redes e da necessidade de auditoria de eventos de segurança, estima-se aumento progressivo da demanda sobre a solução de firewall e seus recursos de processamento, armazenamento de logs, gerenciamento e inspeção de tráfego.

Dessa forma, a solução deverá permitir expansão progressiva da capacidade operacional, processamento, interfaces, licenciamento, retenção de logs e recursos



de segurança, preservando os requisitos mínimos de desempenho, disponibilidade, segurança e continuidade operacional da Câmara Municipal de Divinópolis.

6.2. Tabela de Quantitativos

Para fins de dimensionamento e composição da contratação, o objeto será constituído por 01 (uma) solução integrada de segurança de borda do tipo Firewall de Próxima Geração – NGFW/UTM, em regime de locação com cessão de uso/comodato, composta pelos elementos tecnológicos discriminados abaixo. Os componentes relacionados não constituem itens autônomos ou passíveis de contratação isolada, mas partes integrantes e interdependentes da solução, observadas as especificações e requisitos estabelecidos neste ETP.

Item da contratação:

Item	Qtda.	Un	Descrição
1	1	Solução	Solução integrada de segurança de borda do tipo Firewall de Próxima Geração – NGFW/UTM, em regime de locação com cessão de uso/comodato, incluindo 01 (um) appliance dedicado, sistema operacional/firmware, licenciamento e subscrições de segurança, conectividade segura, gerenciamento centralizado, documentação e acessos oficiais, garantia, suporte técnico oficial, atualização tecnológica, treinamento e demais componentes necessários ao atendimento integral dos requisitos deste ETP durante toda a vigência contratual.

Composição mínima do item 1 da contratação:

Componente	Qtda.	Unid.	Descrição Detalhada
1.1 – Appliances NGFW	1	Unid.	Appliance dedicado de Firewall de Próxima Geração – NGFW, novo, em linha de produção atual, disponibilizado em regime de locação com cessão de uso/comodato. O equipamento deverá atender integralmente às especificações mínimas de hardware, capacidade e desempenho estabelecidas no item 5.1.5, possuindo capacidade suficiente para suportar toda a demanda prevista da rede institucional, incluindo sistema operacional/firmware nativo ou homologado, kit de instalação em rack e demais componentes e acessórios necessários ao funcionamento da solução. Quando tecnicamente necessários ao adequado funcionamento e proteção do equipamento, deverão igualmente integrar a solução os dispositivos complementares previstos neste ETP, observadas as condições da infraestrutura disponibilizada pela Administração.



Componente	Qtda.	Unid.	Descrição Detalhada
1.2 – Licenciamento/Subscrição de Segurança	1	Conjunto	Licenciamento, subscrição ou disponibilização integral de todos os recursos de segurança necessários ao appliance NGFW durante toda a vigência contratual, com capacidade técnica e de licenciamento para suportar no mínimo 500 dispositivos, abrangendo, quando aplicável à arquitetura ofertada, IPS, antivírus, antimalware, filtragem de conteúdo, controle de aplicações, inspeção de tráfego, análise comportamental, Inteligência Artificial – IA e/ou Machine Learning, inteligência de ameaças e demais funcionalidades de segurança exigidas neste ETP.
1.3 – Conectividade segura/VPN	1	Conjunto	Licenciamento, habilitação ou disponibilização dos recursos necessários à conectividade segura via VPN IPsec, SSL VPN, VPN baseada em TLS/SSL ou tecnologia equivalente, abrangendo a solução durante toda a vigência contratual. Quando tais funcionalidades forem nativas ou já estiverem abrangidas pelo licenciamento principal da plataforma, não será exigido licenciamento específico adicional, desde que permaneçam integralmente disponíveis.
1.4 – Plataforma de gerenciamento centralizado	1	Plataforma	Licenciamento, subscrição ou disponibilização da plataforma de gerenciamento centralizado do appliance NGFW, recurso tecnológico integrante da solução ofertada, disponibilizado em nuvem, ambiente local, híbrido ou tecnologia equivalente, válido durante toda a vigência contratual, permitindo o gerenciamento centralizado do appliance, visualização das informações operacionais, geração de alertas e relatórios, backup automático das configurações com retenção mínima de 5 (cinco) versões válidas, gerenciamento de políticas e acompanhamento dos indicadores de saúde operacional da solução. A presente exigência refere-se à disponibilização da plataforma, funcionalidades, licenciamento e recursos tecnológicos necessários ao gerenciamento da solução, não abrangendo a prestação continuada de administração, análise humana dos eventos, tratamento operacional dos alertas ou execução das ações de sustentação, atividades atribuídas à empresa responsável pela contratação correlata de serviços especializados.



Componente	Qtda.	Unid.	Descrição Detalhada
1.5 – Garantia, suporte oficial e atualização tecnológica	1	Serviço	Disponibilização, durante toda a vigência contratual, da documentação técnica oficial, acesso aos recursos e portais oficiais aplicáveis, imagens e atualizações oficiais de firmware/software, licenças e subscrições, garantia, suporte técnico oficial da solução, atendimento aos níveis de serviço previstos neste ETP, substituição de hardware quando necessária e mecanismos de atualização tecnológica/Hardware Refresh, inclusive nas hipóteses de descontinuidade, perda de suporte ou incapacidade de atendimento aos requisitos contratados.
1.6 – Treinamento e transferência de conhecimento	1	Serviço	Treinamento técnico destinado à equipe de Tecnologia da Informação da Câmara Municipal, com carga horária mínima de 8 (oito) horas, abrangendo as funcionalidades efetivamente contratadas e observando os requisitos estabelecidos no item 5.6.1 deste ETP.

Observação: Os serviços especializados de instalação física, configuração lógica, migração de regras, integração com o ambiente existente, administração, monitoramento, operação assistida e sustentação operacional não integram os quantitativos da presente contratação, por constituírem objeto da contratação correlata específica. O treinamento técnico previsto no componente 1.6 integra esta contratação e não se confunde com a transferência de conhecimento operacional decorrente dos serviços de implantação.

6.3. Memória de Cálculo e Justificativa

6.3.1. Dimensionamento do quantitativo de appliance

A estimativa de 01 (um) appliance NGFW justifica-se pelo dimensionamento técnico da solução, considerando que o equipamento deverá atender, individualmente e de forma integral, aos requisitos mínimos de hardware, capacidade e desempenho estabelecidos neste ETP, bem como suportar toda a demanda prevista do ambiente tecnológico da Câmara Municipal de Divinópolis.

O appliance deverá possuir capacidade suficiente para operar simultaneamente as funcionalidades de firewall, prevenção de intrusões, antivírus/antimalware, controle de aplicações, filtragem de conteúdo, inspeção de tráfego, VPN, gerenciamento inteligente de links e demais mecanismos de segurança exigidos, observados os parâmetros mínimos de desempenho definidos para a contratação.

A continuidade operacional diante de eventual falha do equipamento será tratada por meio dos mecanismos de monitoramento, suporte técnico, garantia,



contingência, substituição de hardware e níveis de serviço estabelecidos nesta contratação, não sendo exigida arquitetura em cluster ou Alta Disponibilidade entre appliances.

6.3.2. Dimensionamento de Usuários

A capacidade de licenciamento e a robustez do appliance foram estimadas com base no inventário atual da infraestrutura tecnológica da Câmara Municipal, considerando capacidade operacional estimada para atendimento simultâneo de aproximadamente 350 dispositivos, bem como a projeção de crescimento institucional, ampliação dos serviços digitais, expansão do uso de dispositivos conectados e necessidades operacionais futuras. A solução deverá possuir, desde sua disponibilização inicial, capacidade técnica e de licenciamento para suportar no mínimo 500 dispositivos, conforme estabelecido no item 5.1.5, de forma a evitar limitações precoces da plataforma e reduzir a necessidade de novos investimentos a curto e médio prazo.

6.3.3. Regime de locação com cessão de uso/comodato

As quantidades acima se referem ao fornecimento em regime de locação, no qual a contratada permanece responsável pela propriedade dos bens disponibilizados, assegurando o pleno funcionamento, suporte e atualização tecnológica contínua da plataforma durante toda a vigência contratual, incluindo substituição proativa do appliance em casos de descontinuidade, obsolescência ou encerramento do suporte pelo fabricante.

6.3.4. Justificativa da Documentação Técnica e Suporte do Fabricante

A disponibilização de documentação técnica oficial, acesso às atualizações, firmwares, licenciamento e suporte técnico oficial da solução mostra-se necessária para assegurar a correta utilização da plataforma, possibilitar a manutenção da garantia, permitir a atualização tecnológica durante toda a vigência contratual e fornecer o apoio técnico necessário à empresa responsável pela implantação, configuração e sustentação operacional da solução, objeto de contratação específica.

7. ESTIMATIVA DO PREÇO DA CONTRATAÇÃO

Com o objetivo de estabelecer um parâmetro inicial para a estimativa do valor da contratação, foram adotados como referência os valores constante no relatório de pesquisa de preços, obtidos por meio da plataforma Banco de Preços, que reúne informações provenientes de contratações realizadas por órgãos e entidades da Administração Pública.



A estimativa apresentada neste tópico possui finalidade específica de estabelecer parâmetro inicial de valor para a solução efetivamente definida neste ETP e não se confunde com as referências preliminares de valores apresentadas no levantamento de mercado do item 4, utilizadas para análise comparativa das alternativas tecnológicas pesquisadas. Conforme registrado naquele levantamento, tais referências podem apresentar diferenças de quantitativo, configuração, escopo e condições de fornecimento em relação à arquitetura definida para a presente contratação.

Considerando os parâmetros técnicos definidos neste Estudo Técnico Preliminar e a média dos valores obtidos nas pesquisas de preços realizadas, estima-se que o valor anual da futura contratação seja de aproximadamente R\$ 70.359,36 (setenta mil trezentos e cinquenta e nove reais e trinta e seis centavos), correspondente à solução composta por 01 (um) appliance NGFW, incluindo os demais componentes, licenciamento, subscrições, garantia, suporte técnico oficial, atualizações tecnológicas e demais recursos exigidos neste ETP.

A pesquisa de preços definitiva deverá ser realizada em momento oportuno da fase preparatória, observando os parâmetros previstos no art. 23 da Lei nº 14.133/2021, de forma a contemplar todos os custos da solução, incluindo o appliance, licenciamento, garantia, atualização tecnológica, suporte técnico oficial da solução e demais componentes previstos nesta contratação.

8. REQUISITOS DA CONTRATAÇÃO

Buscando realizar contratação com fornecedor apto a atender de forma plena às necessidades da Administração, a prestação dos serviços e o fornecimento da solução deverá obedecer aos requisitos abaixo:

8.1. Validação Técnica da Solução

A validação técnica da solução ofertada terá por finalidade verificar o atendimento aos requisitos mínimos estabelecidos neste documento, compatíveis as características da contratação, mediante o que se segue:

8.1.1 Análise Documental

A comprovação do atendimento aos requisitos técnicos ocorrerá, prioritariamente, mediante análise da documentação técnica oficial apresentada pela licitante. Serão aceitos, dentre outros documentos equivalentes, em português do Brasil:

- a) Datasheets oficiais;
- b) Manuais técnicos;



- c) Guias de administração (Administration Guide);
- d) Guias de instalação;
- e) Guias de arquitetura;
- f) Matrizes oficiais de funcionalidades (Feature Matrix);
- g) Notas técnicas;
- h) Release Notes;
- i) White Papers;
- j) Documentação disponibilizada oficialmente pelo fabricante;
- k) Certificações técnicas;
- l) Declarações oficiais emitidas pelo fabricante ou representante autorizado;
- m) Demais documentos técnicos equivalentes que permitam comprovar objetivamente o atendimento aos requisitos deste ETP.

8.1.2. Diligência Técnica

Quando a documentação apresentada não permitir comprovação objetiva de determinado requisito técnico exigido ou houver dúvida quanto ao seu atendimento, a Administração realizará diligência destinada exclusivamente ao esclarecimento da informação. A diligência poderá consistir na apresentação de documentação complementar, esclarecimentos técnicos ou demonstração técnica da ferramenta ofertada.

8.1.3. Demonstração Técnica dos Requisitos

A demonstração técnica dos requisitos será realizada somente quando a análise da documentação apresentada e eventual diligência técnica forem insuficientes para comprovar, de forma objetiva, o atendimento de um ou mais requisitos técnicos previstos neste estudo técnico preliminar, exclusivamente para a verificação dos requisitos ainda não suficientemente comprovados.

Os requisitos que deverão ser demonstrados serão identificados previamente, de forma objetiva, constando a forma de verificação e as evidências esperadas, sendo vedada a inclusão de funcionalidades, condições, testes ou critérios de avaliação não previstos nos documentos da contratação.

A demonstração ficará restrita aos requisitos indicados pela Administração, não sendo necessária a demonstração integral da solução quando a dúvida estiver limitada a funcionalidades ou requisitos específicos, nem a instalação definitiva



dos equipamentos nas dependências da Câmara Municipal ou a reprodução integral de seu ambiente tecnológico.

A Demonstração Técnica poderá ser realizada presencialmente, por videoconferência, mediante compartilhamento de tela, acesso supervisionado a equipamento ou ambiente contendo a solução ofertada, apresentação prática de funcionalidade ou por outro meio tecnicamente adequado, desde que permita à Administração verificar, de maneira objetiva, o atendimento do requisito questionado.

Durante a demonstração, a Administração poderá solicitar a execução das ações estritamente necessárias à comprovação dos requisitos previamente indicados, bem como esclarecimentos técnicos diretamente relacionados à funcionalidade demonstrada, sem ampliação do objeto da avaliação ou criação de requisito não previsto originalmente.

O resultado deverá ser registrado em ata ou relatório, com a identificação dos requisitos avaliados, dos procedimentos realizados, das evidências verificadas e da conclusão quanto ao seu atendimento, observados os critérios objetivos de avaliação.

A realização da demonstração técnica não implicará obrigação de fornecimento definitivo da solução, nem constituirá etapa de implantação, homologação, aceitação definitiva ou operação assistida, destinando-se exclusivamente à comprovação dos requisitos técnicos que motivaram sua realização.

8.1.4. Critério de Avaliação

A avaliação da documentação, da diligência técnica e da eventual demonstração técnica limitar-se-á à verificação do atendimento ou não dos requisitos previamente estabelecidos neste documento. Deste modo, não haverá atribuição de pontuação, classificação técnica, comparação entre fabricantes, preferência tecnológica ou qualquer outro critério de natureza subjetiva.

O resultado da avaliação será registrado, para cada requisito analisado, apenas como: () Atendeu; ou () Não atendeu;

Ao término da avaliação será lavrada ata ou relatório circunstanciado contendo os requisitos avaliados, as evidências observadas, o resultado individual de cada verificação e a respectiva fundamentação técnica.

8.2. Qualificação Técnica, Regularidade da Solução e Certificações



8.2.1. Regularidade da cadeia de fornecimento, licenciamento e suporte oficial

A contratada deverá assegurar que os equipamentos, licenças, subscrições, atualizações, firmwares, garantia e suporte vinculados à solução ofertada sejam provenientes de cadeia legítima de fornecimento e possam ser regularmente registrados, ativados, atualizados e mantidos durante toda a vigência contratual.

Previamente à ativação da solução, a licitante vencedora deverá comprovar possuir meios legítimos e suficientes para assegurar o fornecimento dos equipamentos e o acesso às licenças, subscrições, atualizações, firmwares, garantia, substituição de hardware, quando aplicável, e suporte técnico oficial exigidos na contratação.

A comprovação poderá ser realizada, conforme o modelo comercial e de suporte adotado pelo fabricante ou desenvolvedor, mediante um ou mais dos seguintes meios:

- a)** Declaração de parceria exclusiva ou Certificado de Distribuidor/Parceiro exclusivo;
- b)** Registro ou credenciamento em programa oficial de parceiros, canais, integradores, revendedores, prestadores de serviços ou equivalente;
- c)** Documento emitido pelo fabricante, desenvolvedor, distribuidor oficial ou representante autorizado;
- d)** Consulta a portal, diretório ou sistema oficial do fabricante ou desenvolvedor;
- e)** Documentação de licenciamento, subscrição, garantia, suporte, números de série, direitos de suporte ou instrumentos equivalentes;
- f)** Comprovação de suporte prestado diretamente pelo fabricante ou desenvolvedor; ou
- g)** Outro documento ou mecanismo idôneo e equivalente que demonstre objetivamente a legitimidade do fornecimento e a disponibilidade dos recursos e serviços exigidos.

8.2.2. Capacidade Técnica Operacional

A proponente deverá comprovar experiência anterior compatível com o objeto mediante atestado de capacidade técnica emitidos por pessoa jurídica de direito público ou privado, demonstrando o fornecimento ou disponibilização de solução de segurança de borda do tipo NGFW/UTM ou tecnologia equivalente,



contemplando equipamentos ou appliances, licenciamento ou subscrições, garantia, atualização tecnológica e suporte técnico em ambiente corporativo ou institucional de complexidade compatível.

Serão admitidos atestados relativos a soluções de fabricantes distintos daquele ofertado, desde que comprovem experiência em tecnologias e atividades de natureza e complexidade compatíveis com o objeto, não sendo exigida identidade de marca ou fabricante.

Certificações, credenciamentos ou reconhecimentos emitidos por fabricantes ou desenvolvedores poderão ser apresentados como elementos complementares, não substituindo os atestados de capacidade técnica exigidos para comprovação da capacidade técnico-operacional.

8.2.3. Qualificação Técnica dos Profissionais

Considerando que as atividades de instalação, configuração, migração, administração e operação rotineira da solução não integram o escopo desta contratação específica, a contratada deverá disponibilizar profissional ou profissionais tecnicamente qualificados para prestar suporte relacionado aos equipamentos, firmwares, softwares, licenças, subscrições, atualizações e demais componentes da solução ofertada.

