PREFEITURA DE CAMPO MOURÃO
CAMPO MOURÃO | CIDADE ESCOLA

TERMO DE REFERÊNCIA
Lei Federal nº. 14.133/2021
Art.70 Decreto Municipal nº. 10.672 de 01 de dezembro de 2023
(Regulamento Geral)

IDENTIFICAÇÃO DA ÁREA TÉCNICA	
Área requisitante	**DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**
Responsável pelo termo	**FÁBIO CESAR DO CARMO E SILVA**
Cargo/função	**DIRETOR DE TECNOLOGIA DA INFORMAÇÃO**
E-mail	**depti@campomourao.pr.gov.br**
Telefone	**(44) 3518-1173**

1. DEFINIÇÃO DO OBJETO

Contratação de empresa de Tecnologia da Informação especializada na área de segurança corporativa digital e implantação de ambientes de salas de centrais de dados, para fornecimento de bens e serviços das seguintes soluções tecnológicas:

- Software de sistema de backup de dados e informações de arquivos digitais em ambiente virtualizado (Backup Virtual Local);
- Serviço para fornecimento de sistema de backup de dados e informações de arquivos digitais em nuvem (Backup Cloud);
- Equipamento e serviços para implantação de segurança virtual na rede de computadores para soluções de serviços de segurança para controle de ameaças virtuais na modalidade “Appliance do tipo UTM (Unified Threat Management) Firewall concentrador” em comodato – Firewall Concentrador Paço Municipal;
- Equipamento e serviços para implantação de segurança virtual na rede de computadores para controle de ameaças virtuais na modalidade “Appliance do tipo UTM (Unified Threat Management) Firewall concentrador redundante de alta disponibilidade (HA)” em comodato – Firewall Concentrador Redundante Paço Municipal em (HA);
- Firewall de borda para unidades com serviços essenciais em saúde pública municipal (**UPA** e **PALP**);
- Ferramenta de software de sistema para suporte remoto tipo “Help Desk”;
- Software de sistema antivírus corporativo para controle de ameaças digitais nos equipamentos da rede de computadores e segurança;
- Licença de uso de software para coleta e armazenamento de Logs (Syslog);
- Software de sistema para detecção e resposta endpoint EDR (ENDPOINT DETECTION AND RESPONSE/DETECÇÃO E RESPOSTA DE ENDPOINT) para implementar solução de segurança cibernética avançada e monitorar continuamente dispositivos finais para detectar comportamentos suspeitos, investigar ameaças em tempo real e responder automaticamente a incidentes como ransonware e malwares em equipamentos estações de trabalho da rede (computadores);
- Ferramenta de software de sistema web para abertura de chamados de suporte técnico tipo “Help Desk”;
- Serviço de implantação física e lógica de redundância de servidores de rede (AD e File Server).
- Implementação e implantação de plano de Disaster Recovery/Recuperação de Desastres; e
- Prestação de serviços continuados de processamento de dados e segurança da informação

Para todas as soluções, deverão ser incluídos treinamentos em níveis avançados especializados aos técnicos de tecnologia da informação da contratante para fins de atualização e reciclagem do conhecimento de forma presencial.

Durante a vigência contratual deverá ser realizado upgrade nas soluções e prestação de serviços de suporte técnico especializado continuado no regime (24x7x6) conforme especificações técnicas e níveis de serviços mínimos exigidos constantes no Termo de Referência, no Edital de Licitações e seus Anexos, tendo como referência o disposto na lei federal n.º 14.133/2021 (nova lei de licitações) e os Regulamentos da Prefeitura Municipal de Campo Mourão – PR.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO (JUSTIFICATIVA)

Desde a sua criação, a Diretoria de Tecnologia da Informação – DIRTI da Secretaria Municipal de Administração – SEADM da Prefeitura Municipal de Campo Mourão – PR, não tem medido esforços com relação ao intuito de gerar e gerenciar toda a sua capacidade de resposta institucional satisfatória à sociedade, em especial no que tange a responsabilidade em manter íntegro, confiável e seguro todo o ambiente de TI e o parque tecnológico da municipalidade, bem como manter e disponibilizar infraestrutura em equipamentos de TI, sistemas de comunicação, servidores de dados digitais e de bases de dados, segurança da informação, entre outros, de forma a possibilitar a disponibilidade de informações precisas e confiáveis à sociedade, aos órgãos reguladores e aos servidores públicos municipais.

Considerando-se que o principal objetivo da referida Diretoria de TI é assegurar aos usuários internos e aos servidores públicos municipais, a adequada prestação de serviços em relação a área tecnológica, uma vez que todas as informações e tarefas desempenhadas, nesse sentido, estão diretamente ligadas à utilização dos recursos de tecnologia da informação na prestação de serviços públicos àqueles que necessitarem.

Considerando-se que as organizações públicas têm o dever de atuar em estreito relacionamento com as políticas definidas pelo Governo Federal Brasileiro, no que se refere à Gestão de Tecnologia da Informação em especial a LEI Nº 13.709, de 14 de agosto de 2018 que “Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)” a qual entrou em vigor em janeiro de 2020.

Considerando-se que os princípios e os fundamentos formulados pelo governo têm como sustentação a utilização dos recursos de infraestrutura tecnológica que garantam a continuidade dos serviços prestados, os quais são uma necessidade fundamental para a existência das grandes instituições, sejam elas públicas ou privadas.

Considerando-se que as ações da Diretoria de Tecnologia da Informação da Secretaria Municipal de Administração da Prefeitura Municipal de Campo Mourão visam, dentre outras, prever a incorporação de novas tecnologias, facilitar e apoiar os processos de negócios, propor iniciativas, conhecimento e experiências para a inovação do negócio e proporcionar a melhoria contínua no ambiente organizacional, integrando-os à tecnologia da informação e aplicações aos projetos estruturantes, de modo que permitirá a Diretoria de TI atender às demandas resultantes da necessidade de alinhamento das ações de tecnologia da informação com o planejamento estratégico institucional.

Considerando-se o término da vigência dos contratos atuais bem como a necessidade da atualização das respectivas tecnologias em uso, com vistas a garantir maiores eficiência e segurança nos processos internos da municipalidade.

Considerando-se que com a Implantação da INFOVIA (rede em MPLS) que permitiu a interligação e criação de uma rede de computadores única para os Próprios Públicos do Município, faz-se necessária a manutenção de serviços que garantam de forma contínua a segurança das informações armazenadas, regras de navegação, política de acesso a sites da internet, software de acesso remoto, software de abertura de chamados e melhoramento do gerenciamento do ambiente, conforme descrito no instrumento convocatório.

A contratação de um conjunto de serviços que integre toda a segurança da informação conforme explicitado acima, é indispensável para que seja possível garantir a continuidade e a segurança das operações tecnológicas da Prefeitura Municipal de Campo Mourão - PR, em conformidade com as diretrizes do Governo Federal e com a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – LGPD), que estabelece regras para o tratamento de dados pessoais, bem como com o Marco Civil da Internet (Lei nº 12.965/2014).

Tratam-se de soluções de segurança e continuidade operacional que exigem estabilidade, previsibilidade e suporte técnico ininterrupto, de forma a mitigar riscos de indisponibilidade de serviços, brechas na rede de computadores e segurança, perda de dados e falhas em sistemas críticos da Administração, todos voltados para o adequado atendimento daqueles que consomem os serviços públicos da municipalidade.

3. DA JUSTIFICATIVA DE AQUISIÇÃO POR "LOTE ÚNICO"

A justificativa das necessidades para aquisição das soluções de Tecnologia da Informação para a área de ambiente e segurança da informação em conjunto mediante licitação por preço global, fundamenta-se na necessidade de **interoperabilidade, padronização técnica, economia de escala, gestão contratual eficiente e responsabilização técnica unificada**, garantindo a integridade dos dados e a continuidade dos serviços prestados a municipalidade.

Além disso, devido as especificidades dos produtos que compõem o objeto desta contratação, a municipalidade optou por estabelecer **"LOTE ÚNICO"** para a realização do certame licitatório conforme previsto no instrumento convocatório.

Na **interoperabilidade e compatibilidade técnica**, as ferramentas de segurança e de gestão de ambiente, devem funcionar de forma integrada. A aquisição separada (por itens) pode gerar "ilhas de tecnologia", dificultando-se a integração entre as ferramentas tecnológicas. Com isso, tem-se que a contratação fracionada comprometeria a interoperabilidade entre sistemas, aumentando riscos de falhas operacionais. O **"LOTE ÚNICO"** garante que todos os componentes de segurança e ambiente funcionem como um ecossistema unificado, com compatibilidade nativa.

Em se tratando de **responsabilidade técnica**, para os casos em que ocorrerem incidentes de segurança como (Ex.: vazamento de dados), ter múltiplos fornecedores neste tipo de contratação, geraria o "jogo de empurra", onde os fornecedores se acusariam mutuamente sob o aspecto de quem seria a responsabilidade pelo ocorrido ou pela solução deste, o que consequentemente acarretaria em atrasos e transtornos de toda a ordem para o destinatário final, ou seja, a municipalidade. Para que isso possa ser evitado, entende-se que o **"LOTE ÚNICO"** permite a responsabilização objetiva e única por falhas sistêmicas. O fornecedor vencedor responde pela eficiência global do ambiente, eliminando-se tais conflitos de responsabilidades técnicas.

Esta condição baseia-se também em possíveis falhas surgidas após a implantação dos serviços. Habitualmente, observa-se que após a solução instalada, em contratações desmembradas, caso ocorra alguma indisponibilidade ou mau funcionamento de um ou de vários elementos do sistema, os diferentes fornecedores passam a debater quanto à responsabilidade pelo restabelecimento do serviço, seja pela falta de diagnóstico preciso em termos de "causa da falha", seja por alegações quanto à competência contratual em intervenções nos produtos de diferentes fornecedores que integram a solução.