Esses profissionais deverão possuir capacidade para realizar a interlocução técnica necessária, efetuar diagnóstico inicial de falhas relacionadas ao produto e, quando necessário, promover a abertura, acompanhamento e escalonamento de chamados junto ao fabricante, desenvolvedor ou estrutura oficial de suporte, de forma a viabilizar a resolução das ocorrências reportadas pela Administração ou pela empresa responsável pela implantação e administração da solução em contratação correlata.

A qualificação deverá ser comprovada mediante certificação técnica do fabricante ou desenvolvedor da solução, certificação emitida por instituição por ele reconhecida ou comprovação técnica equivalente, compatível com as atividades de suporte exigidas.

Serão admitidas certificações com diferentes denominações, níveis ou estruturas, desde que demonstrem competência compatível com a tecnologia ofertada. Certificações exclusivamente comerciais, de vendas ou de caráter meramente introdutório não serão consideradas, isoladamente, suficientes.

Quando não houver programa formal de certificação individual aplicável à solução, será admitida comprovação equivalente de capacitação técnica, acompanhada de



experiência profissional compatível com as atividades de suporte previstas.

8.2.4. Qualificação do Instrutor e Certificação da Capacitação

O treinamento previsto neste ETP, com carga horária mínima de 08 (oito) horas, deverá ser ministrado por profissional com conhecimento técnico comprovado sobre a solução NGFW ofertada.

A qualificação do instrutor poderá ser comprovada mediante certificação técnica emitida pelo fabricante ou desenvolvedor, por instituição por ele reconhecida ou por comprovação equivalente de capacitação específica na tecnologia, acompanhada, quando aplicável, de experiência compatível com suporte, operação ou capacitação de equipes.

Não será exigida denominação específica de certificação, nível de parceria ou vínculo com centro oficial de treinamento do fabricante, desde que demonstrada a qualificação técnica necessária à realização da capacitação.

Ao término do treinamento, deverão ser fornecidos certificados ou declarações individuais de participação ou conclusão contendo, no mínimo, identificação do participante, solução abordada, conteúdo programático, carga horária, período de realização, entidade responsável e identificação do instrutor.

A capacitação destina-se à transferência de conhecimento operacional e ao nivelamento técnico da equipe da Administração, não se confundindo com curso oficial destinado à obtenção de certificação profissional do fabricante.

8.3. Garantia de Atualização Tecnológica (Hardware Refresh)

A contratada responsável pelo fornecimento da solução deverá garantir a modernização contínua da plataforma sempre que o appliance, sistema operacional, licenciamento ou componente integrante da solução fornecida entrar em processo de descontinuidade, fim de suporte, fim de venda ou fim de vida útil e essa condição comprometer o suporte, a atualização, a segurança, a compatibilidade ou o atendimento aos requisitos contratados, bem como nos casos de incompatibilidade técnica ou incapacidade comprovada de atendimento aos requisitos contratados, sem ônus adicional para a Câmara Municipal de Divinópolis.

Sempre que houver atualização crítica de firmware, software, assinaturas, mecanismos de proteção ou versão recomendada pelo fabricante para correção de vulnerabilidades, estabilidade, compatibilidade ou segurança, a contratada deverá comunicar formalmente a Contratante, disponibilizar os arquivos oficiais, imagens, documentação técnica, notas de versão, recomendações do fabricante e demais



informações necessárias à adequada realização da atualização.

A análise de impacto, planejamento da janela de manutenção, realização de backup prévio, definição de procedimento de rollback, execução da atualização autorizada, validação posterior e atualização da documentação operacional serão realizadas pela empresa responsável pela contratação correlata de serviços especializados de implantação, administração e sustentação do firewall.

O fornecedor da solução deverá prestar, sempre que necessário, o suporte técnico oficial da solução durante o planejamento, execução, diagnóstico ou tratamento de eventuais intercorrências relacionadas à atualização.

Quando a atualização depender necessariamente de intervenção direta do fabricante, desenvolvedor da solução ou parceiro autorizado, a atuação deverá ocorrer de forma coordenada com a empresa responsável pela sustentação operacional e mediante autorização da Administração, observados os procedimentos de segurança, controle de mudanças e janela de manutenções aplicáveis.

O hardware deverá ser entregue em estado de novo, em linha de produção atual, sendo vedada a entrega de equipamentos reconicionados (refurbished).

8.3.1 Conformidade do Produto

Não serão aceitos softwares em versões beta, experimentais ou não oficiais, nem appliances que, na data da entrega, estejam em condição de End-of-Life (EOL – fim do ciclo de vida), End-of-Sale (EOS – fim da comercialização) ou End-of-Support (EOSP – fim do suporte pelo fabricante).

Caso o equipamento venha a atingir alguma dessas condições durante a vigência contratual e isso comprometa seu suporte, atualização, segurança ou continuidade operacional, a contratada deverá substituí-lo, sem ônus adicional para a Administração, por equipamento equivalente ou superior, regularmente suportado pelo fabricante e plenamente compatível com os requisitos deste ETP, mediante prévia aprovação da Administração.

8.4. Suporte Técnico, Continuidade Operacional e Acordos de Nível de Serviço (SLA)

O suporte técnico e as medidas necessárias à continuidade operacional da solução deverão observar a criticidade dos incidentes ou solicitações cuja solução dependa de providência atribuída à contratada responsável pelo fornecimento da solução de firewall, observando os tempos máximos de resposta e restabelecimento definidos na tabela abaixo.



Para os incidentes classificados como Críticos, o atendimento deverá estar disponível em regime 24x7, inclusive aos finais de semana e feriados, com contagem ininterrupta dos respectivos prazos de resposta e restabelecimento. Para as demais criticidades, serão observados os prazos em horas úteis definidos na tabela.

Nos incidentes identificados durante a operação da solução, o diagnóstico e o tratamento operacional inicial poderão ser realizados pela empresa responsável pelos serviços de implantação, administração e sustentação do firewall, objeto de contratação correlata. Quando identificada dependência de garantia, substituição física, correção de falha nativa, firmware, licenciamento, funcionalidade da plataforma ou suporte técnico oficial da solução, o incidente deverá ser escalonado à contratada deste fornecimento.

Os prazos de resposta e restabelecimento previstos neste SLA serão contados a partir da abertura formal do chamado junto à contratada deste fornecimento, realizada pela Contratante ou, quando autorizado pela Administração, pela empresa responsável pelos serviços de sustentação, mediante sistema, e-mail, telefone, portal de atendimento ou outro meio disponibilizado pela contratada.

O protocolo do chamado e os respectivos registros de data e horário deverão ser disponibilizados à Administração, de modo a assegurar a rastreabilidade do atendimento, do escalonamento e da apuração dos níveis de serviço desta contratação.

Quando necessário à solução do incidente, a Administração poderá autorizar ou promover o compartilhamento dessas informações com a empresa responsável pela implantação, administração e sustentação operacional da solução, objeto de contratação correlata.

Criticidade	Descrição	Tempo Máximo de Resposta	Tempo Máximo para Restabelecimento
Crítica	Indisponibilidade total do appliance NGFW ou da solução decorrente de falha de hardware, firmware, licenciamento, subscrição ou funcionalidade nativa da plataforma, bem como comprometimento grave de segurança decorrente de falha nativa da solução.	30 minutos	24 horas corridas
Alta	Degradação severa de desempenho ou falha parcial de serviços essenciais do appliance NGFW ou da solução, decorrente de falha de hardware, firmware, licenciamento, subscrição ou funcionalidade nativa da plataforma, ou comprometimento relevante de segurança atribuível ao produto, sem caracterizar indisponibilidade total.	1 hora	16 horas úteis



Média	Falhas em funcionalidades nativas da plataforma, firmware, relatórios, licenciamento ou subscrições, ou degradação moderada atribuível ao produto sem interrupção total dos serviços.	4 horas	24 horas úteis
Baixa	Solicitações administrativas relacionadas a licenciamento, subscrições, garantia ou suporte oficial, dúvidas técnicas sobre funcionalidades nativas ou demandas vinculadas ao produto sem impacto significativo na continuidade operacional.	8 horas	48 horas úteis

Os tempos previstos acima referem-se ao restabelecimento da operação da solução quanto às ocorrências atribuíveis a este fornecimento, podendo o restabelecimento ocorrer por meio de contingência, disponibilização de equipamento substituto de capacidade igual ou superior, correção remota ou outra solução técnica equivalente que restabeleça integralmente as funcionalidades necessárias à operação, sem prejuízo da posterior substituição definitiva do equipamento, quando necessária.

Os prazos de restabelecimento poderão ser suspensos temporariamente quando a execução da correção depender exclusivamente de ação, validação, autorização ou disponibilidade técnica da Contratante, de terceiros responsáveis por infraestrutura externa ou de indisponibilidade comprovada de serviços externos não gerenciados pela contratada.

As manutenções programadas previamente alinhadas entre as partes não serão consideradas indisponibilidade para fins de apuração de SLA.

8.4.1. Substituição de Hardware e Continuidade Operacional

Quando necessária a substituição física definitiva do appliance NGFW, esta deverá ocorrer no prazo máximo de 2 (dois) dias úteis, por equipamento de capacidade igual ou superior, sem prejuízo da obrigação de adoção, pela contratada, das medidas de contingência necessárias ao cumprimento dos tempos máximos de restabelecimento previstos no SLA deste item, inclusive mediante disponibilização de equipamento substituto temporário, quando necessária para o restabelecimento da operação.

8.4.2. Acesso Direto

O suporte deverá possibilitar escalonamento e atendimento por profissionais especializados, pertencentes ao fabricante, desenvolvedor da solução, parceiro autorizado ou equipe técnica formalmente habilitada para a tecnologia ofertada, sempre que necessário à resolução de incidentes críticos ou complexos.

O escalonamento poderá ser solicitado diretamente pela Administração ou, mediante autorização desta, pela empresa responsável pelos serviços de



implantação, administração e sustentação operacional do firewall, devendo a contratada deste fornecimento disponibilizar os canais, credenciais, contatos e demais meios necessários à abertura e ao acompanhamento dos chamados.

8.5. Obrigações do Fornecedor para a Implantação da Solução

A contratada responsável pelo fornecimento da solução deverá disponibilizar as imagens de firmware, arquivos de licenciamento, acesso aos portais do fabricante, informações e orientações técnicas, bem como o suporte necessário ao processo de implantação, para a correta instalação da solução.

A implantação física, configuração lógica, migração de regras, integração com os ambientes existentes, criação de políticas de segurança, testes, homologação, operação assistida e demais serviços técnicos especializados serão executados por empresa contratada especificamente para prestação desses serviços, cabendo ao fornecedor da solução prestar o apoio técnico oficial da solução necessário quando demandado.

8.6. Entrega e Disponibilização da Solução

A contratada responsável pelo fornecimento deverá entregar os equipamentos, licenças, subscrições, documentação técnica, acessórios e demais componentes integrantes da solução nos prazos estabelecidos contratualmente, em condições de instalação, ativação e licenciamento.

A instalação física do appliance será executada pela empresa responsável pelos serviços especializados de implantação, administração e sustentação operacional da solução, objeto de contratação correlata, observados o respectivo cronograma e as especificações técnicas do fabricante.

A atuação conjunta entre as contratadas não implicará transferência de responsabilidades. A empresa responsável pelos serviços permanecerá responsável pelas atividades de instalação, configuração, integração e demais intervenções realizadas no ambiente, enquanto a contratada deste fornecimento permanecerá responsável pelos equipamentos, licenças, subscrições, garantia, atualizações, suporte oficial e demais componentes integrantes da solução fornecida.

Na elaboração de sua proposta, a licitante responsável pelo fornecimento deverá considerar, quando tecnicamente necessário segundo as especificações do fabricante e as condições da infraestrutura elétrica previamente informadas pela Administração, os dispositivos complementares de proteção elétrica indispensáveis à adequada utilização e preservação dos equipamentos.



Caso sejam necessários nobreak, dispositivo de proteção contra surtos ou equipamento equivalente que não integre a infraestrutura disponibilizada pela Câmara Municipal, essa necessidade deverá ser identificada pela licitante e o respectivo equipamento deverá integrar sua proposta, sem custos adicionais posteriores à Contratante.

Os dispositivos complementares fornecidos como parte da solução serão entregues juntamente com os appliances. Sua instalação física e conexão ao ambiente serão realizadas pela empresa responsável pela implantação, observadas as especificações do fabricante, as orientações técnicas da contratada fornecedora e as condições da infraestrutura disponibilizada pela Administração.

A Câmara Municipal irá disponibilizar infraestrutura elétrica e física compatível com as condições previamente informadas para implantação da solução.

A responsabilidade por eventual falha, dano ou indisponibilidade será apurada conforme sua causa, observando-se as obrigações atribuídas a cada contratação, as condições da infraestrutura disponibilizada e as especificações do fabricante, cabendo, conforme o caso:

- a) À contratada responsável pelos serviços, quando decorrente de instalação, conexão, configuração ou intervenção executada de forma inadequada;
- b) À contratada responsável pelo fornecimento, quando decorrente de defeito, vício, incompatibilidade ou inadequação de equipamento ou componente integrante da solução fornecida, inclusive dos dispositivos complementares por ela disponibilizados; e
- c) À Administração, quando comprovadamente decorrente de condição da infraestrutura sob sua responsabilidade que esteja em desacordo com as condições previamente informadas ou com os requisitos técnicos devidamente comunicados para implantação da solução.

8.7. Logística Reversa

Ao término da vigência contratual, em caso de não renovação, substituição da solução ou encerramento do contrato, a contratada deverá providenciar a retirada do appliance e demais equipamentos por ela fornecidos no prazo máximo de 15 (quinze) dias úteis, responsabilizando-se, quando aplicável, por sua destinação ambientalmente adequada e pela sanitização segura dos dados eventualmente armazenados nos equipamentos antes de sua retirada.



9. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

A solução proposta consiste na modernização da camada de segurança perimetral da Câmara Municipal de Divinópolis através da implementação de uma arquitetura integrada de segurança NGFW, operando sob o modelo de locação com cessão de uso/comodato do equipamento, com subscrição/licenciamento durante toda a vigência contratual.

A plataforma compreende uma solução integrada de proteção, composta pelo appliance NGFW, seus recursos de segurança, licenciamento, gerenciamento, monitoramento, suporte técnico, atualização tecnológica e demais componentes previstos neste ETP, estruturada nos seguintes pilares:

9.1. Arquitetura e Dimensionamento da Solução NGFW

A solução será composta por 01 (um) appliance dedicado de Firewall de Próxima Geração – NGFW, dimensionado para atender, individualmente e de forma integral, aos requisitos mínimos de hardware, capacidade e desempenho estabelecidos neste ETP, bem como suportar toda a demanda prevista do ambiente tecnológico da Câmara Municipal de Divinópolis.

O appliance deverá suportar a operação simultânea das funcionalidades de segurança, inspeção de tráfego, conectividade segura, VPN, gerenciamento inteligente de links e demais recursos exigidos para a solução, observados os parâmetros mínimos de desempenho estabelecidos neste ETP.

A continuidade operacional diante de eventual falha do equipamento será tratada por meio dos mecanismos de monitoramento, suporte técnico, garantia, contingência, substituição de hardware e níveis de serviço previstos nesta contratação.

9.2. Inteligência de Segurança e Análise Comportamental

A infraestrutura de segurança deverá possuir recursos avançados de inspeção profunda de pacotes, análise comportamental, inteligência artificial (IA) e/ou Machine Learning, correlação automatizada de eventos e mecanismos de detecção de ameaças compatíveis com o estado da arte da segurança cibernética, permitindo identificar atividades suspeitas, tentativas de exploração, ransomwares e outras ameaças cibernéticas modernas.

9.3. Conectividade Inteligente e SD-WAN

A solução atuará como elemento central de gerenciamento das comunicações da Casa, gerenciando de forma inteligente os links de internet. Através da tecnologia SD-WAN, a solução monitora constantemente a qualidade das conexões (latência e



perda de pacotes), direcionando o tráfego crítico para o melhor link disponível e reduzindo o risco de paralisação dos serviços quando houver enlace alternativo disponível.

9.4. Gestão Unificada e Soberania de Dados

Todo o ecossistema de segurança será gerenciado por meio de painel centralizado, em nuvem, local, híbrido ou solução equivalente, permitindo à equipe de TI monitorar ameaças, usuários, aplicações, VPNs, links de internet, políticas de segurança, alertas e relatórios gerenciais. O ambiente prioriza a conformidade com a LGPD, mantendo trilhas de auditoria e logs detalhados de todas as conexões, assegurando a rastreabilidade necessária à segurança da informação, à auditoria e à governança institucional.

9.5. Sustentabilidade Tecnológica (Hardware Refresh)

A plataforma de segurança como um todo é amparada por um modelo de contratação que transfere o risco de obsolescência ao fornecedor. Isso significa que a Câmara terá a garantia de que, durante toda a vigência contratual, os equipamentos estarão atualizados, contando com suporte técnico oficial da solução e substituição proativa de hardware em caso de descontinuidade de modelos (End-of-Life).

9.6. Conclusão da Solução

Em suma, a infraestrutura de segurança abandona o modelo de gestão manual e reativa para um modelo de segurança integrada, atualizada e resiliente. A integração entre hardware dedicado, licenciamento atualizado, inteligência de segurança, gerenciamento centralizado e suporte técnico oficial da solução resultará em infraestrutura mais resiliente, escalável e adequada ao cenário atual de ameaças cibernéticas, protegendo o patrimônio digital da Câmara Municipal de Divinópolis e preservando maior continuidade aos serviços legislativos.

10. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

A presente contratação refere-se a uma solução integrada de segurança composta por hardware, sistema operacional, licenciamento, subscrições de segurança, suporte técnico oficial da solução, atualização tecnológica e disponibilização dos recursos e da plataforma de gerenciamento centralizado, os quais operam de forma interdependente e tecnicamente vinculada.

Dessa forma, a eventual fragmentação desses componentes poderia comprometer a coerência técnica da solução, a uniformidade das versões de software e firmware, a



compatibilidade entre hardware e licenciamento, bem como a adequada integração entre os elementos necessários ao pleno funcionamento da plataforma de segurança.

A presente justificativa de não parcelamento refere-se exclusivamente aos componentes tecnológicos integrantes da solução de firewall e não abrange os serviços especializados de implantação física e lógica, configuração, migração, administração, monitoramento, operação assistida e sustentação operacional, os quais constituem contratação correlata específica.

10.1. Interdependência Técnica da solução

A solução de Firewall de Próxima Geração (NGFW) é composta por ecossistema integrado no qual hardware, sistema operacional, licenciamento, subscrições de segurança, atualizações, suporte oficial e recursos tecnológicos de gerenciamento centralizado devem operar de forma plenamente compatível e homologada.

Desse modo, o parcelamento desses componentes tecnológicos — como a contratação separada do appliance, licenciamento, subscrições, suporte oficial ou plataforma de gerenciamento vinculada à solução — poderia gerar incompatibilidades, perda de desempenho, conflito de responsabilidades e comprometimento da segurança e da continuidade operacional.

A administração, configuração, monitoramento, análise humana de eventos e sustentação operacional da solução não integram a presente justificativa de não parcelamento, por constituírem objeto da contratação correlata de serviços especializados.

10.2. Gestão unificada e responsabilização contratual

A contratação de solução integrada assegura a centralização da responsabilidade técnica pelo fornecimento, licenciamento e gestão da continuidade tecnológica em um único fornecedor, permitindo maior eficiência na gestão contratual e na resolução de incidentes. O parcelamento geraria o risco de conflito de responsabilidades entre fornecedores, onde o fornecedor do software poderia atribuir a falha ao hardware e vice-versa, comprometendo os níveis mínimos de serviço estabelecidos neste ETP.

10.3. Prejuízo ao conjunto do objeto em caso de parcelamento

Conforme jurisprudência do Tribunal de Contas da União (TCU) e as diretrizes da Lei 14.133/2021, o parcelamento deve ser evitado quando houver prejuízo para o conjunto da solução ou perda de economia de escala. No caso em tela, a separação dos componentes comprometeria a integridade da solução de segurança, uma vez que a eficácia do Firewall depende da renovação contínua e integrada das licenças



de inteligência de ameaças, atualizações, manutenção do suporte aos serviços de segurança vinculados à solução ofertada.

Assim, resta claro que o parcelamento do objeto mostra-se tecnicamente inviável diante da interdependência entre os diversos componentes que integram a solução proposta. Portanto, para garantir a integridade técnica, a celeridade no suporte e a máxima eficiência da segurança perimetral, justifica-se a não divisão do objeto, sendo a contratação realizada de maneira unificada.

11. DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS

A modernização da infraestrutura de segurança perimetral, aliada à transição para o modelo de locação com cessão de uso/comodato, visa transformar a segurança de rede de um centro de custo passivo para uma infraestrutura de segurança mais resiliente, atualizada e com mecanismos de continuidade operacional. Os resultados esperados são:

11.1. Resiliência Operacional e Disponibilidade Crítica

11.1.1. Resultado Técnico

Disponibilização de 01 (um) appliance NGFW dimensionado para atender, individualmente e de forma integral, à demanda do ambiente tecnológico da Câmara Municipal de Divinópolis, com capacidade para suportar simultaneamente as funcionalidades de segurança, conectividade, inspeção de tráfego, VPN, gerenciamento de links e demais recursos previstos neste ETP.

11.1.2. Impacto na Modalidade de Locação

A modalidade de locação com cessão de uso/comodato permitirá à Câmara dispor de equipamento permanentemente coberto por garantia, suporte técnico oficial, atualização tecnológica e mecanismos de substituição previstos contratualmente, reduzindo os riscos associados à obsolescência, indisponibilidade prolongada e necessidade de aquisição emergencial de equipamento substituto.

Em caso de falha do appliance, a continuidade operacional será tratada pelos mecanismos de monitoramento, suporte técnico, contingência, substituição de hardware e níveis de serviço definidos nesta contratação, com o objetivo de reduzir o período de indisponibilidade dos serviços institucionais.

11.2. Defesa Proativa e Mitigação de Ameaças de "Dia Zero"

11.2.1. Resultado Técnico

Ampliação da capacidade de detecção de ameaças por meio de mecanismos de



análise comportamental, correlação de eventos e identificação de atividades suspeitas compatíveis com ataques cibernéticos modernos.

11.2.2. Eficácia

Ampliação da capacidade de detecção de ransomwares e malwares em tempo real antes da efetiva exfiltração de dados. A inspeção de tráfego criptografado (SSL/TLS), quando tecnicamente aplicável e observadas as disposições legais e de privacidade pertinentes, ampliará a capacidade de identificação de comportamentos suspeitos e comunicações potencialmente maliciosas, fortalecendo os mecanismos de detecção, resposta e mitigação de ameaças cibernéticas modernas.

11.3. Otimização de Infraestrutura via SD-WAN e Visibilidade L7

11.3.1. Ganho Operacional

Gerenciamento inteligente de links e controle granular de aplicações (Camada 7).

11.3.2. Benefício Operacional

O sistema deverá priorizar automaticamente o tráfego institucional e sistemas críticos, aplicando Quality of Service (QoS) para evitar gargalos causados por aplicações não prioritárias. O resultado é uma experiência de navegação superior e aproveitamento máximo da banda de internet contratada.

11.4. Preservação do Ciclo de Atualização (Hardware Refresh)

11.4.1. Resultado da Modalidade de Locação

Redução dos riscos de obsolescência e defasagem tecnológica da infraestrutura de segurança, por meio de atualização contínua de firmware, licenciamento, mecanismos de proteção, suporte técnico oficial da solução e possibilidade de evolução da plataforma durante a vigência contratual.

11.4.2. Justificativa Técnica

Em modelos de aquisição direta, o hardware permanece sob responsabilidade patrimonial da Administração durante todo o seu ciclo de vida e poderá tornar-se tecnologicamente insuficiente antes mesmo da ocorrência de falha física, em razão da evolução do volume de tráfego, das exigências de processamento, da inspeção de conexões criptografadas, da conectividade e dos mecanismos de segurança.

A obsolescência tecnológica, portanto, não está necessariamente vinculada a um



período fixo de utilização, podendo decorrer de descontinuidade do produto, perda de suporte, incompatibilidade com novas versões, indisponibilidade de atualizações ou insuficiência de capacidade para atendimento das necessidades institucionais.

Na modalidade de locação com cessão de uso/comodato, o resultado pretendido é assegurar atualização tecnológica contínua da solução sempre que houver descontinuidade, perda de suporte, incompatibilidade técnica ou comprometimento da capacidade operacional necessária ao ambiente da Câmara Municipal de Divinópolis.

Dessa forma, enquanto no modelo de aquisição eventual insuficiência ou obsolescência do equipamento poderá demandar novo investimento da Administração para ampliação ou substituição do ativo, no modelo de locação com cessão de uso/comodato a responsabilidade pela evolução da plataforma, nas hipóteses estabelecidas contratualmente, permanece atribuída à contratada, reduzindo a exposição da Administração ao risco de manter equipamento ainda funcional, porém tecnologicamente inadequado às necessidades da solução.

11.5. Governança de Dados e Conformidade com a LGPD

11.5.1. Efeito esperado

Centralização de logs e trilhas de auditoria correlacionadas com serviços de diretório compatíveis com Active Directory (AD), LDAP ou equivalentes.

11.5.2. Impacto Legal

A centralização de logs e trilhas de auditoria deverá contribuir para a rastreabilidade, o registro e a análise das atividades relacionadas aos acessos e eventos de segurança. O resultado esperado é disponibilizar à Administração informações e mecanismos que auxiliem na elaboração de relatórios técnicos, nas atividades de auditoria, fiscalização e apuração de incidentes de segurança da informação, contribuindo para o atendimento dos princípios e obrigações aplicáveis da Lei Geral de Proteção de Dados – LGPD e das exigências dos órgãos de controle, quando pertinentes.

Os recursos deverão permitir, quando tecnicamente aplicável, a identificação de usuários ou responsáveis, horários, origens dos acessos e ações executadas no ambiente, de modo a ampliar a rastreabilidade e a capacidade de investigação de eventos de segurança.

11.6. Eficiência Financeira, Continuidade Operacional e Suporte Técnico



11.6.1. Resultado da Modalidade de Locação

A contratação da solução em regime de locação com cessão de uso/comodato permitirá à Câmara Municipal de Divinópolis reduzir a necessidade de investimentos iniciais elevados na aquisição de equipamentos e os riscos relacionados à obsolescência tecnológica, adotando modelo contratual que contempla a disponibilização do appliance dedicado, licenças e subscrições durante toda a vigência contratual, garantia, suporte técnico oficial da solução, atualizações de firmware e software, bem como substituição de hardware e atualização tecnológica quando previstas ou necessárias nos termos da contratação.

O modelo proporcionará maior previsibilidade orçamentária, continuidade tecnológica da solução, simplificação da gestão do ativo e redução dos riscos associados à indisponibilidade, descontinuidade de suporte e obsolescência do equipamento de segurança, sem abranger as atividades de instalação lógica, configuração, administração e operação rotineira da solução, que serão objeto de contratação correlata.

11.6.2. Resultado Operacional

A solução deverá proporcionar mecanismos destinados à resiliência e à continuidade operacional, mediante monitoramento da saúde operacional, mecanismos de contingência, suporte técnico especializado, garantia, substituição de hardware e demais funcionalidades previstas neste ETP, compatíveis com a criticidade da infraestrutura tecnológica da Câmara Municipal de Divinópolis.

11.6.3. Suporte e Continuidade

O resultado pretendido é a redução dos períodos de indisponibilidade dos serviços de rede e segurança, mediante atuação integrada dos mecanismos de monitoramento, alerta e contingência disponibilizados pela solução, do suporte técnico oficial, da garantia e substituição de hardware quando necessária, bem como dos serviços de administração, monitoramento e sustentação operacional executados no âmbito da contratação correlata.

As ocorrências atribuíveis ao fornecimento da solução deverão ser tratadas conforme os Acordos de Nível de Serviço (SLA) estabelecidos no item 8.4 deste ETP, enquanto as atividades de diagnóstico, administração, monitoramento e sustentação operacional observarão as responsabilidades e os níveis de serviço definidos na respectiva contratação correlata.

11.7. Melhoria no Atendimento das Demandas pela Equipe Interna de TI



11.7.1. Resultado Técnico

Automação de processos via painel centralizado de gerenciamento da solução.

11.7.2. Ganho de Produtividade

Com ferramentas de diagnóstico rápido, gestão centralizada e monitoramento proativo, a equipe de TI amplia sua capacidade de fiscalização, acompanhamento e governança da solução, concentrando esforços na análise estratégica de segurança da informação. A solução poderá disponibilizar alertas por aplicativo móvel, painel web, e-mail ou mecanismos equivalentes, quando suportados pela plataforma ofertada.

Diferentemente da solução atualmente utilizada pelo Órgão, baseada em servidores próprios, a nova modalidade permite que a Câmara Municipal utilize os appliances e a plataforma de segurança durante a vigência contratual sem incorporar definitivamente os equipamentos ao seu patrimônio, transferindo ao fornecedor os riscos relacionados à propriedade, defeitos dos componentes, garantia, obsolescência tecnológica, indisponibilidade de peças e demais hipóteses de substituição previstas contratualmente.

O modelo busca reduzir os riscos de descontinuidade decorrentes de falhas de hardware, indisponibilidade de peças, obsolescência e perda de suporte tecnológico, sem prejuízo das responsabilidades da empresa encarregada da sustentação operacional e da Administração.

12. PROVIDÊNCIAS PRÉVIAS AO CONTRATO

A presente contratação deverá ser precedida de processo licitatório, em observância à Lei nº. 14.133/2021.

Buscando um adequado planejamento e mitigação de riscos operacionais, a Câmara Municipal, antes da implementação da nova solução, deverá providenciar um levantamento das regras atuais de firewall, NAT, VPN e segmentação de rede, identificação dos links de internet ativos, preparação do ambiente físico, elétrico e lógico para instalação dos novos appliances.

13. CONTRATAÇÕES CORRELATAS / INTERDEPENDENTES

A eficácia da segurança cibernética da Câmara Municipal de Divinópolis depende de um conjunto de componentes técnicos e operacionais interdependentes. A falha ou ausência de qualquer desses elementos pode comprometer a integridade, a disponibilidade e a efetividade da solução pretendida.



13.1. Interdependência entre Solução de Borda (NGFW) e Gestão Especializada

Existe relação técnica direta e interdependente entre o fornecimento da solução em regime de locação com cessão de uso/comodato, compreendendo os appliances dedicados, a subscrição/licenciamento, o suporte técnico oficial da solução e a atualização tecnológica contínua, e a contratação correlata de serviços especializados de implantação, administração e sustentação operacional da solução. O fornecimento da solução constitui requisito técnico para execução dos serviços especializados, tratando-se de contratações distintas, porém tecnicamente interdependentes.

Os serviços especializados de implantação física, configuração lógica, migração de regras, integração com os ambientes existentes, operação assistida e sustentação operacional constituem contratação correlata e tecnicamente vinculada à solução fornecida, porém serão objeto de processo específico. Essa separação administrativa não caracteriza parcelamento indevido da solução de firewall, uma vez que o fornecimento do appliance, do licenciamento, das atualizações e do suporte técnico permanecerá integrado em um único objeto, enquanto os serviços especializados serão executados de forma coordenada e compatível com a plataforma contratada.

13.1.1. Operação Especializada

O hardware compatível com os requisitos tecnológicos atuais (NGFW) exige configuração de políticas complexas (mecanismos de proteção contra ransomware, IPS e Inspeção SSL) que demandam conhecimento técnico especializado compatível com a solução ofertada. A eficácia do hardware é diretamente proporcional à qualidade da gestão técnica contratada.

13.1.2. SLA e Resiliência

Enquanto o contrato de locação visa assegurar a disponibilidade física do equipamento, o serviço de sustentação garante a disponibilidade lógica. A sinergia entre ambos assegura que a Câmara não sofra indisponibilidade significativa dos serviços digitais, mantendo o Processo Legislativo Eletrônico e o Portal da Transparência operacionais através de uma administração proativa.

13.2. Correlação com a Infraestrutura de TI e Conectividade

A solução de firewall depende da infraestrutura física da Casa para sua plena performance:

13.2.1. Ambiente Físico

A operação do firewall em regime 24x7 depende da estabilidade elétrica e



refrigeração providas pelo ambiente de infraestrutura tecnológica da Câmara.

13.2.2. Conectividade de Alta Performance

O suporte ao tráfego atual e projetado, bem como o gerenciamento de links via SD-WAN, dependem da compatibilidade com os ativos de rede, switches, cabeamento, links de internet e demais componentes do ambiente de TI.

13.3. Integração com Serviços em Nuvem (Cloud Computing)

O firewall e sua respectiva gestão técnica são os garantidores para os sistemas institucionais hospedados em nuvem:

13.3.1. Túneis VPN e Segurança

A sustentação técnica será responsável por manter a integridade dos túneis de comunicação segura, permitindo que o trabalho remoto e o tráfego de dados para a nuvem ocorram sob criptografia rigorosa, atendendo aos preceitos da LGPD.

13.4. Da Compatibilidade Técnica entre as Contratações Correlatas

13.4.1. Considerando a diversidade de soluções de Firewall NGFW disponíveis no mercado, a contratação correlata responsável pelos serviços de implantação, configuração, administração, monitoramento e sustentação operacional deverá observar as características técnicas da solução de hardware, software, firmware e licenciamento efetivamente disponibilizada no âmbito desta contratação.

Essa compatibilidade técnica visa assegurar que os serviços executados sobre a solução permitam a adequada utilização de seus recursos e funcionalidades, preservando a disponibilidade, a segurança e a continuidade operacional da infraestrutura institucional.

O suporte oficial relacionado aos equipamentos, firmwares, softwares, licenças, subscrições, garantia e demais componentes fornecidos permanecerá sob responsabilidade da contratada desta solução, inclusive quanto à interlocução e ao escalonamento de ocorrências ao fabricante, desenvolvedor ou estrutura oficial de suporte, quando necessário.

13.4.2. A correlação técnica entre as contratações não implica identidade de fornecedores ou transferência de responsabilidades entre as respectivas contratadas, permanecendo cada empresa responsável pelas obrigações previstas no respectivo instrumento contratual, devendo ambas colaborar tecnicamente quando necessário à identificação e solução de ocorrências que envolvam a interação entre produto e serviços.



A coordenação entre estas contratações correlatas é essencial. A ausência dos serviços especializados de implantação, administração e sustentação operacional tornaria o hardware subutilizado e vulnerável; por outro lado, esses serviços especializados, sem o hardware adequado, seriam inócuos. Portanto, a execução coordenada dessas contratações é o que garantirá a elevação do nível de resiliência digital da Câmara Municipal de Divinópolis.

14. IMPACTOS AMBIENTAIS E SUSTENTABILIDADE

Considerando que o objeto da presente contratação contempla o fornecimento de equipamentos eletrônicos e serviços de suporte técnico, reconhece-se a existência de potenciais impactos ambientais decorrentes, principalmente, da geração de resíduos eletroeletrônicos e do consumo de energia elétrica associado à operação da solução.

Nesse contexto, visando minimizar os impactos ambientais decorrentes da contratação, deverão ser observadas práticas voltadas à sustentabilidade, à eficiência energética e à destinação ambientalmente adequada dos equipamentos e componentes eventualmente substituídos ou tornados inservíveis.