Na prestação dos serviços públicos, independentemente da esfera de atuação, neste caso, mais especificamente, o poder público municipal, os gestores públicos devem sempre primar em optar, em suas tomadas de decisões pela **economia de escala e custos em prol da vantajosidade econômica** para a entidade. Dessa maneira, em um processo de compra de bens e serviços de TI, adquirir um conjunto de ferramentas de um único fornecedor geraria custos menores de licença, implementação e suporte em comparação à compra fragmentada. A pesquisa de mercado indica vantajosidade econômica na aquisição conjunta, reduzindo-se custos com instalação, treinamento e integração de sistemas (Total Cost of Ownership - TCO). Ademais, a precificação realizada comprova que diversas empresas do mercado tecnológico atual, são capazes de fornecer o objeto proposto, não ocasionando restrições na concorrência ou competitividade do certame licitatório.

O parcelamento do objeto a ser licitado em diversos lotes pode acarretar prejuízos quanto à instalação, configuração, operacionalização, e garantia de toda a solução, bem como a sua manutenção, uma vez que se exige total compatibilidade entre os equipamentos da solução a ser adquirida, ou seja, a instalação deve ser uniforme.

Do ponto de vista financeiro, a subdivisão em lote impactaria em perda da economia de escala, uma vez que o fornecimento por empresas distintas traria aumento dos custos aos licitantes vencedores. Considerando o exposto, a aquisição dos serviços por menor preço global justifica-se pela vantagem econômica para a Prefeitura Municipal de Campo Mourão-PR.

Estabelecer a **padronização das ferramentas de TI**, responsáveis pela segurança de dados e informações da municipalidade, é medida comumente utilizada para que brechas de segurança sejam evitadas. Ter vários fornecedores para a solução pode criar pontos cegos no ambiente de TI. Portanto, a padronização dos equipamentos e softwares de segurança no ambiente de TI é crucial para manter a integridade dos dados, evitando-se a complexidade de gerenciar múltiplos fabricantes em um ambiente crítico.

O fornecimento dos serviços e equipamentos correlacionados, por mais de uma empresa acarretaria em elevado custo de administração e complexa coordenação entre os fornecedores, o que certamente comprometeria a qualidade e efetividade dos resultados para a Prefeitura Municipal de Campo Mourão-PR, bem como pela necessidade de garantir a segurança da informação e a proteção de dados sensíveis de Tecnologia da Informação, incluindo-se, nesse sentido, também as exigências da LGPD.
Para a **gestão contratual e operacional** deste tipo de contrato de TI, ter-se apenas um fornecedor para todos os itens da contratação, facilitaria sobremaneira, de forma que um contrato único padronizaria a gestão de ativos onde, a contratação unificada simplificaria a gestão contratual e de suporte, permitindo monitoramento centralizado de incidentes e otimizando a rotina da equipe de TI.
Além disso, a centralização da execução contratual em um único fornecedor, além do que já foi acima citado, contribui para um melhor controle de acesso às informações; redução de riscos de vazamento ou inconsistências operacionais; padronização dos procedimentos técnicos; maior rastreabilidade e responsabilização em caso de incidentes; eficiência na gestão contratual e na comunicação.
A eventual divisão do objeto em múltiplos lotes, com a consequente contratação de diversos fornecedores, ampliaria significativamente também o risco de exposição indevida de informações estratégicas e sensíveis, tais como configurações de rede, credenciais de acesso, topologias de infraestruturas, políticas de segurança e demais dados críticos do ambiente tecnológico do Município.
Por outro lado, com um fornecedor único, responsável pela integração de todos os componentes e pela manutenção da estabilidade e operacionalidade de toda a solução, a Prefeitura Municipal de Campo Mourão, ganhará em capacidade de gestão do contrato, com instrumentos de cobrança efetiva a um único mantenedor de todo o ambiente instalado.
Portanto, com esse cenário, existe um único interlocutor na gestão dos contratos e um único procedimento de chamada de assistência técnica durante o período de garantia, propiciando maior agilidade na resolução de problemas - com economicidade - advindos de falhas de equipamentos ou outros eventos relacionados ao contrato de fornecimento e prestação de serviços.
Situações emergenciais podem surgir a qualquer momento. A contratação em lote único garante a capacidade de resposta imediata a tais eventos, minimizando-se os impactos e prejuízos que poderiam advir de uma solução fragmentada. Tais fatores, em seu conjunto, contribuem para a disponibilidade, segurança e eficiência do sistema, resguardando o investimento realizado e a continuidade das operações.
"A opção pelo lote único no presente certame justifica-se, conforme Art. 23, § 1º da Lei nº 14.133/2021, pela natureza indivisível da solução de segurança e ambiente, visando a padronização, integração operacional e responsabilização técnica, garantindo a melhor relação custo-benefício e a segurança das informações corporativas."
Importante destacar que tal medida está alinhada com os princípios da eficiência, da economicidade e da segurança, previstos na legislação vigente, especialmente na Lei nº 14.133/2021, sendo a solução mais adequada ao interesse público diante da criticidade do objeto.
A opção pela licitação em um único lote justifica-se pelo fato de que os itens que compõem o objeto fazem parte de um ecossistema único de segurança, continuidade e governança da infraestrutura de TI e atendem ao mesmo fim de forma direta e/ou indireta para a garantia contínua da Segurança da Informação.
Por fim, a Súmula 247 do TCU diz ser obrigatória a admissão da adjudicação por item e não por preço global desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala. Nesse sentido, ter várias contratadas para uma mesma prestação de serviços exigiria maior dispêndio para se cuidar e zelar da coisa pública, pois poderia se perder a concentração da responsabilidade pela execução do objeto, tendo-se que designar várias pessoas para fiscalizar, o que poderia comprometer a garantia dos resultados. Isso acarretaria prejuízo para a Prefeitura Municipal de Campo Mourão, considerando todo o conjunto envolvido.

4. DESCRIÇÃO TÉCNICA DO LOTE ÚNICO (BENS E SERVIÇOS)

Itens	Descrição dos Bens e Serviços	Quantidades

1	Un.	Serviços de fornecimento de software de sistema de backup de dados e informações de arquivos digitais em ambiente virtualizado – BACKUP VIRTUAL LOCAL, incluídos: suporte e atualização de versões para 04 (quatro) servidores físicos de rede com 02 (dois) processadores cada, até 15 (quinze) máquinas virtuais e suporte a Tape Library LTO, 12 (doze) meses.	01
1.a	Serv.	Serviços de implantação e configuração de solução de backup de dados em ambiente virtualizado, pagamento único.	01
2	Serv.	Serviços de fornecimento de ferramenta de backup de dados e informações on-line operacionalizado em datacenter especializado com no mínimo 5000Gb de espaço para armazenamento de arquivos digitais em nuvem – BACKUP CLOUD, para usuários ilimitados e computadores com softwares inclusos para o período da vigência contratual de 12 (doze) meses.	01
2.a	Serv.	Serviços de implantação e configuração de ferramenta de BACKUP CLOUD, pagamento único.	01
3	Un.	Serviços de segurança, incluindo-se: 01 (um) equipamento de hardware firewall concentrador appliance UTM (Unified Threat Management) com licenciamento de firewall concentrador, ips, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para appliance de firewall de próxima geração com suporte e atualização de versões durante a vigência contratual, em comodato, 12 (doze) meses. Local: FIREWALL CONCENTRADOR PAÇO MUNICIPAL.	01
3.a	Serv.	Serviços de implantação de firewall e adaptação de rede e ambiente de segurança com MS-AD de solução de firewall concentrador, pagamento único.	01
4	Un.	Serviços de segurança, incluindo-se: 01 (um) equipamento de hardware firewall concentrador appliance UTM (Unified Threat Management) com licenciamento de firewall concentrador redundante de Alta Disponibilidade (HA), ips, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para appliance de firewall de próxima geração com suporte e atualização de versões durante a vigência contratual, em comodato, 12 (doze) meses. Local: FIREWALL CONCENTRADOR REDUNDANTE PAÇO MUNICIPAL em (HA).	01
4.a	Serv.	Serviços de implantação de firewall concentrador redundante em (HA), pagamento único.	01
5	Serv.	Serviços de segurança, incluindo-se: 01 (um) equipamento de hardware firewall de borda appliance UTM licenciamento de firewall, ips, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para appliance de firewall de próxima geração com suporte e atualização de versões, em comodato, 12 (doze) meses. Local: FIREWALL DE BORDA PARA UNIDADES COM SERVIÇOS ESSENCIAIS.	02
5.a	Serv.	Serviços de Implantação e configuração de solução de firewall de borda, pagamento único.	02
6	Serv.	Ferramenta de software de sistema para suporte remoto tipo “Help Desk” compatível com os sistemas operacionais em uso na CONTRATANTE, compreendendo: 01 (uma) licença para até 06 (seis) analistas e licenças para usuários ilimitados, usável em navegador de	01