A contratada deverá promover a destinação final ambientalmente adequada dos resíduos eletroeletrônicos gerados durante a execução contratual, observando a legislação ambiental vigente, em especial a Política Nacional de Resíduos Sólidos, Lei nº 12.305/2010, bem como priorizando, quando aplicável, a reutilização ou reciclagem dos materiais.

Para esta contratação, busca-se solução tecnológica que apresente maior eficiência energética e menor consumo de energia elétrica, contribuindo para a redução do impacto ambiental e para a racionalização do consumo de recursos públicos.

A adoção de appliances de segurança dedicados, desenvolvidos especificamente para a execução das funções de proteção de rede, tende a apresentar maior eficiência operacional e energética quando comparada a arquiteturas baseadas em servidores de uso geral, que normalmente demandam maior consumo de energia e maior quantidade de componentes físicos.

Sempre que possível, deverão ser priorizados equipamentos, componentes e processos que observem os princípios da economia circular, favorecendo a ampliação da vida útil dos ativos, a redução da geração de resíduos e a utilização de tecnologias que representem menor impacto ambiental ao longo de todo o ciclo de vida da solução.

Dessa forma, espera-se que os impactos ambientais decorrentes desta contratação sejam reduzidos e passíveis de mitigação, sendo a solução pretendida compatível com os princípios da sustentabilidade, da eficiência e do desenvolvimento nacional



sustentável previstos na Lei nº 14.133/2021.

15. VIABILIDADE DA CONTRATAÇÃO

A análise de viabilidade desta contratação demonstra que o modelo de locação com cessão de uso/comodato apresenta maior aderência às necessidades técnicas, operacionais e de gestão de riscos tecnológicos da Câmara Municipal de Divinópolis, fundamentada nos seguintes pilares:

15.1. Viabilidade Técnica e Operacional

A substituição dos atuais servidores por appliances NGFW integrados (hardware, sistema operacional e licenciamento) reduz a complexidade decorrente da integração e manutenção de componentes tecnológicos distintos e mitiga riscos de incompatibilidade entre os elementos integrantes da plataforma. A solução de locação com cessão de uso/comodato proporciona:

15.1.1. Disponibilidade Contínua

A continuidade operacional da solução será apoiada por mecanismos de monitoramento, suporte técnico especializado, garantia, contingência, substituição de hardware e níveis de serviço estabelecidos nesta contratação, com o objetivo de reduzir os riscos e os períodos de indisponibilidade dos serviços institucionais.

A solução será dimensionada para que o appliance NGFW atenda integralmente à demanda prevista da infraestrutura tecnológica da Câmara Municipal de Divinópolis, permanecendo a contratada responsável pela adoção das medidas necessárias ao restabelecimento da operação quando ocorrer falha atribuível ao equipamento ou aos demais componentes integrantes do fornecimento.

15.1.2. Suporte Especializado e Divisão de Responsabilidades

O modelo proposto estabelece divisão objetiva de responsabilidades entre as contratações correlatas, atribuindo à contratada deste fornecimento as obrigações relacionadas aos equipamentos, garantia, substituição física, licenciamento, subscrições, atualizações e acesso ao suporte técnico oficial da solução.

As atividades de instalação, configuração, administração, monitoramento, diagnóstico operacional e sustentação permanecerão sob responsabilidade da empresa contratada especificamente para a prestação dos serviços especializados correlatos.

Quando uma ocorrência depender de garantia, substituição de equipamento, correção de firmware ou software, licenciamento, atualização ou atuação da estrutura oficial de suporte da solução, caberá à contratada deste fornecimento



promover o atendimento e o respectivo escalonamento, quando necessário.

Essa separação de atribuições reduz sobreposições, facilita a identificação das responsabilidades, preserva a especialização de cada contratação e contribui para a continuidade operacional da solução, demonstrando a viabilidade técnica e operacional do modelo adotado.

15.2. Viabilidade Econômica (Eficiência do Gasto Público)

A modalidade de locação com cessão de uso/comodato apresenta características favoráveis à previsibilidade do gasto, à continuidade tecnológica e à gestão dos riscos econômicos associados ao ciclo de vida da solução, conforme os seguintes aspectos:

15.2.1. Proteção contra Obsolescência

Os equipamentos de segurança estão sujeitos à evolução tecnológica, descontinuidade, perda de suporte, incompatibilidade e eventual insuficiência de capacidade ao longo de seu ciclo de utilização. No modelo de locação com cessão de uso/comodato, os mecanismos de Hardware Refresh previstos nesta contratação transferem à contratada, nas hipóteses contratualmente estabelecidas, a responsabilidade pela atualização ou substituição da plataforma, sem necessidade de nova aquisição de equipamentos pela Administração.

15.2.2. Previsibilidade Orçamentária

O pagamento periódico da contratação em regime de locação com cessão de uso/comodato (OPEX) evita elevados desembolsos iniciais de capital (CAPEX), proporciona maior previsibilidade orçamentária e incorpora ao modelo contratual, nos limites do escopo contratado, os custos relacionados à substituição de hardware, garantia, suporte e continuidade das subscrições, reduzindo a exposição da Administração a despesas extraordinárias relacionadas a esses componentes.

15.3. Conformidade e Segurança Jurídica

A contratação mostra-se compatível com as diretrizes e princípios aplicáveis da Lei nº 14.133/2021 e contempla recursos de segurança, registro, rastreabilidade e auditoria que contribuem para o atendimento dos princípios e obrigações aplicáveis da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD), bem como para as atividades de governança, fiscalização e controle da Administração.

A disponibilização desses recursos deverá contribuir para a proteção de dados pessoais e informações institucionais, para a rastreabilidade de eventos e para a apuração de incidentes de segurança, sem prejuízo das demais medidas



administrativas, técnicas, organizacionais e jurídicas necessárias à conformidade institucional.

Considerando a viabilidade dos mecanismos previstos para mitigação dos riscos de implementação, a ampliação do nível de segurança cibernética, a integração dos componentes da solução, a continuidade operacional, a atualização tecnológica e a transferência de parte relevante dos riscos associados ao ciclo de vida dos equipamentos, este Estudo Técnico Preliminar conclui pela viabilidade técnica, operacional e jurídica da contratação da solução de firewall na modalidade de locação com cessão de uso/comodato.

Sob o aspecto econômico, o modelo apresenta características favoráveis à redução do investimento inicial, à previsibilidade dos gastos e à gestão dos riscos relacionados à obsolescência e substituição tecnológica, devendo a vantajosidade econômica definitiva ser confirmada pela pesquisa de preços e pela avaliação do custo global da solução, conforme estabelecido neste ETP.

Nesse contexto, o modelo proposto apresenta maior aderência ao conjunto das necessidades técnicas, operacionais, de continuidade e de gestão de riscos tecnológicos identificadas para a Câmara Municipal de Divinópolis.

16. DISPOSIÇÕES GERAIS

Integram este Estudo Técnico Preliminar, para todos os fins e efeitos, sem prejuízo de outros documentos técnicos produzidos durante a fase preparatória, os seguintes anexos:

- Anexo I - Mapa de Gerenciamento de Riscos;
- Anexo II – Relatório de pesquisa de preços.

Divinópolis, 06 de outubro de 2026.

Alexsandro Alves Vasconcelos

Analista Legislativo Tecnologia da Informação



DOCUMENTO DE ANÁLISE DE RISCOS

Objeto:

Contratação de solução integrada de segurança de rede do tipo Firewall de Próxima Geração – NGFW/UTM, em regime de locação com cessão de uso/comodato, compreendendo o fornecimento de 01 (um) appliance dedicado, licenciamentos e subscrições durante toda a vigência contratual, suporte técnico oficial da solução, garantia, atualização tecnológica, gerenciamento centralizado e treinamento técnico para transferência de conhecimento, conforme condições e requisitos estabelecidos no Termo de Referência e seus anexos.



RISCO 01		
Identificação do Risco	Fase	Planejamento
	Evento	Demora excessiva na fase de planejamento da contratação
	Consequência	Atraso na formalização da contratação e risco de descontinuidade dos serviços.
Análise do Risco	Probabilidade da Ocorrência	Média
	Impacto	Alto
	Nível de Aceitação do Risco	Inaceitável
Resposta ao Risco	Ações Preventivas	Iniciar elaboração do processo com antecedência compatível com a complexidade do objeto contratual. Descrição clara das atividades a serem desempenhadas em cada etapa pelos membros da fase de planejamento; Estabelecer cronograma a ser cumprido por todos os envolvidos na fase de planejamento.
	Setor Responsável	Diretoria de Informática e Tecnologia da Informação/ Diretoria de Administração e Suprimentos
	Ações Contingenciais	Redistribuição das atividades em atraso para acelerar a finalização das etapas pendentes.
	Setor Responsável	Diretoria de Administração / Diretoria de Informática e Tecnologia da Informação



RISCO 02		
Identificação do Risco	Fase	Planejamento
	Evento	Dimensionamento inadequado da solução NGFW para o ambiente da Câmara.
	Consequência	Cobertura insuficiente das necessidades de segurança e desempenho da rede, indisponibilidade e comprometimento da continuidade dos serviços.
Análise e do Risco	Probabilidade da Ocorrência	Baixa
	Impacto	Alto
	Nível de Aceitação do Risco	Inaceitável
Resposta ao Risco	Ações Preventivas	Realizar levantamento técnico atualizado do ambiente; identificar quantidade de usuários e dispositivos; mensurar o tráfego atual e estimar crescimento; estabelecer requisitos mínimos de desempenho; prever margem de crescimento da infraestrutura; e exigir que o equipamento ofertado suporte simultaneamente as funcionalidades de segurança previstas na contratação.
	Sector Responsável	Diretoria de Informática e Tecnologia da Informação
	Ações Contingenciais	Readequação da solução; otimizar as configurações, revisar políticas e funcionalidades e adotar medidas temporárias de redistribuição ou priorização do tráfego até a regularização da capacidade da solução.
	Sector Responsável	Diretoria de Informática e Tecnologia da Informação



RISCO 03		
Identificação do Risco	Fase	Planejamento
	Evento	Estimativa de preços incompatível com a realidade do mercado, considerando a diversidade dos serviços que compõem a solução de Firewall de Próxima Geração – NGFW/UTM.
	Consequência	Licitação deserta ou fracassada; apresentação de propostas inexequíveis ou incompatíveis com o mercado; contratação com valor insuficiente para a execução integral da solução; ou fixação de valor excessivo, com risco de contratação antieconômica e planejamento orçamentário inadequado.
Análise do Risco	Probabilidade da Ocorrência	Média
	Impacto	Alto
	Nível de Aceitação do Risco	Inaceitável
Resposta ao Risco	Ações Preventivas	Realizar pesquisa de preços considerando as especificações da solução; Realizar pesquisa de preços ampla, utilizando fontes diversas, inclusive com consulta direta a fornecedores dos serviços demandados.
	Setor Responsável	Diretoria de Administração / Diretoria de Informática e Tecnologia da Informação
	Ações Contingenciais	Caso o certame resulte deserto, fracassado ou com propostas incompatíveis, revisar a estimativa de preços e os requisitos da contratação; realizar nova pesquisa de mercado; avaliar eventuais ajustes no Termo de Referência e no edital, sem comprometer a segurança, a continuidade da solução; e, se necessário, republicar o certame com parâmetros revisados. Análise de realização de contratação emergencial.
	Setor Responsável	Diretoria de Administração / Diretoria de Informática e Tecnologia da Informação



RISCO 04		
Identificação do Risco	Fase	Planejamento
	Evento	Não obtenção de orçamentos de empresas especializadas para subsidiar a pesquisa de preços da contratação.
	Consequência	Dificuldade de concluir a estimativa de preços; fragilização da justificativa do valor estimado; atraso na fase preparatória; questionamentos sobre a suficiência da pesquisa de mercado; e risco de definição de valores incompatíveis com os serviços e requisitos técnicos da solução.
Análise do Risco	Probabilidade da Ocorrência	Média
	Impacto	Médio
	Nível de Aceitação do Risco	Média aceitação
Resposta ao Risco	Ações Preventivas	Solicitar orçamentos com antecedência suficiente à empresas especializadas, apresentando descrição clara da solução, dos principais requisitos técnicos; registrar formalmente as tentativas de cotação, inclusive e-mails enviados, contatos realizados e ausência de resposta; complementar a pesquisa com contratações públicas similares, preços disponíveis no PNCP e outras fontes admitidas; e justificar expressamente eventuais limitações da pesquisa em razão das particularidades da solução e da necessidade de viabilidade técnica nos locais de prestação.
	Setor Responsável	Diretoria de Administração
	Ações Contingenciais	Caso não sejam obtidos orçamentos suficientes, instruir a pesquisa de preços com as tentativas frustradas de cotação, contratações similares, histórico contratual, parâmetros públicos disponíveis e justificativa técnica da estimativa adotada; revisar os valores e a metodologia utilizada, quando necessário; e ajustar a estimativa antes da publicação do edital, caso se mostre insuficiente ou incompatível com o mercado.
	Setor Responsável	Diretoria de Administração



RISCO 05		
Identificação do Risco	Fase	Planejamento
	Evento	Cláusulas de penalidades genéricas ou insuficientes para as peculiaridades da contratação da solução de Firewall NGFW/UTM.
	Consequência	Dificuldade de aplicação de sanções em caso de descumprimento dos níveis de serviço aplicáveis à solução, indisponibilidade decorrente de falha atribuível ao produto, atraso ou falha no fornecimento do appliance, licenças ou subscrições, interrupção do suporte técnico, descumprimento dos prazos de substituição do equipamento ou execução das demais obrigações da contratada em desacordo com o contrato.
Análise do Risco	Probabilidade da Ocorrência	Média
	Impacto	Alto
	Nível de Aceitação do Risco	Inaceitável
Resposta ao Risco	Ações Preventivas	Prever no Termo de Referência, no edital e no contrato hipóteses específicas de descumprimento contratual, incluindo atraso no fornecimento ou disponibilização dos componentes da solução, indisponibilidade decorrente de falha atribuível ao produto, descumprimento dos níveis de serviço, falhas no suporte técnico, interrupção de licenças ou subscrições e descumprimento dos prazos de substituição do appliance, sem imputar à contratada deste objeto obrigações de implantação, configuração, administração, monitoramento ou sustentação operacional atribuídas à contratação correlata. Também deverá constar a aplicabilidade das sanções previstas na Lei nº 14.133/2021 e nas normas internas da Câmara Municipal, especialmente a Portaria nº CM060/2025, quando cabível
	Setor Responsável	Diretoria de Administração



RISCO 05		
	Ações Contingenciais	Identificada conduta irregular, registrar formalmente a ocorrência nos autos da fiscalização; notificar a contratada para correção ou apresentação de justificativa; promover glosa de valores quando houver serviço não executado ou prestado em desconformidade; instaurar procedimento sancionatório quando cabível; aplicar as penalidades previstas no edital, no contrato e na legislação; e, em caso de descumprimento grave ou reiterado, avaliar a extinção contratual e a adoção de nova contratação.
	Setor Responsável	Fiscalização do Contrato / Gestão de Contratos / Procuradoria, quando necessário



RISCO 06		
Identificação do Risco	Fase	Planejamento
	Evento	Falta de clareza na delimitação das responsabilidades entre a contratada responsável pelo fornecimento da solução NGFW/UTM e a empresa responsável pela contratação correlata de serviços especializados de implantação, configuração, administração, monitoramento e sustentação operacional.
	Consequência	Sobreposição ou lacuna de responsabilidades; dificuldades na implantação e no diagnóstico de falhas; atraso na solução de incidentes; transferência indevida de responsabilidades entre fornecedores; dificuldades na fiscalização e aplicação dos níveis de serviço; e risco de indisponibilidade ou comprometimento da continuidade operacional da solução.
Análise do Risco	Probabilidade da Ocorrência	Média
	Impacto	Alto
	Nível de Aceitação do Risco	Inaceitável
Resposta ao Risco	Ações Preventivas	Delimitar expressamente no Termo de Referência, nos anexos técnicos e nos instrumentos contratuais as responsabilidades de cada contratação, estabelecendo mecanismos de interlocução e escalonamento entre a Câmara Municipal, a contratada da solução NGFW/UTM e a empresa responsável pelos serviços especializados correlatos, sem prejuízo do acionamento direto do suporte da solução nos casos relacionados a hardware, firmware, licenciamento, subscrição, garantia ou funcionalidade nativa da plataforma.
	Setor Responsável	Diretoria de Informática / Diretoria de Administração
	Ações Contingenciais	Identificada a falta de clareza antes da publicação do edital, revisar o ETP, o Termo de Referência e os anexos técnicos; se a inconsistência for apontada por pedido de esclarecimento ou impugnação, responder de forma fundamentada e promover a retificação, quando cabível; caso a falha seja verificada durante a execução, limitar as exigências ao escopo contratado, formalizar os ajustes permitidos e avaliar a necessidade de contratação específica ou alteração contratual juridicamente admissível.



RISCO 06		
	Setor Responsável	Diretoria de Informática / Diretoria de Administração / Procuradoria, quando necessário



RISCO 07		
Identificação do Risco	Fase	Planejamento
	Evento	Ausência de recursos orçamentários ou financeiros suficientes para suportar o valor estimado da contratação da solução integrada de Firewall NGFW/UTM.
	Consequência	Impossibilidade de concluir a contratação no valor planejado; necessidade de revisão da estimativa; atraso na publicação do edital; frustração do certame; ou comprometimento da disponibilização e continuidade tecnológica da solução de segurança de rede.
Análise do Risco	Probabilidade da Ocorrência	Baixa
	Impacto	Alto
	Nível de Aceitação do Risco	Média aceitação
Resposta ao Risco	Ações Preventivas	Verificar previamente a existência de dotação orçamentária compatível com o valor estimado da contratação; confirmar a disponibilidade financeira para suportar as despesas durante toda a vigência contratual; e alinhar a estimativa com a Diretoria Contábil e Financeira antes da publicação do edital.
	Setor Responsável	Diretoria de Administração / Diretoria Contábil e Financeira
	Ações Contingenciais	Caso seja constatada insuficiência orçamentária ou financeira, revisar os valores estimados, adequar o planejamento à disponibilidade de recursos, avaliar ajustes tecnicamente admissíveis no objeto, atualizar o Termo de Referência e o edital antes da publicação ou postergar a contratação até a regularização dos recursos necessários.
	Setor Responsável	Diretoria de Administração / Diretoria Contábil e Financeira / Diretoria de Informática



RISCO 08		
Identificação do Risco	Fase	Seleção
	Evento	Não alcançar todos os possíveis interessados em participar da seleção.
	Consequência	Baixa competitividade, número reduzido de propostas, risco de licitação deserta ou fracassada, menor disputa entre os fornecedores, possível contratação em condições menos vantajosas e atraso na implantação dos serviços de conectividade corporativa.
Análise do Risco	Probabilidade da Ocorrência	Média
	Impacto	Alto
	Nível de Aceitação do Risco	Inaceitável
Resposta ao Risco	Ações Preventivas	Divulgar amplamente o aviso de licitação, o edital e seus anexos nos meios oficiais cabíveis; assegurar a publicação no PNCP e no sítio eletrônico da Câmara Municipal; conceder prazo adequado para elaboração das propostas, considerando a complexidade técnica do objeto; disponibilizar o Termo de Referência e os anexos de forma clara e acessível; comunicar a contratação a empresas especializadas conhecidas, sem restrição à competitividade; e responder tempestivamente aos pedidos de esclarecimento.
	Setor Responsável	Diretoria de Informática / Agente de Contratação / Pregoeiro
	Ações Contingenciais	Caso o certame seja deserto, fracassado ou conte com baixa participação, revisar os meios de divulgação utilizados, os prazos concedidos, os requisitos de participação, os critérios de habilitação e eventuais exigências que possam ter reduzido indevidamente a competitividade; avaliar a republicação do edital com ajustes cabíveis; ampliar a divulgação do novo certame; e reexaminar as condições da contratação para torná-la mais clara e compatível com o mercado.
	Setor Responsável	Diretoria de Administração / Diretoria de Informática / Agente de Contratação / Pregoeiro



RISCO 09		
Identificação do Risco	Fase	Seleção
	Evento	Questionamentos administrativos ou judiciais relacionados à falta de publicidade, transparência ou acesso aos documentos e atos do processo de contratação.
	Consequência	Apresentação de impugnações, recursos, representações ou ações judiciais; atraso no procedimento licitatório; suspensão da sessão eletrônica; necessidade de republicação de atos; questionamento da validade do certame; e risco de anulação de fases da licitação.
Análise do Risco	Probabilidade da Ocorrência	Baixa
	Impacto	Alto
	Nível de Aceitação do Risco	Média aceitação
Resposta ao Risco	Ações Preventivas	Planejar o procedimento com prazo suficiente para a prática e divulgação dos atos; publicar o edital, o Termo de Referência, o ETP, os anexos técnicos e os demais documentos essenciais nos meios oficiais cabíveis; divulgar resultados, decisões, julgamentos e prazos recursais; assegurar a possibilidade de pedidos de esclarecimento, impugnações e recursos; e manter os autos do processo devidamente organizados e acessíveis para controle interno e externo.
	Setor Responsável	Diretoria de Administração / Agente de Contratação / Pregoeiro
	Ações Contingenciais	Analisar o questionamento com celeridade e decisão fundamentada; prestar esclarecimentos adicionais aos interessados; juntar aos autos os comprovantes de publicação e os documentos pertinentes; corrigir eventual falha de publicidade ou transparência; republicar o ato quando necessário; reabrir prazo, se a falha tiver comprometido a participação ou o contraditório; e submeter a matéria à Procuradoria em caso de questionamento jurídico relevante.
	Setor Responsável	Diretoria de Informática / Agente de Contratação / Pregoeiro / Procuradoria, quando necessário



RISCO 10		
Identificação do Risco	Fase	Seleção
	Evento	Atraso ou suspensão do processo licitatório em razão de impugnações ao edital, ao Termo de Referência, aos requisitos técnicos, aos critérios de habilitação ou à modelagem dos lotes.
	Consequência	Atraso na contratação dos serviços; necessidade de retificação do edital; suspensão da sessão eletrônica; reabertura de prazos; aumento da carga administrativa; e risco de descontinuidade dos serviços.
Análise do Risco	Probabilidade da Ocorrência	Média
	Impacto	Alto
	Nível de Aceitação do Risco	Inaceitável
Resposta ao Risco	Ações Preventivas	Submeter previamente o ETP, o Termo de Referência, o edital e os anexos técnicos à análise jurídica; elaborar documentos claros quanto ao objeto, à exigência de operadoras e rotas distintas, aos requisitos de habilitação, aos critérios de julgamento e aos prazos de impugnação e recurso; justificar tecnicamente as exigências que possam restringir a competitividade; publicar todos os anexos necessários; e prever prazo adequado entre a publicação e a sessão eletrônica.
	Setor Responsável	Diretoria de Administração / Agente de Contratação / Pregoeiro / Procuradoria
	Ações Contingenciais	Analisar a impugnação com celeridade e decisão fundamentada; acolhê-la total ou parcialmente quando procedente; retificar o edital, o Termo de Referência ou os anexos técnicos, se necessário; republicar os documentos alterados e reabrir prazo quando a modificação afetar a formulação das propostas; suspender ou redesignar a sessão eletrônica, quando cabível; e registrar e divulgar todas as decisões pelos meios oficiais.
	Setor Responsável	Diretoria de Administração / Agente de Contratação / Pregoeiro / Procuradoria



RISCO 11		
Identificação do Risco	Fase	Seleção
	Evento	Apresentação de propostas comerciais inexecutáveis, insuficientemente dimensionadas ou elaboradas sem consideração de todos os serviços exigidos no Termo de Referência e em seus anexos.
	Consequência	Desclassificação de propostas; atraso na etapa de julgamento; redução da competitividade; risco de contratação por valor insuficiente; falhas na implantação ou na execução dos serviços; necessidade de reequilíbrio indevido; e possível fracasso do certame.
Análise do Risco	Probabilidade da Ocorrência	Média
	Impacto	Alto
	Nível de Aceitação do Risco	Inaceitável
Resposta ao Risco	Ações Preventivas	Elaborar o Termo de Referência e os anexos técnicos com descrição clara de todos os serviços, equipamentos e obrigações incluídos no preço; disponibilizar planilha ou estrutura de formação de custos, quando necessária; esclarecer que a proposta deverá contemplar todos os encargos da execução; permitir pedidos de esclarecimento; e analisar a exequibilidade dos valores apresentados antes da aceitação definitiva da proposta.
	Setor Responsável	Diretoria de Administração / Diretoria de Informática / Agente de Contratação / Pregoeiro
	Ações Contingenciais	Identificada proposta aparentemente inexecutável ou incompleta, solicitar esclarecimentos e documentos que demonstrem sua viabilidade; realizar diligência, quando cabível; desclassificar a proposta caso a exequibilidade não seja comprovada; convocar a próxima licitante classificada; e, se todas as propostas forem inadequadas, revisar a estimativa de preços e os requisitos da contratação antes de promover novo certame.
	Setor Responsável	Agente de Contratação / Pregoeiro / Diretoria de Administração / Diretoria de Informática



RISCO 12		
Identificação do Risco	Fase	Seleção
	Evento	Instabilidade, indisponibilidade ou funcionamento inadequado da plataforma Compras.gov.br durante a sessão pública, a fase de lances, o envio de propostas ou documentos, o julgamento ou a habilitação.
	Consequência	Impossibilidade de envio de propostas, lances ou documentos; interrupção da sessão eletrônica; prejuízo à participação dos licitantes; atraso no procedimento; necessidade de suspensão ou reagendamento da sessão; e risco de questionamentos quanto à isonomia e à regularidade dos atos praticados.
Análise do Risco	Probabilidade da Ocorrência	Média
	Impacto	Alto
	Nível de Aceitação do Risco	Inaceitável
Resposta ao Risco	Ações Preventivas	Acompanhar previamente as condições de funcionamento da plataforma; verificar eventuais comunicados de indisponibilidade; iniciar os procedimentos com antecedência suficiente; manter registro das ocorrências e mensagens do sistema; prever no edital regras para suspensão e retomada da sessão; e orientar os licitantes quanto aos canais oficiais de comunicação durante o certame.
	Setor Responsável	Agente de Contratação / Pregoeiro
	Ações Contingenciais	Constatada falha da plataforma, registrar a ocorrência e suspender a sessão quando necessário; comunicar os licitantes pelos meios disponíveis; preservar os atos validamente praticados; reagendar ou retomar a sessão após o restabelecimento do sistema, com prazo adequado e divulgação prévia; e, caso a falha comprometa a isonomia ou a validade do procedimento, anular os atos afetados e repeti-los.
	Setor Responsável	Agente de Contratação / Pregoeiro / Diretoria de Administração / Procuradoria, quando necessário



RISCO 13		
Identificação do Risco	Fase	Seleção
	Evento	Realização de comando equivocado na plataforma Compras.gov.br, incluindo aceitação, recusa, classificação, desclassificação, habilitação, inabilitação ou encerramento indevido de etapa do procedimento.
	Consequência	Aceitação indevida de proposta ou documentação irregular; exclusão injustificada de licitante; comprometimento da isonomia; apresentação de recursos; atraso no procedimento; necessidade de correção ou repetição de atos; e risco de anulação da fase afetada.
Análise do Risco	Probabilidade da Ocorrência	Baixa
	Impacto	Alto
	Nível de Aceitação do Risco	Média aceitação
Resposta ao Risco	Ações Preventivas	Conduzir o procedimento com atenção e observância às etapas da plataforma; conferir previamente a proposta, os documentos e a decisão a ser registrada; evitar a execução de comandos durante interrupções ou acúmulo de tarefas; manter registros das análises realizadas; e, sempre que possível, revisar os atos relevantes antes da confirmação definitiva no sistema.
	Setor Responsável	Agente de Contratação / Pregoeiro
	Ações Contingenciais	Identificado o erro, registrar imediatamente a ocorrência nos autos e no sistema, quando possível; suspender a sessão se necessário; comunicar os licitantes; corrigir ou anular o ato equivocado, quando juridicamente admissível; restabelecer a etapa afetada e os prazos pertinentes; e, caso não seja possível o saneamento, submeter a questão à autoridade competente e à Procuradoria para adoção das providências cabíveis.
	Setor Responsável	Agente de Contratação / Pregoeiro / Diretoria de Administração / Procuradoria, quando necessário



RISCO 14		
Identificação do Risco	Fase	Seleção
	Evento	Inabilitação dos licitantes por exigências excessivas, documentação inadequada ou descumprimento dos requisitos de habilitação técnica, jurídica, fiscal, social, trabalhista ou econômico-financeira.
	Consequência	Licitação fracassada, redução da competitividade, atraso na contratação dos serviços de conectividade, necessidade de reabertura de prazo ou realização de novo certame, além de questionamentos quanto à proporcionalidade das exigências de habilitação.
Análise do Risco	Probabilidade da Ocorrência	Baixa
	Impacto	Alto
	Nível de Aceitação do Risco	Média aceitação
Resposta ao Risco	Ações Preventivas	Definir requisitos de habilitação proporcionais e compatíveis com o objeto; evitar exigências excessivamente restritivas quanto a atestados, quantitativos mínimos ou experiência anterior; prever documentação clara e objetiva no edital; exigir comprovação de capacidade técnica pertinente aos serviços objeto da contratação conforme o lote; e submeter as exigências à análise jurídica antes da publicação do edital.
	Setor Responsável	Diretoria de Administração / Diretoria de Informática
	Ações Contingenciais	Analisar a documentação de habilitação conforme o edital e a legislação aplicável; permitir o saneamento de falhas formais quando juridicamente admissível e sem prejuízo à isonomia; fundamentar as decisões de habilitação ou inabilitação; abrir prazo recursal quando cabível; e, caso todos os licitantes sejam inabilitados, avaliar a concessão de prazo para nova documentação ou a revisão das exigências e realização de novo certame.
	Setor Responsável	Agente de Contratação / Pregoeiro / Diretoria de Administração / Procuradoria, quando necessário



RISCO 15		
Identificação do Risco	Fase	Seleção
	Evento	Não publicação da íntegra dos documentos do processo após finalizada a licitação.
	Consequência	Descumprimento de formalidade legal, redução da transparência do certame, dificuldade de controle interno e externo, questionamentos por licitantes ou órgãos de controle e risco de determinação para complementação da publicidade dos atos.
Análise do Risco	Probabilidade da Ocorrência	Média
	Impacto	Baixo
	Nível de Aceitação do Risco	Aceitável
Resposta ao Risco	Ações Preventivas	Adotar lista de verificação contemplando a publicação dos documentos essenciais do processo; conferir a publicação no PNCP, quando aplicável, no sítio eletrônico da Câmara Municipal e nos demais meios oficiais cabíveis; designar responsável pela conferência final da publicidade dos atos antes do encerramento da fase de seleção.
	Setor Responsável	Agente de Contratação / Comissão Especial de Contratação
	Ações Contingenciais	Publicar os documentos faltantes tão logo seja detectada a ausência de publicidade; registrar nos autos a providência adotada; comunicar a complementação aos interessados, quando necessário; republicar ou complementar ato específico se a ausência tiver prejudicado prazo de recurso, impugnação ou contraditório; e revisar a lista de verificação para evitar repetição da falha em futuros processos.
	Setor Responsável	Agente de Contratação / Comissão Especial de Contratação



RISCO 16		
Identificação do Risco	Fase	Gestão Contratual
	Evento	Não formalização do contrato pela empresa vencedora.
	Consequência	Impedimento do início da implantação; atraso na substituição dos serviços vigentes; necessidade de convocação de licitante remanescente ou realização de novo procedimento; e risco de descontinuidade dos serviços.
Análise do Risco	Probabilidade da Ocorrência	Média
	Impacto	Alto
	Nível de Aceitação do Risco	Inaceitável
Resposta ao Risco	Ações Preventivas	Antes da adjudicação e homologação, verificar a regularidade da empresa vencedora, a manutenção das condições de habilitação, a validade da documentação exigida e a inexistência de impedimentos à contratação; prever no edital prazo claro para assinatura do contrato; informar as consequências da recusa injustificada; manter comunicação formal com a vencedora após a homologação; e preparar previamente a minuta contratual e os documentos necessários à formalização.
	Setor Responsável	Núcleo de Contratos / Pregoeira
	Ações Contingenciais	Notificar formalmente a empresa vencedora para assinatura do contrato no prazo estabelecido; registrar eventual recusa, inércia ou descumprimento da convocação; aplicar as sanções cabíveis, quando caracterizada recusa injustificada; avaliar a convocação das licitantes remanescentes, observada a ordem de classificação; e, se não for possível a contratação, iniciar as providências para novo certame do lote correspondente.
	Setor Responsável	Gestão de Contratos / Diretoria de Administração / Pregoeira / Procuradoria, quando necessário



RISCO 17		
Identificação do Risco	Fase	Gestão contratual
	Evento	Não publicação do contrato ou de seus anexos nos meios oficiais exigidos.
	Consequência	Descumprimento de formalidade legal indispensável; prejuízo à transparência da contratação; risco de questionamentos por órgãos de controle; ou necessidade de regularização posterior da publicidade do ajuste.
Análise do Risco	Probabilidade da Ocorrência	Média
	Impacto	Baixo
	Nível de Aceitação do Risco	Aceitável
Resposta ao Risco	Ações Preventivas	Adotar lista de verificação para a fase de formalização contratual, contemplando a publicação dos contratos dos dois lotes e de seus anexos nos meios oficiais cabíveis; conferir a publicação no PNCP, no sítio eletrônico da Câmara Municipal e nos demais meios exigidos; designar responsável pela verificação da publicidade antes do início da execução; e registrar nos autos os respectivos comprovantes.
	Setor Responsável	Gestão de Contratos / Controle Interno
	Ações Contingenciais	Publicar o contrato e seus anexos tão logo seja detectada a ausência de publicidade; juntar aos autos os comprovantes da publicação; comunicar a regularização aos setores responsáveis pela implantação e fiscalização; avaliar se a omissão afetou a eficácia, o início da execução ou algum prazo contratual; e revisar a lista de verificação interna para evitar reincidência.
	Setor Responsável	Gestão de Contratos / Diretoria de Administração / Procuradoria, quando necessário



RISCO 18		
Identificação do Risco	Fase	Execução contratual
	Evento	Atraso na disponibilização do appliance, licenças, subscrições, documentação, acessos, atualizações ou demais componentes da solução NGFW/UTM sob responsabilidade da Contratada, ou incompatibilidade de cronogramas e dependências entre esta contratação e a contratação correlata responsável pelos serviços especializados de implantação, configuração, migração, integração, testes e homologação.
	Consequência	Atraso na implantação e entrada em operação da solução NGFW/UTM; necessidade de reprogramação das atividades previstas nas contratações correlatas; prolongamento da utilização da solução atualmente existente; risco de descontinuidade ou redução temporária da proteção da infraestrutura tecnológica; e comprometimento do cronograma de transição para a nova solução.
Análise do Risco	Probabilidade da Ocorrência	Média
	Impacto	Alto
	Nível de Aceitação do Risco	Inaceitável
Resposta ao Risco	Ações Preventivas	Definir claramente, nos respectivos instrumentos contratuais, as responsabilidades e os prazos atribuídos à fornecedora da solução NGFW/UTM e à empresa responsável pelos serviços especializados correlatos; estabelecer cronograma coordenado para disponibilização do appliance, licenças, subscrições, documentação e acessos necessários à implantação; identificar previamente as dependências entre as contratações; promover reuniões de alinhamento entre a Câmara e as empresas envolvidas, quando necessário; e prever mecanismos de acompanhamento e contingência para evitar que atrasos em uma contratação comprometam a execução da outra.
	Setor Responsável	Diretoria de Informática / Fiscalização do Contrato / Gestão de Contratos