		internet com comunicação através deste serviço, 2000 (dois mil) hosts por 12 (doze) meses.	
6.a	Serv.	Serviços de implantação, configuração e instalação de ferramenta de software de sistema para suporte remoto tipo “Help Desk”, pagamento único.	01
7	Serv.	Sistema de software de antivírus corporativo: licenças para estações de trabalho e servidores de rede, compatível com todos os sistemas operacionais legados com console de gerenciamento WEB incluso, 2000 (duas mil) licenças para estações de trabalho e 20 (vinte) licenças para servidores de rede, por 12 (doze) meses.	01
7.a	Serv.	Serviços de implantação, configuração e instalação de antivírus para todas as estações de trabalho e servidores de rede, pagamento único.	01
8	Serv.	Software para coleta e armazenamento de log’s centralizados (Syslog) em ambiente Windows para 01 (um) servidor, 12 (doze) meses.	01
8.a	Serv.	Serviços de implantação e configuração de software de coleta de log’s, pagamento único.	01
9	Serv.	Software de sistema para detecção e resposta endpoint EDR (ENDPOINT DETECTION AND RESPONSE/DETECÇÃO E RESPOSTA DE ENDPOINT) para implementar solução de segurança cibernética avançada e monitorar continuamente dispositivos finais para detectar comportamentos suspeitos, investigar ameaças em tempo real e responder automaticamente a incidentes como ransonware e malwares em equipamentos estações de trabalho da rede (computadores), 25 (vinte e cinco) equipamentos, 12 (doze) meses.	01
9.a	Serv.	Serviços de implantação, configuração e instalação de software de sistema para detecção e resposta endpoint EDR (ENDPOINT DETECTION AND RESPONSE/DETECÇÃO E RESPOSTA DE ENDPOINT), pagamento único.	01
10	Serv.	Ferramenta de software de sistema web para abertura de chamados de suporte técnico tipo “Help Desk” para solicitações internas e gerenciador de tarefas em cloud para 20 (vinte) analistas, 12 (doze) meses.	01
10.a	Serv.	Serviços de implantação, configuração e instalação de ferramenta de software de sistema web para abertura de chamados de suporte técnico tipo “Help Desk”, pagamento único.	01
11	Serv.	Serviço de implantação física e lógica de redundância de servidores de rede (AD e File Server), pagamento único sob demanda.	01
12	Serv.	Implementação de plano de Disaster Recovery/Recuperação de Desastres, englobando planejamento e diagnostico, Desenho/Projeto da solução de DR, implementação, testes, validação, documentação e treinamento, prazo de até 180 (cento e oitenta) dias, pagamento único pós-implantação.	01
12.a	Serv.	Suporte e sustentação pós-implantação de plano de Disaster Recovery/Recuperação de Desastres, pagamento único.	01
13	Serv.	Prestação de serviços continuados de processamento de dados e segurança da informação no ambiente da contratante, compreendendo atividades especializadas de monitoramento, operação assistida no ambiente de tecnologia da informação e segurança da informação, com visita técnica presencial trimestral de 04 (quatro) horas para verificação do ambiente, análise de conformidade e de vulnerabilidades e apoio técnico operacional com emissão de relatório técnico. O serviço contempla: monitoramento de segurança; criação, suporte e execução de upgrades no ambiente de virtualização, Storages, Servidores físicos,	01

		Ativos de rede, Active Directory (Ms-ad), Servidores de arquivos (file server) e Sistemas de armazenamento nas (12 meses).	

4.1 CONDIÇÕES PARA FORNECIMENTO

O fornecedor deverá entregar os itens no prazo estipulado no Termo de Referência, bem como informar a CONTRATADA sobre as intercorrências de problemas com o referido prazo.
Não será admitida qualquer subcontratação do objeto contratual.
A CONTRATADA deverá preencher todos os requisitos de regularidade jurídica, fiscal, técnica e econômico-financeira, previstos na Lei nº 14133/2021.

4.2 DESCRIÇÃO TÉCNICA (ITEM-1)
SOFTWARE DE SISTEMA DE BACKUP DE DADOS E INFORMAÇÕES DE ARQUIVOS DIGITAIS EM AMBIENTE VIRTUALIZADO – BACKUP VIRTUAL LOCAL

A solução do software do sistema de backup de dados e informações de arquivos digitais em ambiente virtualizado deverá preencher no mínimo os requisitos a seguir:

Objeto: Software de sistema de backup de dados e informações de arquivos digitais em ambiente virtualizado - BACKUP VIRTUAL LOCAL.
Produto: Serviços de fornecimento de software de sistema de backup de dados e informações de arquivos digitais em ambiente virtualizado – BACKUP VIRTUAL LOCAL, incluídos: suporte e atualização de versões para 04 (quatro) servidores físicos de rede com 02 (dois) processadores cada, até 15 (quinze) máquinas virtuais e suporte a Tape Library LTO, 12 (doze) meses.
Implantação: Serviços de implantação e configuração de solução de backup de dados em ambiente virtualizado, pagamento único.
Suporte: Atendimento de suporte por 12 (doze) meses de solução de Backup de dados em ambiente virtualizado.

Tabela 1 – Descritivos dos Itens 01 e 01.a

A solução deverá incluir funcionalidades de proteção de dados (backup e restore) para ambientes virtual e físico além de replicação de dados de backup e máquinas virtuais, integradas em uma única solução podendo ser um novo software ou atualização do atual ambiente atendendo as especificações do edital.
Deverá prover suporte para gravação em unidades de fita LTO single e tape librarys.
A solução deverá ter capacidade de gravação dos jobs de backup das máquinas virtuais diretamente para ad fitas LTO.
Possuir controle de biblioteca de fitas tipo gfs.
A solução deverá ter capacidade de restauração de objetos do diretório ativo da Microsoft de contas de usuário, senha e computador individual por exportação ldifde. Deverá também ter a capacidade de restauração de objetos de política de grupo (gpo), registros dns e objetos da partição da configuração.
A solução deverá realizar suas tarefas de proteção, recuperação e replicação das máquinas virtuais sem a necessidade de instalação de agentes nas máquinas virtuais ou nos hypervisores.
Não deverá necessitar de agentes para recuperação de arquivos, pastas e itens de aplicações.
Deverá ser capaz de realizar backup e replicação, sem interromper a atividade das máquinas virtuais e sem prejudicar sua performance, facilitando as tarefas de proteção e replicação.
Deverá realizar a recuperação instantânea de uma máquina virtual montando-a em um servidor com vmware ou hyper-v diretamente a partir de um arquivo de backup compactado e desduplicado sem necessidade, inclusive de “hidratação” dos dados gravados. A imagem do backup da vm deverá permanecer somente leitura para preservar sua integridade.
Deverá prover a recuperação de arquivos e pastas do sistema operacional hospedado sob demanda e diretamente a partir de um backup no nível de imagem, sem a etapa preliminar de extração dos discos virtuais, recuperação da máquina virtual ou conexão de rede com a máquina virtual destino da recuperação.
Para a recuperação granular, deverá suportar os seguintes sistemas de arquivos:

- Fat, fat32, ntfs e refs (Microsoft Windows);

- Ext2, ext3, ext4, reiserfs, jfs, xfs e btrfs (linux);
- Ufs, ufs2 (bsd);
- Hfs, hfs+ (mac);
- Ad-enabled nss (novell); e
- Ufs e zfs (solaris).

Deverá delegar funções e privilégios a usuários para que os mesmos criem, restaurem e monitorem seus próprios backups.
Para reduzir tanto o tráfego de rede e a área de armazenamento utilizada para o backup, deverá prover meios de otimização de dados como a desduplicação e compressão.
Deverá ser capaz de proteger, de forma indistinta uma máquina virtual completa ou discos virtuais específicos de uma máquina virtual.
Deverá possuir console de gerenciamento para administração local e remota instalada em sistema operacional Microsoft Windows.
Deverá ter a capacidade de integração através de api's dos fabricantes de infraestrutura virtualizada para a proteção de dados.
Deverá possuir a funcionalidade de recuperar dados para servidores diferentes do equipamento de origem.
Deverá ter a capacidade de realizar proteção incremental aproveitando a tecnologia de "rastreio de blocos modificados" (cbt – changed block tracking), reduzindo ao mínimo necessário, o tempo de backup e replicação.
Deverá oferecer múltiplas estratégias e opções de transporte de dados para as áreas de proteção (backup) a saber:

- Diretamente através de storage area network (san);
- Diretamente do dispositivo de armazenamento, por meio do hypervisor i/o (virtual appliance);
- Mediante uso da rede local (lan);
- Diretamente de snapshot de dispositivos de backup onde dados das vms estejam armazenados; e
- Diretamente de repositório nfs.

Deverá realizar cópias de dados de forma sintética eliminando assim a necessidade de realizar backups completos (full) periódicos e incremental permanente, o que permitirá economizar tempo e espaço.
Deverá proporcionar proteção quase contínua de dados (near-cdp), permitindo que a perda de dados seja mínima.
Deverá permitir a recuperação de mais de uma máquina virtual e/ou ponto de restauração simultâneo, permitindo assim, ter múltiplos pontos de tempo de uma ou mais máquinas virtuais.
Toda a recuperação de máquinas virtuais do repositório de backup até o dispositivo de armazenamento da produção, não deverá afetar a disponibilidade e acesso pelo usuário que deverá ser realizada sem paradas.
Deverá possuir um assistente para recuperação instantânea de arquivos de sistemas operacionais mais utilizados como Windows e Linux.
Deverá possuir um índice (catálogo) de todos os arquivos protegidos pela solução de modo a facilitar pesquisas para encontrar e restaurar um arquivo sem a necessidade de saber sua localização exata.
Deverá assegurar a consistência de aplicações transacionais de forma automática por meio da integração com Microsoft VSS, dentro de sistemas operacionais Windows.
Deverá permitir notificações por e-mail, snmp ou através dos atributos da máquina virtual do resultado da execução de suas tarefas.
Deverá permitir a truncagem e transporte agendado de logs transacionais (transaction logs) para máquinas virtuais com Microsoft Exchange, Sql server e Oracle, sem a instalação de agentes na máquina virtual.
Deverá possuir ferramenta para recuperação granular e consistente, sem necessidade da instalação de agentes adicionais para o ambiente virtualizado principalmente para as seguintes aplicações: microsoft active directory 2016 e superiores, microsoft sql 2019 e superiores, oracle database 11g e superiores.
O espaço livre em cada datastore (lun) deverá ser monitorado pela solução de forma a se evitar a criação de snapshots caso não haja espaço livre suficiente para a operação.