RISCO 18		
	Ações Contingenciais	Identificada a origem do atraso, notificar formalmente a contratada responsável pela obrigação inadimplida; exigir plano de recuperação com novos prazos e medidas corretivas; reprogramar, quando necessário, o cronograma das atividades interdependentes; intensificar o acompanhamento das contratações correlatas; manter temporariamente a solução existente ou adotar medida de contingência tecnicamente viável, quando necessário; e aplicar as medidas contratuais cabíveis exclusivamente à contratada responsável pelo descumprimento.
	Setor Responsável	Fiscalização dos Contratos Correlatos / Gestão de Contratos / Diretoria de Informática / Diretoria de Administração



RISCO 19		
Identificação do Risco	Fase	Execução Contratual
	Evento	Interrupção ou degradação dos serviços de rede durante a implantação, integração ou migração para a nova solução NGFW/UTM, em razão de falha de integração, indisponibilidade de componente da solução fornecida ou ocorrência relacionada à execução dos serviços especializados da contratação correlata.
	Consequência	Indisponibilidade total ou parcial da conectividade e dos serviços de rede dependentes da solução de segurança; interrupção temporária de atividades administrativas ou legislativas; necessidade de retorno à configuração anterior ou acionamento de contingência; e atraso na entrada em produção da nova solução.
Análise do Risco	Probabilidade da Ocorrência	Média
	Impacto	Alto
	Nível de Aceitação do Risco	Inaceitável
Resposta ao Risco	Ações Preventivas	Delimitar, nos respectivos instrumentos contratuais, as responsabilidades relacionadas ao fornecimento da solução NGFW/UTM e à execução dos serviços especializados de implantação e migração; coordenar previamente o cronograma entre as contratações correlatas; assegurar a disponibilidade do appliance, licenças, subscrições, firmwares, documentação e suporte técnico necessários à implantação; exigir, no âmbito da contratação correlata de serviços especializados, planejamento da migração, testes, procedimentos de contingência e possibilidade de retorno à configuração anterior; e programar as atividades com potencial de indisponibilidade para períodos de menor impacto às atividades institucionais.
	Setor Responsável	Diretoria de Informática / Fiscalização dos Contratos Correlatos / Gestão de Contratos



RISCO 19		
	Ações Contingenciais	Identificar a origem da ocorrência e acionar imediatamente a contratada responsável; adotar, por meio da equipe responsável pelos serviços especializados correlatos, os procedimentos de contingência ou retorno à configuração anterior, quando tecnicamente viáveis; acionar o suporte técnico oficial da solução quando a ocorrência envolver hardware, firmware, software, licenciamento, subscrição ou funcionalidade nativa da plataforma; restabelecer prioritariamente os serviços essenciais; registrar a ocorrência e aplicar, quando cabível, as medidas contratuais à empresa responsável pela falha.
	Setor Responsável	Gestão de Contratos / Fiscalização dos Contratos Correlatos / Diretoria de Informática

RISCO 20		
Identificação do Risco	Fase	Execução contratual
	Evento	Configuração inadequada das políticas, regras ou parâmetros de segurança da solução NGFW/UTM durante sua implantação, migração, administração ou sustentação operacional no âmbito da contratação correlata de serviços especializados.
	Consequência	Exposição da infraestrutura tecnológica da Câmara Municipal; comprometimento da confidencialidade, integridade ou disponibilidade dos recursos de rede; bloqueios ou liberações indevidas de tráfego; acessos não autorizados; aumento da exposição a ataques e vulnerabilidades; interrupção de serviços; e eventual dano institucional.
Análise do Risco	Probabilidade da Ocorrência	Média
	Impacto	Alto
	Nível de Aceitação do Risco	Inaceitável



RISCO 20		
Resposta ao Risco	Ações Preventivas	Prever, na contratação correlata de serviços especializados, equipe tecnicamente qualificada para implantação, configuração, administração e sustentação da solução; realizar levantamento e registro das configurações existentes antes da migração; manter backup das configurações necessárias à recuperação; submeter alterações relevantes das políticas de segurança aos procedimentos de validação definidos pela Câmara; realizar testes antes da entrada em produção; e manter interlocução com o suporte técnico da solução NGFW/UTM quando houver dúvida, incompatibilidade ou comportamento relacionado a funcionalidade nativa da plataforma.
	Setor Responsável	Diretoria de Informática / Fiscalização da Contratação Correlata de Serviços Especializados
	Ações Contingenciais	Acionar imediatamente a empresa responsável pelos serviços especializados correlatos para revisão das políticas ou regras afetadas e, quando tecnicamente indicado, restauração de configuração anterior válida; isolar temporariamente segmentos, serviços ou acessos afetados, quando necessário à contenção do risco; acionar o suporte técnico oficial da solução caso haja indício de falha ou comportamento relacionado a funcionalidade nativa da plataforma; validar as correções antes do restabelecimento integral do ambiente; e registrar a ocorrência e as providências adotadas.
	Setor Responsável	Diretoria de Informática / Fiscalização da Contratação Correlata de Serviços Especializados / Gestão de Contratos



RISCO 21		
Identificação do Risco	Fase	Gestão contratual
	Evento	Falha do appliance ou de componente da solução NGFW/UTM sob responsabilidade da contratada.
	Consequência	Indisponibilidade total ou parcial da solução de segurança, redução das funcionalidades de proteção, comprometimento da conectividade ou aumento da exposição da infraestrutura a riscos de segurança.
Análise e do Risco	Probabilidade da Ocorrência	Baixa
	Impacto	Alto
	Nível de Aceitação do Risco	Inaceitável
Resposta ao Risco	Ações Preventivas	Manter suporte técnico oficial da solução durante toda a vigência contratual; assegurar a disponibilidade dos mecanismos de backup e restauração das configurações; manter firmware, software, licenças e subscrições em condições regulares de funcionamento; e observar os níveis de serviço e mecanismos de atualização tecnológica previstos no Termo de Referência.
	Setor Responsável	Fiscalização do Contrato / Gestão de Contratos / Diretoria de Informática
	Ações Contingenciais	Acionar imediatamente o suporte técnico da solução; adotar, em conjunto com a equipe técnica da Câmara e, quando aplicável, com a empresa responsável pelos serviços especializados correlatos, as medidas de contingência necessárias ao restabelecimento do serviço; e realizar a substituição do appliance ou componente defeituoso nos prazos estabelecidos no Termo de Referência, inclusive mediante solução temporária quando prevista e necessária à continuidade operacional.
	Setor Responsável	Fiscalização do Contrato / Gestão de Contratos / Diretoria de Informática



RISCO 22		
Identificação do Risco	Fase	Gestão contratual
	Evento	Falhas, atrasos ou interrupções na ativação, manutenção ou renovação das licenças, subscrições e assinaturas de segurança da solução NGFW/UTM.
	Consequência	Indisponibilidade ou redução de funcionalidades de segurança, interrupção de atualizações de assinaturas, aumento da exposição da infraestrutura a vulnerabilidades.
Análise do Risco	Probabilidade da Ocorrência	Média
	Impacto	Alto
	Nível de Aceitação do Risco	Inaceitável
Resposta ao Risco	Ações Preventivas	Prever contratualmente que todas as licenças, subscrições e assinaturas permaneçam ativas durante todo o período de vigência da contratação, sem interrupções; manter monitoramento periódico da situação das licenças pela equipe técnica e pela fiscalização do contrato; exigir da contratada comprovação da regularidade e vigência dos licenciamentos, sempre que solicitado; prever sanções contratuais para atrasos ou falhas imputáveis à contratada que ocasionem interrupção das funcionalidades licenciadas; Manter registros das licenças, datas de ativação, vencimentos e renovações para facilitar a fiscalização contratual.
	Setor Responsável	Diretoria de Informática / Gestão e Fiscalização do contrato.
	Ações Contingenciais	Acionamento imediato da contratada para regularização emergencial das licenças, priorizando a restauração das funcionalidades críticas de proteção, com adoção temporária de controles de segurança até o restabelecimento integral da solução.
	Setor Responsável	Fiscalização do Contrato / Gestão de Contratos / Diretoria de Informática / Procuradoria, quando necessário



RISCO 23		
Identificação do Risco	Fase	Gestão contratual
	Evento	Prorrogação, revisão ou manutenção dos contratos sem análise adequada da vantajosidade, dos preços praticados, da qualidade dos serviços, do desempenho técnico e das condições atuais do mercado.
	Consequência	Manutenção de contratos em condições desfavoráveis; pagamento de valores superiores aos praticados no mercado; continuidade de serviços com qualidade insatisfatória; perda da oportunidade de obter melhores condições; prejuízo ao erário; e questionamentos por órgãos de controle.
Análise e do Risco	Probabilidade da Ocorrência	Média
	Impacto	Alto
	Nível de Aceitação do Risco	Inaceitável
Resposta ao Risco	Ações Preventivas	Realizar, antes de qualquer prorrogação ou revisão, análise formal da vantajosidade; pesquisar preços de contratações similares e do mercado; avaliar o cumprimento dos níveis de serviço, os registros de indisponibilidade, a qualidade do suporte, a atualização dos equipamentos e licenças; verificar a regularidade dos reajustes e demais alterações contratuais; e registrar justificativa técnica e administrativa para a decisão.
	Setor Responsável	Gestão de Contratos / Fiscalização do Contrato / Diretoria de Informática / Diretoria Contábil e Financeira
	Ações Contingenciais	Suspender a prorrogação ou revisão até a conclusão da análise; solicitar documentos, memórias de cálculo e justificativas complementares; negociar condições mais vantajosas, quando cabível; corrigir valores ou critérios aplicados em desacordo com o contrato; não prorrogar caso a vantajosidade não seja demonstrada; e iniciar novo processo licitatório em tempo hábil.
	Setor Responsável	Gestão de Contratos / Diretoria de Administração / Diretoria de Informática / Diretoria Contábil e Financeira / Procuradoria, quando necessário



RISCO 24		
Identificação do Risco	Fase	Gestão contratual
	Evento	Extinção anormal do contrato por caso fortuito, força maior ou impossibilidade superveniente de continuidade da execução.
	Consequência	Interrupção dos serviços; comprometimento das atividades administrativas e legislativas; necessidade de adoção de solução temporária; e realização de nova contratação em caráter urgente.
Análise do Risco	Probabilidade da Ocorrência	Baixa
	Impacto	Alto
	Nível de Aceitação do Risco	Média aceitação
Resposta ao Risco	Ações Preventivas	Munir o contrato com cláusulas que estabeleçam critérios e condições para rescisão e transição contratual e transição dos serviços; realizar consultas periódicas ao contratado quanto ao interesse de manutenção e/ou renovação da relação contratual.
	Setor Responsável	Gestão de Contratos / Fiscalização do Contrato / Diretoria de Informática
	Ações Contingenciais	Acionar imediatamente o plano de continuidade aplicável à solução; preservar as configurações, backups, documentação e demais informações necessárias à continuidade tecnológica; acionar, quando aplicável, a empresa responsável pelos serviços especializados correlatos para adoção das medidas operacionais de contingência; e, conforme a situação concreta e a legislação aplicável, adotar as providências necessárias para contratação emergencial ou outra solução temporária que assegure a continuidade da proteção da infraestrutura tecnológica.
	Setor Responsável	Gestão de Contratos / Diretoria de Informática / Diretoria de Administração / Procuradoria, quando necessário



Relatório de Cotação: Contratação de solução de Firewall de nova geração (NGFW) - Estimativa preliminar

Pesquisa realizada entre 23/06/2026 15:10:13 e 23/06/2026 15:25:49

Relatório gerado no dia 23/06/2026 15:27:04 (IP: 200.146.241.153)

Em conformidade com a Instrução Normativa N° 65 de 07 de Julho de 2021 (Lei n° 14.133).

Método Matemático Aplicado: Média Aritmética dos preços obtidos - Preço calculado com base na média aritmética de todos os preços selecionados pelo usuário para aquele determinado Item.

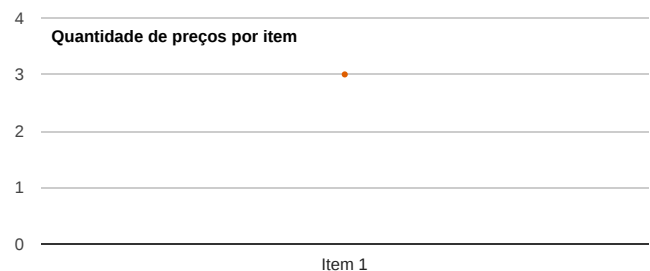
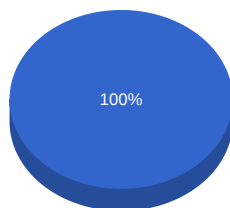
Conforme Instrução Normativa N° 65 de 07 de Julho de 2021 (Lei n° 14.133), no Artigo 3°, "A pesquisa de preços será materializada em documento que conterá: INC V-Método matemático aplicado para a definição do valor estimado."

Item	Preços	Quantidade	Preço Estimado	Percentual	Preço Estimado Calculado	% Valor Global	Total
1) Firewal de nova geração NGFW	3	12 Meses	R\$ 5.863,28 (un)	-	R\$ 5.863,28	100%	R\$ 70.359,36

Valor Global: R\$ 70.359,36

Valor do item em relação ao total

● 1) Firewal de nova...



Detalhamento dos Itens

Item 1: Firewal de nova geração NGFW

Preço Estimado: R\$ 5.863,28 (un)

Percentual: -

Preço Estimado Calculado: R\$ 5.863,28

Média dos Preços Obtidos: R\$ 5.863,28

Quantidade	Descrição	Observação
12 Meses	Solução integrada de segurança de rede do tipo Firewall de Próxima Geração (NGFW/UTM)	

Preço (Compras Governamentais) 1: Média Saneada das Propostas Finais (TCU)

R\$ 4.599,00

Inc. I Art. 5° da IN 65 de 07 de Julho de 2021 (Lei n° 14.133)



Relatório gerado no dia 23/06/2026 15:27:04 (IP: 200.146.241.153)

Código Validação: RNTzWcWsw%2fQclBvPbBa6v4rmme57RwFMXsGsjlKfrGkqHU8nPtm6WA%3d%3d

<http://www.bancodeprecos.com.br/CertificadoAutenticidade?token=RNTzWcWsw%252fQclBvPbBa6v4rmme57RwFMXsGsjlKfrGkqHU8nPtm6WA%253d%253d>

1 / 5

CNPJ: 18.400.945/0001-66

Órgão: MUNICIPIO DE RIO PIRACICABA / 700 - Unidade Única

Objeto: Contratação de serviços de conectividade, segurança da informação, infraestrutura e armazenamento em nuvem

Descrição: SERVIÇO PROTEÇÃO (FIREWALL) SERVIÇO PROTEÇÃO (FIREWALL) Serviço de Firewall de Nova Geração (NGFW) para monitorar e filtrar recursos avançados de filtragem de pacotes e análise profunda de tráfego (DPI) e proteção contra invasões e alertas em tempo real. - SERVIÇO PROTEÇÃO (FIREWALL) SERVIÇO PROTEÇÃO (FIREWALL) Serviço de Firewall de Nova Geração (NGFW) para monitorar e filtrar recursos avançados de filtragem de pacotes e análise profunda de tráfego (DPI) e proteção contra invasões e alertas em tempo real.

Fonte: <https://pncp.gov.br/app/editais/18400945000166/2026/4>

Data: 23/02/2026 00:00

Modalidade: Pregão - Eletrônico

SRP: NÃO

Identificação: 18400945000166-1-000004/2026

Lote/Item: 1/43

Ata: N/A

Homologação: 23/02/2026 00:00

Quantidade: 12

Unidade: MÊS

UF: MG

CNPJ	Razão Social do Fornecedor				Valor da Proposta Final
05.684.180/0001-91	COMPANHIA ITABIRANA DE TELECOMUNICACOES LTDA				R\$ 4.599,00
VENCEDOR					
Estado:	Cidade:	Endereço:	Telefone:	Email:	
MG	Itabira	RUA AGUA SANTA, 450	(31) 3067-7000	fiscal@valenet.com.br	

Preço (Compras Governamentais) 2: Média Saneada das Propostas Finais (TCU)

R\$ 6.670,83

Inc. I Art. 5º da IN 65 de 07 de Julho de 2021 (Lei nº 14.133)

CNPJ: 18.561.209/0001-90

Órgão: CONTAGEM CAMARA MUNICIPAL / 1476 - Unidade Única

Objeto: CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA PRESTAÇÃO DE DOIS SERVIÇOS DISTINTOS: O FORNECIMENTO, INSTALAÇÃO E CONFIGURAÇÃO DE DOIS LINKS DEDICADOS DE INTERNET DE 1 GBPS, COM PROTEÇÃO CONTRA ATAQUES DOS/DDOS E UMA SOLUÇÃO DE SEGURANÇA INTEGRADA (FIREWALL UTM/NGFW), E A PRESTAÇÃO DE SERVIÇO DE COMUNICAÇÃO MULTIMÍDIA (SAAS), QUE INCLUI UMA SOLUÇÃO DE PABX VIRTUAL EM NUVEM BASEADA EM PROTOCOLO SIP/VOIP, COM RAMAIS DDR E CAPACIDADE PARA TRÁFEGO ILIMITADO EM LIGAÇÕES LOCAIS E NACIONAIS (FIXO-FIXO E FIXO-MÓVEL) PARA ATENDER AS DEMANDAS DA CÂMARA MUNICIPAL DE CONTAGEM.