Deverá oferecer arquivamento em fita, suportando vtl (virtual tape libraries), biblioteca de fitas e drives lto5 ou superior, possibilitando a gravação paralela em múltiplos drives, além da criação de pools de mídia globais e pools de mídia gfs, sem a necessidade de licenciamento individual por drive.
Deverá suportar o uso de fitas do tipo worm (write once, read many).
Possibilitar o arquivamento em fita com os dados migrados do repositório em disco mantendo a desduplicação e compressão, ou seja, sem que aconteça a reidratação dos dados.
Deverá proporcionar cópias de backup com implementação de políticas de retenção com o objetivo de manter uma cópia dos arquivos de backup em caso de desastre.
Deverá possuir recurso que possibilite a exclusão de blocos “sujos” (dados apagados, swap, etc.) durante a execução do backup, de modo a diminuir a quantidade de dados trafegados/armazenados.
Deverá possuir recurso que monitore os snapshots criados durante a execução do backup, bem como rotinas que evitem que os snapshots não sejam deletados ou a não consolidação dos discos virtuais, a fim de evitar snapshots órfãos ou qualquer outro comportamento similar ao término das atividades de proteção.
Deverá permitir a configuração de um nível máximo aceitável de latência para os datastores de produção de forma a garantir as atividades de backup e replicação sem afetar as cargas de trabalho da produção.
Deverá oferecer a possibilidade de armazenar os arquivos de backup de forma criptografada, com algoritmo mínimo aes-256 bits, sendo possível ativar e desativar tal operação, assim como assegurar o trânsito da informação criptografada.
Deverá possuir meios de proteção da chave de criptografia.
A solução deverá realizar a replicação de dados de backup e máquinas virtuais para outras localidades como dispositivos de armazenamento secundário, datacenter secundário e/ou nuvem aumentando a disponibilidade do ambiente em caso de desastre.
Deverá permitir recuperar dados do sistema de arquivos ou itens de aplicação de forma granular diretamente das réplicas realizadas.
Deverá permitir a seleção de um destino de armazenamento do backup em um provedor de serviços em nuvem.
Deverá permitir a seleção de um destino para a réplica dos dados que poderá ser em um provedor de serviços em nuvem.
A solução deverá possuir funcionalidade para gerar um repositório global para os dados de backup que possa incluir vários e distintos dispositivos de armazenamento como se fosse único além de permitir o crescimento do mesmo de forma transparente para as tarefas de backup.
Integração com appliances de desduplicação abaixo:

- Dell EMC Data Domain; e
- Hpe storeonce.

Possuir integração com armazenamento de objetos compatíveis com S3 como amazon S3, Azure blob storage, IBM object cloud storage e qualquer outro dispositivo de armazenamento local compatível com S3.
Realizar arquivamento dos dados de backup nos dispositivos e locais de armazenamento de objetos compatíveis com S3.
Em caso de desastre, deverá ser possível realizar a recuperação dos dados diretamente do arquivamento em S3.
Capacidade de integração ao Oracle para manipulação durante o backup dos LOGs com arquivamento ou deleção seletiva por hora ou tamanho.
Capacidade de integração com o SQL Server para truncagem de logs.
Possuir recursos de aceleração de réplicas de máquinas virtuais em redes WAN para otimização de transferência de dados em redes de baixa velocidade.
Deverá ser ofertada a versão mais atual do software de backup, liberada oficialmente pelo fabricante do software. Caso haja necessidade, por razões de compatibilidade com os demais componentes de hardware e software do ambiente de backup, a contratante se reserva o direito de utilizar a versão do software imediatamente anterior à versão mais atual, sem nenhum ônus adicional para a contratante.
Deverá integrar uma solução unificada de monitoração de ambientes virtualizados, com fornecimento de relatórios capazes de apresentar informações do tipo:

- Relatórios que permitam o planejamento de capacidade da infraestrutura virtual e de backup;
- Relatórios que permitam determinar a ineficiência dos recursos em utilização;
- Relatórios que facilitem a visibilidade de tendências negativas e anomalias;
- Relatórios que possibilitem billing dos backups e réplicas realizadas;
- Quadros de controle claros, apresentáveis e integráveis em sites web; e
- Envio automático e programado de relatórios de auditoria para operações de recuperação e modificação de políticas de backup e replicação.

Deverá permitir a criação de relatórios customizados para análise da infraestrutura virtual e da infraestrutura de proteção de dados (backup).
Deve ter a capacidade de gerar segregação de acesso de acordo com o perfil do usuário, para monitorar a infraestrutura conectada à plataforma.
Deverá oferecer a capacidade de relatar a conformidade com as políticas de proteção e disponibilidade de dados de acordo com os parâmetros definidos.
Deverá ter uma base de conhecimento integrada nos alarmes, embora também deva apoiar a personalização dos alarmes e descrições da base de conhecimento.
A plataforma deverá fornecer um mecanismo de diagnóstico inteligente que analise os logs da solução para identificar proativamente e alertar sobre problemas de infraestrutura.
A plataforma deve conter relatórios inteligentes para verificar se a infraestrutura virtual está pronta para executar backups de acordo com boas práticas. Deve conter recomendações para a correção de problemas encontrados.
A plataforma deve conter relatórios inteligentes para a revisão após a implementação da solução de backup, para validar se ela está em conformidade com as boas práticas de implementação e configuração.
A plataforma deve fornecer monitoramento das aplicações, isto é, conhecer o status de integridade dos serviços e aplicações encontradas nas máquinas virtuais da plataforma.
Deverá possibilitar o envio de notificações de alarme quando um processo de recuperação for iniciado.
Deverá possuir suporte para relatórios de backup de agentes físicos da solução.
A plataforma deverá conter relatórios genéricos, tais como:

- Histórico das tarefas de backup;
- Relatórios de máquinas protegidas, físicas e virtuais;
- Relatório de atividade de recuperação de dados;
- Relatório de verificação de recuperabilidade;
- Último status das tarefas de backup;
- Resumo dos alarmes de backup;
- Relatório de configuração da infraestrutura virtual;
- Relatório de backup em fitas;
- Relatório de máquinas em conformidade; e
- Inventário de backup.

Além disso, deve conter relatórios avançados, como:

- Auditoria de alterações de objeto da infraestrutura virtual
- Auditoria de alterações da infraestrutura de backup;
- Modelagem em caso de falhas;
- Capacidade planejamento da infraestrutura virtual;
- Relatórios para otimização de infraestrutura virtual;
- Crescimento de máquinas;
- Capacidade planejamento de infraestrutura de backup;
- Avaliação de desempenho do armazenamento de dados;
- Avaliação de configuração de máquinas virtuais; e
- Estimativa da taxa de alteração de máquinas virtuais.

A plataforma deverá permitir visualizar dashboards da plataforma virtual e de backup, além de prover um mapa (heatmap) dos recursos utilizados pela infraestrutura de backup, a fim de permitir a análise de consumo dos recursos envolvidos.

O suporte técnico deverá ser prestado em regime 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, com prazo máximo de atendimento presencial em até 06 (seis) horas após a abertura de chamado para incidentes críticos conforme exposto nas **Tabelas 14 e 15** para questões referentes à instalação, configuração, manutenção, administração e atualização de todo o ambiente de backup a ser utilizada pelo contratante, em sua versão atual e posteriores, envolvendo as seguintes atividades:

- Suporte dos softwares cliente e servidor de backup centralizado.
- Suporte a rotinas operacionais de backup.
- Disponibilizar atualização de versões, releases e patches aplicados em todo o ambiente de backup, com o devido histórico.
- Possuir agentes de backup para ambientes de S.O's Windows e Linux para backup de dados dos discos locais que não fazem parte do hypervisor como hd externos, drives iscsi e outros.

Ao término da implantação, instalação e realização de todas as configurações necessárias para o pleno funcionamento da ferramenta, a empresa contratada deverá realizar treinamento presencial destinado à reciclagem de conhecimentos, atualização técnica e capacitação de novos integrantes da equipe. O treinamento deverá ter duração mínima de 04 (quatro) horas e será realizado nas dependências da contratante, voltado à equipe de Tecnologia da Informação, contemplando, no mínimo, os procedimentos de instalação, administração e utilização da solução. O horário de realização será definido pela Diretoria de Tecnologia da Informação (DIRTI), podendo, quando necessário, ser estabelecido que a prestação do serviço ocorra fora do horário de expediente do órgão.

Como referência técnica para fornecimento deste item, informamos, que atualmente a municipalidade, através da Diretoria de TI, faz uso da ferramenta "**VEEAM BACKUP ESSENTIALS UNIVERSAL LICENCE COM O PACOTE ENTERPRISE PLUS EDITION)**" para a realização dos serviços de Backups. Informamos ainda que a prefeitura, através da Diretoria de TI, possui armazenada extensa biblioteca de dados históricos de Backups com cobertura sobre um período de vários anos, o que ao longo do tempo estabeleceu um padrão de usabilidade da ferramenta atual, o que tem garantindo a eficiência e a segurança adequadas ao lidar-se com o gerenciamento das cópias de segurança de dados e informações em Backups. Dessa maneira, informa-se que a ferramenta atual já descrita deverá ser mantida com a mesma especificação técnica mínima exigida de modelo/ marca para a nova contratação de forma que, tecnicamente possam ser garantidas as restaurações de cópias de dados e informações legados da biblioteca histórica.

4.3 DESCRIÇÃO TÉCNICA DO (ITEM-2)
SERVIÇO PARA FORNECIMENTO DE SISTEMA DE BACKUP DE DADOS E INFORMAÇÕES DE ARQUIVOS DIGITAIS EM NUVEM (BACKUP CLOUD)

A solução do serviço para sistema de backup de dados e informações de arquivos digitais em nuvem (internet) compreenderá bens e serviços, que deverão ser fornecidos pela contratada com os devidos licenciamentos e atualizações de versões contínuas durante a vigência contratual.

Objeto: Serviço para fornecimento de sistema de backup de dados e informações de arquivos digitais em nuvem (Backup Cloud).
Produto: Serviços de fornecimento de ferramenta de backup de dados e informações on-line operacionalizado em datacenter especializado com no mínimo 5000Gb de espaço para armazenamento de arquivos digitais em nuvem – BACKUP CLOUD, para usuários ilimitados e computadores com softwares inclusos para o período da vigência contratual de 12 (doze) meses.
Implantação: Serviços de implantação e configuração de ferramenta de BACKUP CLOUD, pagamento único.
Suporte: Suporte 12 (doze) meses de solução de Backup Cloud de dados em arquivos digitais em nuvem.

Tabela 2 – Descritivos dos Itens 02 e 02a

A solução do serviço para sistema de backup de dados e informações de arquivos digitais em nuvem (internet) deverá cumprir os requisitos a seguir:

- Permitir o backup de ilimitadas estações de trabalho e servidores em uma única conta, com cada computador tendo seu backup em pasta separada;
- Possuir software cliente de backup multiplataforma (windows/linux/macos);
- Possuir software para backup de dispositivos moveis IOS e Androiod;
- Possuir instalador msi para instalação em múltiplos computadores via microsoft active directory group policy;
- Permitir a instalação do software de backup sem custos para ilimitadas estações de trabalho usando a mesma conta de backup;
- Possuir capacidade de Disaster Recovery/ Recuperação de Desastres (DR) para réplica completa de dados críticos para outro local físico;
- O software cliente deverá ter capacidade para backup e restauração do diretório ativo da Microsoft (Active Directory) atualmente em uso pelo contratante;
- Capacidade de realizar uma segunda cópia em Storage local dos dados das estações de trabalho;
- Possuir capacidade de exclusão de pastas e tipos de arquivo, backup de open files, controle do uso máximo de banda durante as tarefas de backup e autenticação com conta específica para backup de dados em rede;
- O software cliente deve possibilitar o recurso de sincronização entre dispositivos, copiando determinados dados em uma pasta especifica entre os computadores com os softwares instalados a partir de uma mesma conta;
- Possuir agendamento de tarefas com notificação de sucesso ou falha no backup via e-mail com servidor de e-mail próprio;
- Possuir capacidade de “snapshot” para recuperar dados no tempo para proteção contra ransonwares;
- Usar chave de criptografia de dados de 256 bits podendo ser definida chave privada única com acesso apenas ao cliente e transferência de dados entre o sistema de cloud em SSL de 128bits;
- Permitir o backup de no mínimo 5000Gb de dados;
- Acesso aos dados de backup via software cliente ou por navegador web https para restauração e manutenção de dados, como cópia, movimentação pesquisa e exclusão;
- Possuir capacidade de versionamento para até 10 (dez) versões do mesmo arquivo, com datas diferentes sem consumir a franquia de espaço contratada;
- A solução deve permitir a transferência de dados de backup e restauração (download e upload) ilimitados sem cobrança de valores adicionais; e
- Prever a possibilidade de aumento do espaço para o backup, quando solicitado em até 24 (vinte e quatro) horas após a formalização do pedido pela contratante.

O suporte técnico deverá ser prestado em regime 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, com prazo máximo de atendimento presencial em até 06 (seis) horas após a abertura de chamado para incidentes críticos conforme exposto nas **Tabelas 14 e 15**, para as questões referentes à instalação, configuração, manutenção, administração e atualização de todo o ambiente de backup a ser utilizada pelo contratante.

O serviço de instalação do ambiente deverá ser executado nas instalações da licitante de forma presencial.

Ao término da implantação, instalação e realização de todas as configurações necessárias para o pleno funcionamento da ferramenta, a empresa contratada deverá realizar treinamento presencial destinado à reciclagem de conhecimentos, atualização técnica e capacitação de novos integrantes da equipe. O treinamento deverá ter duração mínima de 04 (quatro) horas e será realizado nas dependências da contratante, voltado à equipe de Tecnologia da Informação, contemplando, no mínimo, os procedimentos de instalação, administração e utilização da solução. O horário de realização será definido pela Diretoria de Tecnologia da Informação (DIRTI), podendo, quando necessário, ser estabelecido que a prestação do serviço ocorra fora do horário de expediente do órgão.

4.4 DESCRIÇÃO TÉCNICA DO (ITEM-3)
FIREWALL CONCENTRADOR DO PAÇO MUNICIPAL

A segurança corporativa a ser implantada através do serviço de segurança para controle de ameaças virtuais via “appliance utm firewall concentrador” compreenderá: solução de segurança de rede, endpoint e criptografia com a utilização de bens e serviços, que deverão ser fornecidos pela contratada com os devidos licenciamentos e atualizações de versões contínuas durante a vigência contratual.

Objeto: Equipamento e serviços para implantação de segurança virtual na rede de computadores para soluções de serviços de segurança para controle de ameaças virtuais na modalidade “Appliance do tipo UTM (Unified Threat Management) Firewall concentrador” em comodato – Firewall Concentrador Paço Municipal.
Produto: Serviços de segurança, incluindo-se: 01 (um) equipamento de hardware firewall concentrador appliance UTM (Unified Threat Management) com licenciamento de firewall concentrador, ips, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para appliance de firewall de próxima geração com suporte e atualização de versões durante a vigência contratual, em comodato, 12 (doze) meses. Local: FIREWALL CONCENTRADOR PAÇO MUNICIPAL.
Implantação: Serviços de implantação de firewall e adaptação de rede e ambiente de segurança com MS-AD de solução de firewall concentrador, pagamento único.
Suporte: Suporte por 12 (doze) meses.

Tabela 3 – Descritivos dos Itens 03 e 03.a

A solução de serviços de segurança para controle de ameaças virtuais “appliance utm firewall concentrador” deverá cumprir os requisitos a seguir:

- Desempenho mínimo de 40Gbps de throughput para firewall;
- Desempenho mínimo de 13Gbps de throughput de ips;
- Desempenho mínimo de 2,5Gbps de throughput de Threat Protection;
- Desempenho mínimo de 3Gbps de Inspeção TLS/SSL;
- Desempenho mínimo de 6,0Gbps de throughput de vpn;
- Suporte a, no mínimo, 13.000.000 de conexões simultâneas;
- Suporte a, no mínimo, 250.000 novas conexões por segundo;
- Possuir o número irrestrito quanto ao máximo de usuários licenciados;
- Possuir armazenamento interno de no mínimo 240gb para sistema operacional, quarentena local, logs e relatórios;
- Possuir no mínimo 16gb de memória ram;
- Possuir no mínimo oito interfaces de rede 1000base-tx sendo duas com o recurso “lan bypass” que permite a passagem livre de tráfego em caso de falha do hardware;
- Possuir no mínimo duas interfaces SFP fiber e duas interface SFP 10Gb fiber;
- Possuir uma interface do tipo console ou similar;
- Possuir uma saída vga/hdmi ou similar e três portas usb 2.0;
- Entrada para segunda fonte redundante;
- Modulo de expansão com suporte a 08 portas gbe de cobre ou fiber ou 04 portas 10 gbe sfp;
- Appliance de proteção de rede com funcionalidades de next generation firewall (ngfw) e console de gerência, monitoração e logs;
- Por funcionalidades de next generation firewall (ngfw) entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- As funcionalidades de proteção de rede que compõe a plataforma de segurança podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
- A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 07;
- O software deverá ser fornecido em sua versão mais atualizada;
- O HA (modo de alta disponibilidade) deve suportar o uso de dois equipamentos em modo ativo-passivo ou modo ativo-ativo e deve possibilitar monitoração de falha de link;
- Uma interface completa de comando de linha (cli command-line-interface) deverá ser acessível através da interface gráfica e via porta serial;
- A atualização de software deverá enviar avisos de atualização automáticos;

- O sistema de objetos deverá permitir a definição de redes, serviços, hosts períodos de tempos, usuários e grupos, clientes e servidores;
- O backup e o reestabelecimento de configuração deverão ser feitos localmente via ftp ou email com frequência diária, semanal ou mensal, podendo também ser realizado por demanda;
- As notificações deverão ser realizadas via email e snmp;
- Suportar snmp e netflow;
- O firewall deverá ser stateful, com inspeção profunda de pacotes (deep packet inspection);
- As zonas deverão ser divididas pelo menos em wan, lan e dmz, sendo necessário que as zonas lan e dmz possam ser customizáveis;
- As políticas de nat deverão ser customizáveis para cada regra;
- A proteção contra flood deverá ter proteção contra dos (denial of service), ddos (distributed dos) e bloqueio de portscan;
- Proteção contra anti-spoofing;
- Suportar ipv4 e ipv6;
- Ipv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e ipv6 rapid deployment (6rd) de acordo com a rfc 5969;
- Suporte aos roteamentos estáticos, dinâmico (rip, bgp e ospf) e multicast (pim-sm e igmp);
- Deve suportar a definição de vlans no firewall conforme padrão ieee 802.1q e tagging de vlan;
- O balanceamento de link wan deve permitir múltiplas conexões de links internet, checagem automática do estado de links, failover automático e balanceamento por peso;
- A solução deverá permitir port-aggregation de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces;
- A solução deverá permitir configurar os serviços de dns, dynamic dns, dhcp e ntp;
- O traffic shapping (qos) deverá ser baseado em rede ou usuário;
- A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas;
- Deve possuir otimização em tempo real de voz sobre ip;
- Deve implementar o protocolo de negociação link aggregation control protocol (lacp);
- Possuir plataforma next-generation firewall (ngfw) para proteção de informação perimetral e de rede interna que inclui stateful firewall com capacidade para operar em alta disponibilidade (ha) em modo ativo- passivo ou ativo-ativo para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (qos), vpn ipsec e ssl, ips, prevenção contra ameaças de vírus, malwares, filtro de url, criptografia de email, inspeção de tráfego criptografado e proteção de firewall de aplicação web;
- Deverá ser fornecida console de gerenciamento dos equipamentos e centralização de logs em cloud;
- Deverão ser fornecidas as licenças para atualização de todos os componentes de software, vacinas de antivírus / malwares, endpoints, softwares de criptografia de armazenamento em nuvem e assinaturas de ips, filtro de conteúdo web, controle de aplicações e proteção de firewall de aplicação web sem custo adicional, pelo período contratual;
- Por cada appliance físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento;
- Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
- Por alta disponibilidade (HA), entende-se que a solução é composta ao menos por dois appliances, licenciados para funcionamento em redundância podendo ser solicitados a qualquer tempo sem troca do hardware atualmente instalado, podendo ser contratado o segundo hardware a qualquer tempo dentro do período de vida útil de vendas do fabricante da solução;
- Cada appliance deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos; e
- O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