Descrição: Serviço de Firewall UTM-NGFW, com treinamento da equipe técnica, serviço de suporte técnico contínuo (inclusive monitoramento proativo). Quantidade: 1 - Serviço de Firewall UTM-NGFW, com treinamento da equipe técnica, serviço de suporte técnico contínuo (inclusive monitoramento proativo). Quantidade: 1

Fonte: <https://pncp.gov.br/app/editais/18561209000190/2025/17>

Data: 29/10/2025 09:15

Modalidade: Pregão - Eletrônico

SRP: NÃO

Identificação: 18561209000190-1-000017/2025

Lote/Item: 1/2

Ata: N/A

Homologação: 17/11/2025 00:00

Quantidade: 24

Unidade: MÊS

UF: MG

CNPJ		Razão Social do Fornecedor			Valor da Proposta Final
71.208.516/0001-74		ALGAR TELECOM S/A			R\$ 6.670,83
VENCEDOR					
Estado:	Cidade:	Endereço:	Telefone:	Email:	
MG	Uberlândia	RUA JOSE ALVES GARCIA, 415	(34) 2183-0000	algar@algar.com.br	

Preço (Compras Governamentais) 3: Média Saneada das Propostas Finais (TCU)

R\$ 6.320,00

Inc. I Art. 5º da IN 65 de 07 de Julho de 2021 (Lei nº 14.133)



Relatório gerado no dia 23/06/2026 15:27:04 (IP: 200.146.241.153)
Código Validação: RNTzWcWsw%2fQclBvPbBa6v4rmme57RwFMXGsjlkfrGkqHU8nPtm6WA%3d%3d
<http://www.bancodeprecos.com.br/CertificadoAutenticidade?token=RNTzWcWsw%252fQclBvPbBa6v4rmme57RwFMXGsjlkfrGkqHU8nPtm6WA%253d%253d>

CNPJ: 18.715.466/0001-39

Órgão: MUNICIPIO DE ESMERALDAS / 01 - Prefeitura Municipal de Esmeraldas

Objeto: [Portal de Compras Públicas] - O objeto da presente licitação é a Contratação de serviços de Appliance de Firewall de Próxima Geração (do inglês NGFW), contemplando o fornecimento dos equipamentos no regime de locação, suporte técnico especializado, implantação, configuração, armazenamento de log e relatório e monitoramento de cibersegurança, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

Descrição: **Lote 1 - Serviços de appliance de firewall de próxima geração (do inglês ngfw) tipo 2 - contemplando fornecimento de equipamento em regime de locação, instalação, configuração, suporte técnico especializado, armazenamento de logs e relatórios, monitoramen** - Lote 1 - Serviços de appliance de firewall de próxima geração (do inglês ngfw) tipo 2 - contemplando fornecimento de equipamento em regime de locação, instalação, configuração, suporte técnico especializado, armazenamento de logs e relatórios, monitoramento de cibersegurança e gerenciamento centralizado.

Fonte: <https://pncp.gov.br/app/editais/18715466000139/2025/61>

Data: 21/08/2025 09:00

Modalidade: Pregão - Eletrônico

SRP: NÃO

Identificação: 18715466000139-1-000061/2025

Lote/Item: 1/2

Ata: N/A

Homologação: 23/09/2025 00:00

Quantidade: 12

Unidade: Mês

UF: MG

CNPJ		Razão Social do Fornecedor			Valor da Proposta Final
08.208.805/0001-37		JRV SERVICOS LTDA			R\$ 6.320,00
VENCEDOR					
Estado:	Cidade:	Endereço:	Telefone:	Email:	
BA	Salvador	AVENIDA TANCREDO NEVES, 000620	(71) 3018-7381	sac@xlogic.com.br	



Relatório gerado no dia 23/06/2026 15:27:04 (IP: 200.146.241.153)
Código Validação: RNTzWcWsw%2fQclBvPbBa6v4rmme57RwFMXSgsjlkfrGkqHU8nPtm6WA%3d%3d
<http://www.bancodeprecos.com.br/CertificadoAutenticidade?token=RNTzWcWsw%252fQclBvPbBa6v4rmme57RwFMXSgsjlkfrGkqHU8nPtm6WA%253d%253d>

Os cálculos deste relatório foram elaborados com base nas metodologias descritas na 4ª edição do Manual de Orientação de Pesquisa de Preços do Superior Tribunal de Justiça (STJ). A utilização desse manual assegura a precisão e a confiabilidade dos cálculos apresentados, conforme os padrões estabelecidos pelo STJ. Para mais detalhes, acesse [aqui](#).

Critérios Estatísticos Gerais	
30%	Preços excessivamente elevados: valores superiores a 30% da média do rol de preços obtidos
70%	Inexequível: valores inferiores a 70% da média do rol de preços obtidos

Critérios Estatísticos por item									
Nº	Item	Média	Mediana	Desvio Padrão Amostral	Coeficiente de Variação	Método Estatístico	Preço Mínimo	Válidos	
								Média	Mediana
1	Firewal de nova geração NGFW	R\$ 5.863,28	R\$ 6.320,00	1108,86	18,91	Média	R\$ 4.599,00	R\$ 5.863,28	R\$ 6.320,00

Item	Especificação	Und	Qtd	Cotação	Parâmetros	Empresas	Porte	Valor Unit	Média	Avaliação	Obs Avaliação
1	Solução integrada de segurança de rede do tipo Firewall de Próxima Geração (NGFW/UTM)	mes	12,00	MUNICIPIO DE RIO PIRACICABA / 700 - Unidade Única	Portal Nacional de Contratações Públicas	COMPANHIA ITABIRANA DE TELECOMUNICACOES LTDA	Grupo II – Empresa de Grande Porte	R\$ 4.599,00	R\$ 5.863,28	VÁLIDO	
				CONTAGEM CAMARA MUNICIPAL / 1476 - Unidade Única	Portal Nacional de Contratações Públicas	ALGAR TELECOM S/A	Demais	R\$ 6.670,83		VÁLIDO	
				MUNICIPIO DE ESMERALDAS / 01 - Prefeitura Municipal de Esmeraldas	Portal Nacional de Contratações Públicas	JRV SERVICOS LTDA	Empresa de Pequeno Porte (EPP)	R\$ 6.320,00		VÁLIDO	





Extrato de fontes utilizadas neste relatório

ATENÇÃO - O Banco de Preços é uma solução tecnológica que atende aos parâmetros de pesquisa dispostos em Leis vigentes, Instruções Normativas, Acórdãos, Regulamentos, Decretos e Portarias. Sendo assim, por reunir diversas fontes governamentais, complementares e sites de domínio amplo, o sistema não é considerado uma fonte e, sim, um meio para que as pesquisas sejam realizadas de forma segura, ágil e eficaz.

Fontes utilizadas nesta cotação:

1 - Portal Nacional de Contratações Públicas

<https://pncp.gov.br/app/>

Data: 23/06/2026 15:21:10

Acessar a fonte [aqui](#)



Relatório gerado no dia 23/06/2026 15:27:04 (IP: 200.146.241.153)
Código Validação: RNTzWcWsw%2fQclBvPbBa6v4rmme57RwFMXSgsjIkfrGkqHU8nPtm6WA%3d%3d
<http://www.bancodeprecos.com.br/CertificadoAutenticidade?token=RNTzWcWsw%252fQclBvPbBa6v4rmme57RwFMXSgsjIkfrGkqHU8nPtm6WA%253d%253d>

5 / 5



Assinado digitalmente por Alexsandro Alves Vasconcelos. Verifique a autenticidade em verificador.betha.cloud e insira o código 6L1-RV5-2GL-L3V.

Assinantes



Alexsandro Alves Vasconcelos

Assinou em 06/10/2026 às 16:08:30 com o certificado avançado da Betha Sistemas e possui a identidade verificada com o CPF ***.245.806-**.

Eu, Alexsandro Alves Vasconcelos, 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.betha.cloud** e insira o código abaixo:

6L1-RV5-2GL-L3V



MINUTA DO CONTRATO
Lei nº 14.133, de 1º de abril de 2021

PROCESSO ADMINISTRATIVO nº /2026

A **CÂMARA MUNICIPAL DE DIVINÓPOLIS/MG**, inscrita no CNPJ nº 23.774.227/0001-90, com sede na Rua São Paulo, 277, Centro, Divinópolis/MG, CEP 35500-006, adiante denominada **CONTRATANTE**, neste ato representada por seu Presidente, Vereador _____ e a empresa _____, adiante denominada **CONTRATADA**, representada por seu representante legal _____, celebram o presente Termo de Contrato, decorrente do processo licitatório nº _____ sob a regência da Lei Federal nº 14.133, de 2021 e legislação pertinente, mediante as cláusulas e condições a seguir pactuadas:

1. CLÁUSULA PRIMEIRA – DO OBJETO

- 1.1.** O presente contrato tem por objeto a contratação de solução integrada de segurança de rede do tipo Firewall de Próxima Geração (NGFW/UTM), em regime de locação com cessão de uso/comodato do appliance, incluindo fornecimento de 01 (um) appliance, licenciamentos e subscrições durante toda a vigência, recursos de conectividade segura/VPN, plataforma de gerenciamento centralizado, suporte técnico oficial, atualizações, garantia de continuidade tecnológica e treinamento técnico para a equipe de Tecnologia da Informação da Câmara Municipal, conforme o Termo de Referência, seus anexos, o Edital e a proposta da Contratada.
- 1.2.** Integram este contrato, independentemente de transcrição:
 - 1.2.1.** O Edital e seus anexos;
 - 1.2.2.** O Termo de Referência e seus anexos;
 - 1.2.3.** A proposta final da Contratada; e
 - 1.2.4.** Os demais documentos que instruem o procedimento e que sejam expressamente vinculados à contratação.



2. CLÁUSULA SEGUNDA – DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS

- 2.1. A solução será fornecida pelo preço global mensal e anual abaixo indicado, contemplando integralmente os componentes e obrigações descritos neste contrato e no Termo de Referência:

Item	Descrição da Solução	Catmat/ Catser	Quant	Unidade	Valor unitário	Valor Total
01	<i>Fornecimento de solução integrada de segurança de rede do tipo Firewall de próxima geração (NGFW), em regime de locação com cessão de uso/comodato do appliance</i>	27090	12	Mês	R\$	R\$
TOTAL MENSAL						R\$
TOTAL ANUAL						R\$

- 2.1.1. Os quantitativos, especificações técnicas mínimas, funcionalidades e critérios de conformidade são os constantes do Termo de Referência e de seus anexos, que prevalecerão para a avaliação do atendimento técnico.
- 2.1.2. Todos os equipamentos e componentes físicos deverão ser novos, sem uso anterior, e o appliance deverá pertencer à linha atual do fabricante e estar regularmente comercializado, com suporte e atualizações oficiais disponíveis na data da entrega. Não serão aceitos equipamentos reconicionados, remanufaturados, nem softwares ou firmwares beta, experimentais ou não oficiais.

3. CLÁUSULA TERCEIRA – DA VIGÊNCIA E DA PRORROGAÇÃO

- 3.1. O prazo de vigência será de 12 (doze) meses, contado da assinatura do contrato, observadas as condições de eficácia e divulgação legal.
- 3.2. Por se tratar de contratação de natureza continuada, a vigência poderá ser prorrogada sucessivamente, observado o limite máximo de 10 (dez) anos e os requisitos dos arts. 106 e 107 da Lei nº 14.133/2021, especialmente a demonstração de vantajosidade, a disponibilidade orçamentária e a autorização da autoridade competente.
- 3.3. A prorrogação não constitui direito subjetivo da Contratada e dependerá de formalização própria, antes do término da vigência, mediante avaliação do interesse



público e do cumprimento das obrigações contratuais.

4. CLÁUSULA QUARTA – DO MODELO DE EXECUÇÃO, ENTREGA E RECEBIMENTO

- 4.1.** A execução, os prazos de entrega e disponibilização do appliance, dos licenciamentos e subscrições, a documentação exigida, o treinamento e os demais procedimentos observarão integralmente o Termo de Referência e seus anexos.
- 4.2.** O recebimento provisório ocorrerá no ato da entrega dos equipamentos e licenças, mediante conferência pela equipe de Tecnologia da Informação e pelo fiscal do contrato quanto à conformidade com o Termo de Referência e a proposta final.
- 4.3.** Constatada irregularidade, desconformidade ou pendência, a Contratada será formalmente comunicada para realizar a correção ou substituição no prazo fixado pela Contratante, sem prejuízo das medidas e sanções cabíveis.
- 4.4.** O recebimento definitivo dependerá da verificação da conformidade do appliance e dos demais componentes, licenciamentos, subscrições, documentação técnica, acessos oficiais, garantia, suporte e funcionalidades exigidas. A implantação, configuração, migração, integração, testes e homologação operacional executados no âmbito de contratação correlata não constituem condição para o recebimento definitivo deste fornecimento.
- 4.5.** O recebimento definitivo não afasta a responsabilidade da Contratada pela qualidade, adequação, suporte e funcionamento dos componentes sob sua responsabilidade durante toda a vigência contratual.
- 4.6.** Ao término ou encerramento da contratação, a Contratada deverá retirar o equipamento fornecido no prazo e nas condições previstos no Termo de Referência, em especial no prazo máximo ali estabelecido, sem ônus adicional à Contratante.

5. CLÁUSULA QUINTA – DA GESTÃO E FISCALIZAÇÃO

- 5.1.** O contrato deverá ser executado fielmente pelas partes, de acordo com suas cláusulas, com o Termo de Referência e com a Lei nº 14.133/2021, respondendo cada parte pelas consequências de sua inexecução total ou parcial.
- 5.2.** A gestão e a fiscalização serão exercidas por agentes públicos formalmente designados pela Contratante, nos termos do art. 117 da Lei nº 14.133/2021 e da regulamentação interna da Câmara Municipal.
- 5.3.** Compete à fiscalização acompanhar e avaliar a execução, conferir a conformidade do objeto, registrar ocorrências, solicitar esclarecimentos e determinar a regularização de falhas e desconformidades, comunicando ao gestor e à autoridade



competente as situações que excedam sua atribuição.

- 5.4. A Contratada deverá aceitar os procedimentos de inspeção, verificação e controle adotados pela fiscalização e fornecer os dados, documentos e esclarecimentos solicitados.
- 5.5. A atuação da gestão e da fiscalização não exclui nem reduz a responsabilidade da Contratada pela execução do objeto, inclusive perante terceiros.
- 5.6. As comunicações formais entre as partes serão realizadas por escrito, admitido o meio eletrônico quando cabível.

6. CLÁUSULA SEXTA – DA SUBCONTRATAÇÃO

- 6.1. É vedada a subcontratação integral do objeto, bem como a transferência a terceiros da responsabilidade pelas obrigações principais assumidas pela Contratada, especialmente quanto ao fornecimento e à disponibilização da solução e de seus componentes, incluindo o appliance de Firewall NGFW, licenciamentos, subscrições, plataforma de gerenciamento, garantia, atualização tecnológica, continuidade da solução e suporte técnico oficial

7. CLÁUSULA SÉTIMA – DO PREÇO E DOS ENCARGOS

- 7.1. O valor total da contratação é de R\$ _____ (_____), correspondente a 12 (doze) parcelas mensais de R\$ _____ (_____).
- 7.2. No preço estão incluídas todas as despesas diretas e indiretas necessárias ao cumprimento integral do objeto, inclusive tributos, encargos, licenças, subscrições, frete, seguro, acessórios, suporte, atualizações, garantia, substituições, treinamento e demais custos previstos no Termo de Referência, não sendo devido pagamento adicional por tais componentes.
- 7.3. A Contratada arcará com os ônus decorrentes de eventual equívoco no dimensionamento dos custos de sua proposta, ressalvadas as hipóteses legais de reequilíbrio econômico-financeiro.

8. CLÁUSULA OITAVA – DO PAGAMENTO E DA MEDIÇÃO

- 8.1. A avaliação da execução e a medição dos resultados observarão o Instrumento de Medição de Resultados (IMR) e os critérios objetivos previstos no Termo de Referência e em seu Anexo III, inclusive quanto aos impactos sobre os valores devidos.



- 8.2. O pagamento será efetuado em moeda corrente nacional no prazo de até 10 (dez) dias úteis após o recebimento da nota fiscal, mediante ordem bancária para crédito em conta indicada pela Contratada ou por boleto bancário, observadas a liquidação da despesa e as condições deste contrato.
- 8.3. O pagamento ficará condicionado à comprovação da execução correspondente e à regularidade fiscal exigível, mediante consulta ao SICAF ou, na impossibilidade, aos sítios oficiais ou à documentação prevista no art. 68 da Lei nº 14.133/2021.
- 8.4. Serão efetuadas as retenções tributárias previstas na legislação aplicável. A Contratada optante pelo Simples Nacional deverá comprovar sua condição para fins de eventual tratamento tributário favorecido.
- 8.5. Havendo erro na nota fiscal ou circunstância que impeça a liquidação da despesa, o pagamento ficará suspenso até a regularização, reiniciando-se o prazo após a comprovação da correção, sem ônus para a Contratante.
- 8.6. Havendo controvérsia sobre parcela da execução, a Contratante poderá observar o art. 143 da Lei nº 14.133/2021 quanto à liquidação e ao pagamento da parcela incontroversa.