4.4.1 CONTROLE POR POLÍTICAS DE FIREWALL

- Deve suportar controles por: porta e protocolos tcp/udp, origem/destino e identificação de usuários;
- O controle de políticas deverá monitorar as políticas de redes, usuários, grupos e tempo, bem como identificar as regras não-utilizadas, desabilitadas, modificadas e novas políticas;
- As políticas deverão ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas, redes e por tipos de serviços;
- Controle de políticas por usuários, grupos de usuários, ips, redes e zonas de segurança;
- Controle de políticas por países via localização por ip;
- Suporte a objetos e regras ipv6;
- Suporte a objetos e regras multicast;
- Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de ips, antivírus, anti-malware e firewall de proteção web (waf) integrados no próprio appliance de firewall ou entregue em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
- Deve realizar a inspeção profunda de pacotes (dpi deep packet inspection) para prevenção de intrusão (ips) e deve incluir assinaturas de prevenção de intrusão (ips);
- As assinaturas de prevenção de intrusão (ips) devem ser customizadas;
- Exceções por usuário, grupo de usuários, ip de origem ou de destino devem ser possíveis nas regras;
- Deve suportar granularidade nas políticas de ips antivírus e anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens, com customização completa;
- A proteção anti-malware deverá bloquear todas as formas de vírus, web malwares, trojans e spyware em http e https, ftp e web-emails;
- A proteção anti-malware deverá realizar a proteção com emulação Javascript;
- Deve ter proteção em tempo real contra novas ameaças criadas;
- Deve possuir pelo menos duas engines de antivírus independentes e de diferentes fabricantes para a detecção de malware, podendo ser configuradas isoladamente ou simultaneamente;
- Deve permitir o bloqueio de vulnerabilidades;
- Deve permitir o bloqueio de exploits conhecidos;
- Deve detectar e bloquear o tráfego de rede que busque acesso a contact command e servidores de controle utilizando múltiplas camadas de dns, afc e firewall;
- Deve incluir proteção contra-ataques de negação de serviços;
- Ser imune e capaz de impedir ataques básicos como: syn flood, icmp flood, udp flood, etc;
- Suportar bloqueio de arquivos por tipo;
- Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- Os eventos devem identificar o país de onde partiu a ameaça;
- Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas de segurança considerando uma das opções ou a combinação de todas elas: usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de ips, sendo essas políticas por usuários, grupos de usuários, origem, destino, zonas de segurança;
- O firewall deve ter capacidade para contratação futura de módulo de proteção de firewall web (waf) que deverá ter a função de reverse proxy, com a função de url hardening realizando deep-linking e prevenção dos ataques de path traversal ou directory traversal;
- O firewall de aplicação web (waf) deverá realizar cookie signing com assinaturas digitais, roteamento baseado por caminho, autenticações reversas e básicas para acesso do servidor;
- O firewall de aplicação web (waf) deverá possuir a função de balanceamento de carga de visitantes por múltiplos servidores, com a possibilidade de modificação dos parâmetros de desempenho do waf e

permissão e bloqueio de ranges de ip. Proteção pelo menos contra os seguintes ataques, mas não limitado a: sql injection e cross-site scripting;

- Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 07, utilizando portas padrões (80 e 443), portas não padrões, port hopping e túnel através de tráfego ssl encriptado;
- Reconhecer pelo menos 2.300 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, serviços de rede, voip, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de softwares;
- Reconhecer pelo menos as seguintes aplicações: 4shared file transfer, active directory/smb, citrix ica, dhcp protocol, dropbox download, easy proxy, facebook graph api, firefox update, freegate proxy, freevpn proxy, gmail video, chat streaming, gmail webchat, gmail webmail, gmail-way2sms webmail, gtalk messenger, gtalk messenger file transfer, gtalk-way2sms, http tunnel proxy, httport proxy, logmein remote access, ntp, oracle database, rar file download, redtube streaming, rpc over http proxy, skydrive, skype, skype services, skyzip, snmp trap, teamviewer conferencing e file transfer, tor proxy, torrent clients p2p, ultrasurf proxy, ultravpn, vnc remote access, vnc web remote access, whatsapp, whatsapp file transfer e whatsapp web;
- Deve realizar o escaneamento e controle de micro app incluindo, mas não limitado a: facebook (applications, chat, commenting, events, games, like plugin, message, pics download e upload, plugin, post attachment, posting, questions, status update, video chat, video playback, video upload, website), freegate proxy, gmail (android application, attachment), google drive (base, file download, file upload), google earth application, google plus, linkedin (company search, compose webmail, job search, mail inbox, status update), skydrive file upload e download, twitter (message, status update, upload, website), yahoo (webmail, webmail file attach) e youtube (video search, video streaming, upload, website);
- O escaneamento de micro app deverá ser habilitado via console gráfica (gui) e via comando de linha (cli);
- Para tráfego criptografado ssl, deve decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- Atualizar a base de assinaturas de aplicações automaticamente;
- Reconhecer aplicações em ipv6;
- Limitar a banda usada por aplicações (traffic shaping);
- Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft active directory, sem a necessidade de instalação de agente no domain controller, nem nas estações dos usuários;
- Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuírem acesso a estes aplicativos devem ter a utilização bloqueada;
- Implementar controle e proteção na web;
- Deve permitir especificar política de navegação web por tempo, ou seja, a definição de regras para um determinado dia da semana e horário de início e fim, permitindo a adição de múltiplos dias e horários na mesma definição de política por tempo. Esta regra de tempo pode ser recorrente ou em uma única vez;
- Deve ser possível a criação de políticas por usuários, grupos de usuários, ips e redes;
- Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais urls através da integração com serviços de diretório, autenticação via ldap, active directory, radius, e-directory e base de dados local;
- Permitir popular todos os logs de url com as informações dos usuários conforme descrito na integração com serviços de diretório;
- Possuir pelo menos 80 categorias de urls;
- Suportar a capacidade de criação de políticas baseadas no controle por url e categoria de url;

- Deve ser capaz de forçar o uso da opção safe search em sites de busca;
- Deve ser capaz de categorizar as urls a partir de base ou cache de urls locais ou através de consultas dinâmicas na nuvem do fabricante, independentemente do método de classificação a categorização não deve causar atraso na comunicação visível ao usuário;
- Suportar a criação categorias de urls customizadas;
- Suportar a opção de bloqueio de categoria http e liberação da categoria apenas em https;
- Permitir a customização de página de bloqueio;
- Suportar a inclusão nos logs do produto de informações das atividades dos usuários;
- Deverão salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado;
- Deve realizar caching do conteúdo web;
- Deve realizar filtragem por mime-type, extensão e tipos de conteúdo ativos, tais como, mas não limitado a: activex, applets e cookies;
- Identificação de usuários;
- Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticando via ldap, active directory, radius, edirectory, tacacs+ e via base de dados local, para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (captive portal);
- Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço ip em ambientes citrix e Microsoft terminal server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- Deve permitir autenticação em modos: transparente, autenticação proxy (ntlm e kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, Mac OS x e Linux 32/64;
- Deve possuir a autenticação single sign-on para, pelo menos, os sistemas de diretórios active directory e edirectory;
- Deve possuir portal do usuário para que os usuários tenham acesso ao uso de internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução;
- Qualidade de serviço – QOS, com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações;
- A solução deverá suportar traffic shaping (qos) e a criação de políticas baseadas em categoria web e aplicação por: endereço de origem. endereço de destino. usuário e grupo do ldap/ad;
- Deve ser configurado o limite e a garantia de upload/download, bem como ser priorizado o tráfego total e bitrate de modo individual ou compartilhado;
- Suportar priorização real-time de protocolos de voz (voip);
- Redes virtuais privadas – VPN;
- Suportar vpn site-to-site e cliente-to-site;
- Suportar ipsec vpn;
- Suportar acesso remoto ssl, ipsec e vpn cliente para android e iphone/ipad;
- Deve ser disponibilizado o acesso remoto ilimitado, até o limite suportado de túneis vpn pelo equipamento, sem a necessidade de aquisição de novas licenças e sem qualquer custo adicional para o licenciamento de clientes para estações Windows;
- Deve possuir um portal encriptado baseado em html5 para suporte pelo menos a: rdp, http, https, ssh, telnet e vnc, sem a necessidade de instalação de clientes vpn nas estações de acesso;
- A vpn ipsec deve suportar: des e 3des, autenticação md5 e sha-1, diffie-hellman group 1, group 2, group 5 e group 14, algoritmo internet key exchange (ike), aes 128, 192 e 256 (advanced encryption standard), sha 256, 384 e 512, autenticação via certificado pki (x.509) e pre-shared key (psk);
- Deve possuir interoperabilidade com os seguintes fabricantes: cisco, check point, dell sonicwall, fortinet, huawei, juniper, palo alto networks e sophos;

- Deve permitir criar políticas de controle de aplicações, ips, antivírus, anti-malware e filtro de url para tráfego dos clientes remotos conectados na vpn ssl;
- Suportar autenticação via ad/ldap, token e base de usuários local;
- Permitir estabelecer um túnel vpn com uma solução de autenticação via ldap, active directory, radius, edirectory, tacacs+ e via base de dados local;
- Gerência administrativa centralizada;
- Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos através de uma única console central, com administração de privilégios e funções;
- O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar S. pelos equipamentos da plataforma de segurança;
- Estar licenciada para gerenciar as soluções de firewall de próxima geração;
- Deve ser centralizada a gerência de todas as políticas do firewall e configurações para as soluções de firewall de próxima geração, sem necessidade de acesso direto aos equipamentos.
- Deve possuir indicadores do estado de equipamentos e rede;
- Deve emitir alertas baseados em thresholds customizáveis, incluindo também alertas de expiração de subscrição, mudança de status de gateways, uso excessivo de disco, eventos atp, ips, ameaças de vírus, navegação, entre outros;
- Deve permitir a criação de grupos de equipamentos por nome, modelo, firmware e regiões.
- Deve ter controle de privilégios administrativos, com granularidade de funções (vpn admin, app e web admin, ips admin, etc.);
- Deve ter controle das alterações feitas por usuários administrativos, comparar diferentes versões de configurações e realizar o processo de rollback de configurações para mudanças indesejadas;
- Deve ter logs de auditoria de uso administrativo e atividades realizadas nos equipamentos;
- Deve ter integração com a solução de logs e relatórios, habilitando o provisionamento automático de novos equipamentos e a sincronização dos administradores da centralização da gerência com a centralização de logs e relatórios;
- Gerência de logs e relatórios centralizados;
- Deve possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução através de uma única console central;
- Estar licenciada para gerenciar as soluções de firewall de próxima geração;
- Devem ser fornecidas soluções em cloud desde que obedeçam a todos os requisitos desta especificação, com armazenamento mínimo de 07 (sete) dias sem limite de volume e expansível até 1TB de dados;
- Deverá prover relatórios baseados em usuários, com visibilidade sobre acesso a aplicações, navegação, eventos atp, downloads e consumo de banda, independente em qual rede ou ip o usuário esteja se conectando;
- Devem possibilitar a identificação de ataques como a identificação de malware identificados pelos eventos atp, usuários suspeitos, tráfegos anômalos incluindo tráfego icmp e consumo não-usual de banda;
- Deve conter relatórios pré-configurados, pelo menos de: aplicações, navegação, web server (waf), ips, atp e vpn;
- Deve fornecer relatórios históricos para análises de mudanças e comportamentos;
- Deve conter customizações dos relatórios para inserção de logotipos próprios;
- Deve fornecer relatórios de compliance, hipaa e pci;
- Deve permitir a exportação via pdf ou excel;
- Deve fornecer relatórios sobre os acessos de procura no google, yahoo, bing e wikipedia;
- Deve fornecer relatórios de tendências;
- Deve fornecer logs em tempo real, de auditoria e arquivados;
- Deve possuir mecanismo de procura de logs arquivados;
- Deve ter acesso baseado em web com controles administrativos distintos;
- Instalação, suporte e monitoramento; e
- O equipamento deverá ser compatível com os já existentes de modo a possibilitar o gerenciamento central de todos eles.

A empresa vencedora deverá fazer a instalação e configuração do diretório ativo da Microsoft (ms ad) com configuração de contas para todos os usuários de forma presencial usando gpo por setor, migrando os dados dos perfis dos computadores atuais.
O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de suporte ou vida.
A segurança corporativa a ser implantada através do equipamento de segurança firewall de próxima geração deverá ser fornecidos pela contratada com os devidos licenciamentos e atualizações de versões contínuas durante a vigência contratual em comodato.
O serviço de instalação do ambiente deverá ser executado presencialmente nas dependências da contratante por, no mínimo, dois profissionais certificados pelo fabricante da solução. Todas as atividades de configuração, bem como a migração e/ou criação de regras, deverão ser realizadas de forma a não interferir no funcionamento da infraestrutura atual da Prefeitura, considerando que o equipamento a ser implantado é responsável pelo funcionamento da rede que atende mais de 100 (cem) prédios municipais.
A entrada definitiva em operação do equipamento deverá ocorrer somente após a completa validação e realização de testes pela Contratada que comprovem o seu pleno funcionamento. Eventuais procedimentos que possam ocasionar pausa ou interrupção dos serviços deverão ser executados fora do horário normal de atendimento do Município em data e hora a ser definida pela Diretoria de Tecnologia da Informação, sendo inclusive realizado preferencialmente em finais de semana, de modo a garantir o mínimo impacto possível na infraestrutura tecnológica e na continuidade dos serviços públicos.
Ao término da implantação, instalação e realização de todas as configurações necessárias para o pleno funcionamento do Firewall, a empresa contratada deverá realizar treinamento presencial destinado à reciclagem de conhecimentos, atualização técnica e capacitação de novos integrantes da equipe, por profissional certificado pelo fabricante. O treinamento deverá ter duração mínima de 08 (oito) horas e será realizado obrigatoriamente nas dependências da contratante, voltado à equipe de Tecnologia da Informação, contemplando, no mínimo, os procedimentos de instalação, administração e utilização da solução. O horário de realização será definido pela Diretoria de Tecnologia da Informação (DIRTI), podendo, quando necessário, ser estabelecido que a prestação do serviço ocorra fora do horário de expediente do órgão. A Transferência de conhecimento deverá ser realizada por profissional certificado pelo fabricante da solução, incluindo-se técnicas de execução, gerenciamento e monitoramento.
Como referência técnica para fornecimento deste **Item-3**, informamos que, atualmente a municipalidade, através da Diretoria de TI, faz uso da solução: 01 (um) equipamento de hardware firewall concentrador appliance UTM (Unified Threat Management) com licenciamento de firewall concentrador, ips, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para appliance de firewall de próxima geração com suporte e atualização de versões durante a vigência contratual, instalado no local como **FIREWALL CONCENTRADOR PAÇO MUNICIPAL** para a realização da segurança da rede de computadores em mais de 100 (cem) prédios públicos, esta solução, tem garantido a esta municipalidade, eficiência e constância no gerenciamento da segurança contra invasões a estas redes ao longo dos anos, estabelecendo-se um padrão de usabilidade. Dessa maneira, informa-se que a solução atual já descrita deverá ser mantida com a mesma especificação técnica mínima exigida de modelo/ marca da **SOPHOS LTD**.
O suporte técnico deverá ser prestado em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, com prazo máximo de atendimento presencial em até 06 (seis) horas após a abertura de chamado para incidentes críticos conforme exposto nas **Tabelas 14 e 15.**

4.5 DESCRIÇÃO TÉCNICA DO (ITEM-4)
FIREWALL CONCENTRADOR REDUNDANTE PAÇO MUNICIPAL EM (HA)

A solução de serviços de segurança para controle de ameaças virtuais “appliance utm firewall concentrador” para uso como segundo firewall em (HA) deverá cumprir os requisitos a seguir:

Objeto: Equipamento e serviços para implantação de segurança virtual na rede de computadores para controle de ameaças virtuais na modalidade “Appliance do tipo UTM

(Unified Threat Management) Firewall concentrador redundante de alta disponibilidade (HA)" em comodato – Firewall Concentrador Redundante Paço Municipal em (HA).
Produto: Serviços de segurança, incluindo-se: 01 (um) equipamento de hardware firewall concentrador appliance UTM (Unified Threat Management) com licenciamento de firewall concentrador redundante de Alta Disponibilidade (HA), ips, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para appliance de firewall de próxima geração com suporte e atualização de versões durante a vigência contratual, em comodato, 12 (doze) meses. Local: FIREWALL CONCENTRADOR REDUNDANTE PAÇO MUNICIPAL em (HA).
Implantação: Serviços de implantação de firewall concentrador redundante em (HA), pagamento único.
Suporte: Suporte por 12 (doze) meses.

Tabela 4 – Descritivos dos Itens 04 e 04.a

Para perfeita utilização do equipamento em alta disponibilidade (HA) em conjunto com o **Item-3** acima descrito, deve ser respeitada mesma marca/modelo e especificações técnicas isso garantindo máxima compatibilidade e interoperabilidade com o Firewall Concentrador em operação.
Para operação em regime de alta disponibilidade (High Availability – HA), a solução ofertada no **Item-4** deverá ser plenamente compatível com o equipamento exigido e descrito no **Item-3**, permitindo sincronização integral de configurações, políticas, sessões e atualizações, etc. Dessa forma deve ser respeitada mesma marca/modelo e especificações técnicas acima já descritas para garantia de máxima compatibilidade com o Firewall Concentrador.
O (HA) (modo de alta disponibilidade) deve suportar o uso de dois equipamentos em modo ativo-passivo ou modo ativo-ativo e deve possibilitar monitoração de falha de link.
Deverá estar licenciado para operar em modo (HA) (modo de alta disponibilidade), assumindo automaticamente a operação do equipamento que apresentar falha e fazer uso do licenciamento do firewall principal sem necessidade de licenças adicionais.
Por cada appliance físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento.
Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.
Por alta disponibilidade (HA), entende-se que a solução é composta ao menos por dois Appliances licenciados para funcionamento em redundância (**Item-3 e Item-4**) podendo ser solicitados a qualquer tempo sem troca do hardware atualmente instalado, podendo ser contratado o segundo hardware a qualquer tempo dentro do período de vida útil de vendas do fabricante da solução.
Cada Appliance deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos.
O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.
O equipamento deverá ser compatível com os já existentes de modo a possibilitar o gerenciamento central de todos eles em conjunto.
A segurança corporativa a ser implantada através do equipamento de segurança firewall de próxima geração deverá ser fornecidos pela contratada com os devidos licenciamentos e atualizações de versões contínuas durante a vigência contratual em comodato.
O serviço de instalação do ambiente deverá ser executado presencialmente nas dependências da contratante por, no mínimo, dois profissionais certificados pelo fabricante da solução. Todas as atividades de configuração, bem como a migração e/ou criação de regras, deverão ser realizadas de forma a não interferir no funcionamento da infraestrutura atual da Prefeitura, considerando que o equipamento a ser implantado é responsável pelo funcionamento da rede que atende mais de 100 (cem) prédios municipais.
A entrada definitiva em operação do equipamento deverá ocorrer somente após a completa validação e realização de testes pela Contratada que comprovem o seu pleno funcionamento. Eventuais