9. CLÁUSULA NONA – DO REAJUSTE E DO EQUILÍBRIO ECONÔMICO-FINANCEIRO

- 9.1. Os preços inicialmente contratados são fixos e irrevogáveis no prazo de um ano contado da data do orçamento estimado, em 06/10/2026.
- 9.2. Após o interregno anual, os preços poderão ser reajustados mediante aplicação do IPCA-e, ou do índice oficial que venha a substituí-lo, exclusivamente quanto às obrigações iniciadas e concluídas após a ocorrência da anualidade.
- 9.3. Nos reajustes subsequentes, o interregno mínimo de 1 (um) ano será contado dos efeitos financeiros do último reajuste. O reajuste será formalizado por apostilamento, quando cabível, nos termos do art. 136 da Lei nº 14.133/2021.
- 9.4. Os pedidos de restabelecimento do equilíbrio econômico-financeiro serão instruídos e analisados conforme a legislação aplicável, mediante comprovação dos pressupostos legais, preservada a matriz de riscos e as condições da contratação.

10. CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DA CONTRATANTE

- 10.1. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com o contrato, o Edital e seus anexos.
- 10.2. Disponibilizar a infraestrutura física e elétrica predial necessária à implantação, compatível com as condições e requisitos previamente informados, nos limites



previstos no Termo de Referência.

- 10.3.** Proporcionar as informações e facilidades de acesso necessárias ao cumprimento das obrigações contratuais, observadas as regras de segurança da informação.
- 10.4.** Acompanhar, fiscalizar, avaliar e registrar a execução, notificando a Contratada sobre falhas, vícios, defeitos ou desconformidades e fixando prazo para saneamento.
- 10.5.** Receber o objeto provisória e definitivamente, conforme os critérios estabelecidos no Termo de Referência.
- 10.6.** Efetuar os pagamentos devidos no prazo e nas condições estabelecidas, após a regular liquidação da despesa.
- 10.7.** Aplicar as sanções cabíveis, assegurados o contraditório e a ampla defesa, e adotar as medidas administrativas necessárias diante de descumprimentos.
- 10.8.** Emitir decisão sobre solicitações e reclamações relacionadas à execução, ressalvados requerimentos manifestamente impertinentes, protelatórios ou sem interesse para a boa execução.
- 10.9.** A Administração não responderá por compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução contratual, nem por danos causados a terceiros por atos da Contratada, seus empregados, prepostos ou subordinados.

11. CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES DA CONTRATADA

- 11.1.** Cumprir integralmente as obrigações previstas neste contrato, no Edital, no Termo de Referência e em seus anexos, assumindo os riscos e despesas necessários à execução adequada do objeto.
- 11.2.** Fornecer e manter disponibilizada, durante toda a vigência, a solução integrada, o appliance, os licenciamentos e subscrições, os recursos VPN, a plataforma de gerenciamento, a documentação, a garantia, o suporte técnico oficial e as atualizações exigidas.
- 11.3.** Assegurar que o appliance e os componentes físicos sejam novos, sem uso anterior, e que a solução esteja regularmente suportada e atualizada pelo fabricante, observados os requisitos de ciclo de vida previstos no Termo de Referência.
- 11.4.** Manter canal de atendimento apto ao recebimento de chamados e prestar suporte técnico especializado, com atendimento humano em língua portuguesa, nos canais e níveis de serviço estabelecidos no Termo de Referência.
- 11.5.** Atender aos chamados nos prazos de resposta e restabelecimento definidos no Termo de Referência, adotando medidas corretivas, contingenciais ou substitutivas



necessárias à continuidade da solução.

- 11.6.** Providenciar a atualização tecnológica ou substituição do appliance por equipamento de capacidade igual ou superior, sem ônus adicional, nas hipóteses de descontinuidade, fim de suporte, fim de vida útil, incompatibilidade ou incapacidade de atendimento dos requisitos, conforme condições do Termo de Referência.
- 11.7.** Substituir definitivamente o appliance nas hipóteses de falhas recorrentes e nos prazos estabelecidos no Termo de Referência, inclusive quando ocorrerem 4 (quatro) ou mais ocorrências atribuíveis ao hardware ou aos componentes sob sua responsabilidade em período de 60 (sessenta) dias corridos, devidamente comprovadas.
- 11.8.** Fornecer os acessórios, cabos, adaptadores, componentes de montagem e dispositivos complementares de proteção elétrica necessários ao funcionamento da solução, sem cobrança posterior, ressalvadas as adequações ou ampliações da infraestrutura predial atribuídas à Contratante.
- 11.9.** Prestar apoio técnico à implantação, configuração, integração e operação da solução nos limites estabelecidos no Termo de Referência e na contratação correlata de serviços especializados, sem assumir como objeto deste contrato as atividades expressamente excluídas.
- 11.10.** Realizar treinamento técnico à equipe de Tecnologia da Informação da Contratante, com carga horária mínima de 8 (oito) horas, abrangendo as funcionalidades contratadas, e apresentar previamente a documentação de qualificação do instrutor exigida no Termo de Referência.
- 11.11.** Comprovar, no momento da assinatura do contrato, a qualificação do profissional ou equipe de suporte técnico, nos termos do Termo de Referência.
- 11.12.** Manter, durante toda a vigência, as condições de habilitação e qualificação exigidas na licitação, comunicando qualquer fato impeditivo superveniente.
- 11.13.** Cumprir as determinações regulares do gestor e do fiscal do contrato e prestar os esclarecimentos e informações solicitados.
- 11.14.** Corrigir, reparar, substituir ou remover, às suas expensas e no prazo fixado pela Contratante, o objeto ou componente com vício, defeito, falha ou desconformidade.
- 11.15.** Responsabilizar-se pelos danos causados à Contratante ou a terceiros em decorrência da execução contratual, inclusive por vícios, defeitos ou inadequações dos equipamentos, acessórios ou serviços sob sua responsabilidade, sem que a fiscalização reduza essa responsabilidade.
- 11.16.** Guardar sigilo sobre as informações a que tiver acesso em razão do contrato, restringindo seu uso às finalidades contratuais e adotando medidas de segurança adequadas.



- 11.17.** Cumprir a Lei nº 13.709/2018 (LGPD), tratando dados pessoais somente para finalidades legítimas relacionadas ao contrato, vedado o compartilhamento indevido com terceiros, e comunicar incidentes de segurança conforme as regras do Termo de Referência e da legislação aplicável.
- 11.18.** Observar a legislação ambiental aplicável, a eficiência energética e a logística reversa, responsabilizando-se pela retirada e destinação ambientalmente adequada das peças, equipamentos e materiais substituídos.
- 11.19.** Retirar o equipamento ao término ou encerramento do contrato, no prazo e nas condições do Termo de Referência, sem prejuízo da continuidade e da segurança dos dados e informações da Contratante.
- 11.20.** Não permitir trabalho de menor de 16 (dezesesseis) anos, salvo na condição de aprendiz a partir de 14 (quatorze) anos, nem trabalho noturno, perigoso ou insalubre por menor de 18 (dezoito) anos.
- 11.21.** Arcar com os custos decorrentes de eventual erro no dimensionamento de sua proposta, ressalvadas as hipóteses legais de alteração e recomposição do equilíbrio econômico-financeiro.
- 11.22.** Cumprir, durante toda a execução contratual, as exigências legais de reserva de cargos para pessoas com deficiência, reabilitados da Previdência Social e aprendizes, bem como as demais reservas de cargos previstas em legislação específica, quando aplicáveis, comprovando seu atendimento sempre que solicitado pela Contratante, nos termos do art. 92, inciso XVII, da Lei nº 14.133/2021.

12. CLÁUSULA DÉCIMA SEGUNDA – DA GARANTIA DE EXECUÇÃO

- 12.1.** Não será exigida garantia contratual de execução, conforme avaliação constante do Termo de Referência, sem prejuízo das garantias, do suporte, das substituições e das demais responsabilidades técnicas assumidas pela Contratada.

13. CLÁUSULA DÉCIMA TERCEIRA – DA PROTEÇÃO DE DADOS E DA SEGURANÇA DA INFORMAÇÃO

- 13.1.** A Contratada deverá observar a Lei nº 13.709/2018 (LGPD), as normas de segurança da informação aplicáveis e as disposições do Termo de Referência quanto aos dados pessoais a que tenha acesso em razão do certame ou da execução contratual.
- 13.2.** Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram o acesso, observados os princípios da boa-fé, finalidade, adequação, necessidade, segurança, prevenção e responsabilização.



- 13.3.** É vedado o compartilhamento de dados com terceiros, salvo quando necessário à execução contratual e juridicamente autorizado, observadas as condições legais e as instruções da Contratante.
- 13.4.** A Contratada deverá adotar controles de acesso, rastreabilidade, confidencialidade e proteção compatíveis com os riscos da solução, bem como orientar seus profissionais quanto aos deveres de sigilo e proteção de dados.
- 13.5.** A Contratante poderá solicitar informações e documentos para verificar o cumprimento desta cláusula, devendo a Contratada atender às solicitações pertinentes.
- 13.6.** A Contratada deverá comunicar imediatamente à Contratante qualquer incidente de segurança da informação de que tenha conhecimento e que possa comprometer a confidencialidade, a integridade ou a disponibilidade dos dados, credenciais, configurações, registros, sistemas ou demais recursos tecnológicos institucionais, fornecendo as informações disponíveis para análise da ocorrência e adotando as medidas necessárias à preservação dos registros e das evidências técnicas pertinentes, nos termos do Termo de Referência.
- 13.7.** A Contratada deverá assegurar que o acesso às informações, configurações, credenciais e demais recursos tecnológicos da Contratante seja restrito aos profissionais devidamente autorizados e às finalidades estritamente necessárias à execução contratual, mediante credenciais individualizadas, observados o princípio do menor privilégio e os requisitos de identificação e rastreabilidade dos acessos administrativos, quando tecnicamente disponíveis, conforme o Termo de Referência.
- 13.8.** Encerrada a contratação ou terminado o tratamento dos dados, a Contratada deverá adotar, relativamente às informações sob sua responsabilidade, as providências necessárias à devolução, eliminação ou conservação legalmente exigida dos dados e informações institucionais a que tenha tido acesso, observadas as orientações da Contratante, as disposições do Termo de Referência e as hipóteses legais de conservação previstas na Lei nº 13.709/2018.

14. CLÁUSULA DÉCIMA QUARTA – DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

- 14.1.** Comete infração administrativa, nos termos da Lei nº 14.133, de 2021 e da Portaria n.º CM-060/2025, o contratado que:
 - 14.1.1.** Der causa à inexecução parcial do contrato;
 - 14.1.2.** Der causa à inexecução parcial do contrato que cause grave dano ao contratante, ao funcionamento dos serviços públicos ou ao interesse coletivo;
 - 14.1.3.** Der causa à inexecução total do contrato;



- 14.1.4.** Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
 - 14.1.5.** Apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
 - 14.1.6.** Praticar ato fraudulento na execução do contrato;
 - 14.1.7.** Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
 - 14.1.8.** Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 2013.
- 14.2.** Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:
- 14.2.1.** Advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);
 - 14.2.2.** Impedimento de licitar e contratar com a administração, quando praticadas as condutas descritas nos itens 14.1.2, 14.1.3 e 14.1.4, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);
 - 14.2.3.** Declaração de inidoneidade para licitar e contratar com a administração pública, quando praticadas as condutas descritas nos itens 14.1.5, 14.1.6, 14.1.7 e 14.1.8, bem como nos itens 14.1.2, 14.1.3 e 14.1.4, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).
 - 14.2.4.** Multa:
 - a)** Moratória de 2% (dois por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 10 (dez) dias;
 - b)** Moratória de 2% (dois por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 10% (dez por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia.
 - c)** Compensatória de 3% (três por cento) sobre o valor total do contrato, no caso de inexecução total do objeto.
 - 14.2.5.** O atraso superior a 10 (dez) dias autoriza o contratante a promover a rescisão do contrato motivada por descumprimento ou cumprimento irregular de suas cláusulas, conforme art. 137, I da Lei nº 14.133, de 2021.
- 14.3.** A aplicação das sanções previstas no contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021).
- 14.4.** Todas as sanções previstas no contrato poderão ser aplicadas cumulativamente com



a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

- 14.4.1.** Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021).
- 14.4.2.** Se a multa aplicada e as indenizações devidas forem superiores ao valor do pagamento devido ao contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será objeto de cobrança, inclusive por via judicial (art. 156, §8º, da Lei nº 14.133, de 2021).
- 14.4.3.** Previamente ao encaminhamento do débito para cobrança judicial, a multa poderá ser recolhida administrativamente em favor do contratante, no prazo máximo de 07 (sete) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.
- 14.5.** A aplicação das sanções realizar-se-á em processo administrativo que assegure ao contratado o exercício do contraditório e da ampla defesa, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar com a administração e de declaração de inidoneidade para licitar ou contratar com a administração pública.
- 14.6.** Na aplicação das sanções serão considerados:
 - 14.6.1.** A natureza e a gravidade da infração cometida;
 - 14.6.2.** As peculiaridades do caso concreto;
 - 14.6.3.** As circunstâncias agravantes ou atenuantes;
 - 14.6.4.** Os danos que dela provierem para o contratante;
 - 14.6.5.** A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.
- 14.7.** Os atos descritos como infrações administrativas na Lei nº 14.133, de 2021, ou na legislação pertinente, que também sejam tipificados como infrações pela Lei nº 12.846, de 2013, serão apurados e julgados em conjunto, nos mesmos autos, observado o rito procedimental e a autoridade competente definidos na Lei nº 12.846, de 2013 e na Portaria n.º CM-060/2025.
- 14.8.** A personalidade jurídica do contratado poderá ser desconsiderada sempre que utilizada com abuso de direito, para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos no contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o contratado, observados, em todos os casos, o contraditório,



a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021).

- 14.9.** O contratante deverá, no prazo máximo 15 (quinze) dias úteis, a contar da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161, da Lei nº 14.133, de 2021).
- 14.10.** As sanções de impedimento de licitar e contratar com a administração e declaração de inidoneidade para licitar ou contratar com a administração pública são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.
- 14.11.** Os débitos do contratado para com o contratante, resultantes de multa administrativa e/ou indenizações não recolhidas, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo contratante em decorrência deste mesmo contrato ou de outros contratos administrativos que o contratado possua com o contratante.
- 14.12.** Eventual descumprimento ou inadimplemento parcial das obrigações, isto é, referente a quantidade de itens inferior à total, será considerado como inadimplemento restrito àquele(s) item(ns) específico(s), não implicando, automaticamente, a caracterização de inadimplemento global do contrato em relação aos demais itens regularmente executados.

15. CLÁUSULA DÉCIMA QUINTA – DA EXTINÇÃO CONTRATUAL

- 15.1.** O contrato será extinto nas hipóteses previstas nos arts. 137 a 139 da Lei nº 14.133/2021, observados o contraditório, a ampla defesa e as formalidades legais.
- 15.2.** A extinção poderá ocorrer por ato unilateral e escrito da Contratante, por acordo entre as partes ou por decisão judicial ou arbitral, quando cabível, nas hipóteses legalmente admitidas.
- 15.3.** A extinção não prejudicará a apuração de responsabilidades, a aplicação de sanções cabíveis nem a exigência de reparação de danos.
- 15.4.** Encerrado o contrato, a Contratada deverá cooperar com a retirada segura do equipamento e com as providências necessárias à preservação das informações da Contratante, observadas as obrigações do Termo de Referência.

16. CLÁUSULA DÉCIMA SEXTA – DA DOTAÇÃO ORÇAMENTÁRIA

- 16.1.** As despesas decorrentes da presente contratação estão programadas em dotações



orçamentárias própria do exercício de 2026, prevista no orçamento da Câmara Municipal nas seguintes classificações:

- 16.1.1.** Função programática: 01.001.001.01.122.1010.2003 – Gestão das atividades operacionais.
- 16.1.2.** Natureza da despesa: Ficha 1199 – 3.3.90.40.00.00.00.00 Serviços de Tecnologia da Informação.

17. CLÁUSULA DÉCIMA SÉTIMA – DOS CASOS OMISSOS

- 17.1.** Os casos omissos na execução deste Contrato serão decididos pela Contratante, observadas as disposições da Lei Federal nº 14.133/2021, os preceitos de direito público, a regulamentação interna da Câmara Municipal de Divinópolis, especialmente a Portaria CM nº 188/2023, os decretos federais cuja aplicação tenha sido incorporada à regulamentação municipal, os decretos municipais pertinentes e demais normas legais e regulamentares aplicáveis à matéria. Serão considerados, ainda, como parâmetros interpretativos, os entendimentos consolidados do Tribunal de Contas do Estado de Minas Gerais (TCMG), no que couber. Supletivamente, aplicar-se-ão os princípios da teoria geral dos contratos e as disposições de direito privado, nos termos do art. 89 da Lei Federal nº 14.133/2021.

18. CLÁUSULA DÉCIMA OITAVA – DAS ALTERAÇÕES

- 18.1.** Eventuais alterações contratuais reger-se-ão pelos arts. 124 e seguintes da Lei nº 14.133/2021 e deverão ser formalizadas por meio do instrumento adequado, observadas as competências, justificativas e limites legais.
- 18.2.** A Contratada fica obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, nos limites e hipóteses previstos na legislação aplicável.

19. CLÁUSULA DÉCIMA NONA – DA PUBLICAÇÃO

- 19.1.** Incumbirá à Contratante divulgar o instrumento contratual no Portal Nacional de Contratações Públicas (PNCP), na forma e nos prazos previstos na Lei nº 14.133/2021, sem prejuízo de outras publicações exigidas.

20. CLÁUSULA VIGÉSIMA – DO FORO

- 20.1.** Fica eleito o foro da Comarca de Divinópolis/MG para dirimir os litígios decorrentes



da execução deste contrato que não puderem ser compostos pela conciliação, observada a legislação aplicável.

[Local], [dia] de [mês] de [ano].

Representante legal da CONTRATANTE

Representante legal da CONTRATADA

TESTEMUNHAS:

- 1-
- 2-