procedimentos que possam ocasionar pausa ou interrupção dos serviços deverão ser executados fora do horário normal de atendimento do Município em data e hora a ser definida pela Diretoria de Tecnologia da Informação, sendo inclusive realizado preferencialmente em finais de semana, de modo a garantir o mínimo impacto possível na infraestrutura tecnológica e na continuidade dos serviços públicos.
Ao término da implantação, instalação e realização de todas as configurações necessárias para o pleno funcionamento do Firewall, a empresa contratada deverá realizar treinamento presencial destinado à reciclagem de conhecimentos, atualização técnica e capacitação de novos integrantes da equipe, por profissional certificado pelo fabricante. O treinamento deverá ter duração mínima de 08 (oito) horas e será realizado obrigatoriamente nas dependências da contratante, voltado à equipe de Tecnologia da Informação, contemplando, no mínimo, os procedimentos de instalação, administração e utilização da solução. O horário de realização será definido pela Diretoria de Tecnologia da Informação (DIRTI), podendo, quando necessário, ser estabelecido que a prestação do serviço ocorra fora do horário de expediente do órgão. A Transferência de conhecimento deverá ser realizada por profissional certificado pelo fabricante da solução, incluindo-se técnicas de execução, gerenciamento e monitoramento.
Como referência técnica para fornecimento deste **Item-4**, informamos que, atualmente a municipalidade, através da Diretoria de TI, faz uso da solução: 01 (um) equipamento de hardware firewall concentrador appliance UTM (Unified Threat Management) com licenciamento de firewall concentrador redundante de Alta Disponibilidade (HA), ips, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para appliance de firewall de próxima geração com suporte e atualização de versões durante a vigência contratual, instalado no local como **FIREWALL CONCENTRADOR REDUNDANTE PAÇO MUNICIPAL em (HA)** para a realização da segurança da rede de computadores em mais de 100 (cem) prédios públicos, esta solução, tem garantido a esta municipalidade, eficiência e constância no gerenciamento da segurança contra invasões a estas redes ao longo dos anos, estabelecendo-se um padrão de usabilidade. Dessa maneira, informa-se que a solução atual já descrita deverá ser mantida com a mesma especificação técnica mínima exigida de modelo/ marca da **SOPHOS LTD.**
O suporte técnico deverá ser prestado em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, com prazo máximo de atendimento presencial em até 06 (seis) horas após a abertura de chamado para incidentes críticos conforme exposto nas **Tabelas 14 e 15.**

4.6 DESCRIÇÃO TÉCNICA DO (ITEM-5)
FIREWALL DE BORDA PARA UNIDADES COM SERVIÇOS ESSENCIAIS (UPA e PALP)

As licenças de uso específicas deverão ser fornecidas pela contratante.
Deverão ser incluídos: treinamento técnico avançado especializado e suporte técnico especializado 24x7x6.
A solução de serviços de segurança para controle de ameaças virtuais “appliance utm firewall de borda” deverá englobar os seguintes itens:

ESPECIFICAÇÕES TÉCNICAS

Objeto: Firewall de borda para unidades com serviços essenciais em saúde pública municipal (UPA e PALP).
Produto: Serviços de segurança, incluindo-se: 01 (um) equipamento de hardware firewall de borda appliance UTM licenciamento de firewall, ips, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para appliance de firewall de próxima geração com suporte e atualização de versões, em comodato, 12 (doze) meses. Local: FIREWALL DE BORDA PARA UNIDADES COM SERVIÇOS ESSENCIAIS UPA E PALP.
Implantação: Serviço de Implantação e configuração de solução de solução de Firewall de Borda – Pagamento Único.
Suporte: Suporte por 12 (doze) meses.

Tabela 5 – Descritivos dos Itens 05 e 05.a

A Solução deverá ser presencialmente instalada nos seguintes locais:

Unidade de Saúde com Serviços Essenciais	Endereço
Unidade de Pronto Atendimento **(UPA)** - Maria Zuleica Theodoro	Av. Pref. Pedro Viriato de Souza Filho, 172 Jardim Paulista
Unidade de Pronto Atendimento Lar Paraná **(PALP)**	Rua João Vecchi, 600 Jardim Lar Paraná

A Solução deverá cumprir os requisitos a seguir:

- Desempenho mínimo de 7000 mbps de throughput para firewall;
- Desempenho mínimo de 1200 mbps de throughput de ips;
- Desempenho mínimo de 1000 mbps de throughput de Threat Protection;
- Desempenho mínimo de 400 mbps de Inspeção TLS/SSL;
- Desempenho mínimo de 2000 mbps de throughput de vpn;
- Suporte a, no mínimo, 1.500.000 de conexões simultâneas;
- Suporte a, no mínimo, 40.000 novas conexões por segundo;
- Possuir o número irrestrito quanto ao máximo de usuários licenciados;
- Possuir armazenamento interno de no mínimo 64 gb para sistema operacional, quarentena local, logs e relatórios;
- Possuir no mínimo 4gb de memória ram;
- Possuir no mínimo 08 (oito) interfaces de rede 1000base-tx;
- Possuir no mínimo uma interface SFP fiber 1Gb;
- Possuir uma interface do tipo console ou similar;
- Possuir duas portas usb;
- Entrada para segunda fonte redundante;
- Appliance de proteção de rede com funcionalidades de next generation firewall (ngfw) e console de gerência, monitoração e logs;
- Por funcionalidades de next generation firewall (ngfw) entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- As funcionalidades de proteção de rede que compõe a plataforma de segurança podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
- A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 07;
- O software deverá ser fornecido em sua versão mais atualizada;
- O (HA) (modo de alta disponibilidade) deve suportar o uso de dois equipamentos em modo ativo-passivo ou modo ativo-ativo e deve possibilitar monitoração de falha de link;
- Uma interface completa de comando de linha (cli command-line-interface) deverá ser acessível através da interface gráfica e via porta serial;
- A atualização de software deverá enviar avisos de atualização automáticos;
- O sistema de objetos deverá permitir a definição de redes, serviços, hosts períodos de tempos, usuários e grupos, clientes e servidores;
- O backup e o reestabelecimento de configuração deverão ser feitos localmente via ftp ou email com frequência diária, semanal ou mensal, podendo também ser realizado por demanda;
- As notificações deverão ser realizadas via email e snmp;
- Suportar snmp e netflow;
- O firewall deverá ser stateful, com inspeção profunda de pacotes (deep packet inspection);
- As zonas deverão ser divididas pelo menos em wan, lan e dmz, sendo necessário que as zonas lan e dmz possam ser customizáveis;
- As políticas de nat deverão ser customizáveis para cada regra;
- A proteção contra flood deverá ter proteção contra dos (denial of service), ddos (distributed dos) e bloqueio de portscan;
- Proteção contra anti-spoofing;
- Suportar ipv4 e ipv6;

- Ipv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e ipv6 rapid deployment (6rd) de acordo com a rfc 5969;
- Suporte aos roteamentos estáticos, dinâmico (rip, bgp e ospf) e multicast (pim-sm e igmp);
- Deve suportar a definição de vlans no firewall conforme padrão ieee 802.1q e tagging de vlan;
- O balanceamento de link wan deve permitir múltiplas conexões de links internet, checagem automática do estado de links, failover automático e balanceamento por peso;
- A solução deverá permitir port-aggregation de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces;
- A solução deverá permitir configurar os serviços de dns, dynamic dns, dhcp e ntp;
- O traffic shapping (qos) deverá ser baseado em rede ou usuário;
- A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas;
- Deve possuir otimização em tempo real de voz sobre ip;
- Deve implementar o protocolo de negociação link aggregation control protocol (lacp);
- Plataforma next-generation firewall (ngfw) para proteção de informação perimetral e de rede interna que inclui stateful firewall com capacidade para operar em alta disponibilidade (HA) em modo ativo-passivo ou ativo-ativo para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (qos), vpn ipsec e ssl, ips, prevenção contra ameaças de vírus, malwares, filtro de url, criptografia de email, inspeção de tráfego criptografado e proteção de firewall de aplicação web;
- Deverá ser fornecida console de gerenciamento dos equipamentos e centralização de logs em cloud;
- Deverão ser fornecidas as licenças para atualização de todos os componentes de software, vacinas de antivírus / malwares, endpoints, softwares de criptografia de armazenamento em nuvem e assinaturas de ips, filtro de conteúdo web, controle de aplicações e proteção de firewall de aplicação web sem custo adicional, pelo período contratual;
- Por cada appliance físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento;
- Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
- Por alta disponibilidade (HA), entende-se que a solução é composta ao menos por dois appliances, licenciados para funcionamento em redundância podendo ser solicitados a qualquer tempo sem troca do hardware atualmente instalado, podendo ser contratado o segundo hardware a qualquer tempo dentro do período de vida útil de vendas do fabricante da solução;
- Cada appliance deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos;
- O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de suporte ou vida;
- Controle por políticas de firewall;
- Deve suportar controles por: porta e protocolos tcp/udp, origem/destino e identificação de usuários;
- O controle de políticas deverá monitorar as políticas de redes, usuários, grupos e tempo, bem como identificar as regras não-utilizadas, desabilitadas, modificadas e novas políticas;
- As políticas deverão ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas, redes e por tipos de serviços;
- Controle de políticas por usuários, grupos de usuários, ips, redes e zonas de segurança;
- Controle de políticas por países via localização por ip;
- Suporte a objetos e regras ipv6;
- Suporte a objetos e regras multicast;
- Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de ips, antivírus, anti-malware e firewall de proteção web (waf) integrados no próprio appliance de firewall ou entregue em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
- Deve realizar a inspeção profunda de pacotes (dpi deep packet inspection) para prevenção de intrusão (ips) e deve incluir assinaturas de prevenção de intrusão (ips);

- As assinaturas de prevenção de intrusão (ips) devem ser customizadas;
- Exceções por usuário, grupo de usuários, ip de origem ou de destino devem ser possíveis nas regras;
- Deve suportar granularidade nas políticas de ips antivírus e anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens, com customização completa;
- A proteção anti-malware deverá bloquear todas as formas de vírus, web malwares, trojans e spyware em http e https, ftp e web-emails;
- A proteção anti-malware deverá realizar a proteção com emulação Javascript;
- Deve ter proteção em tempo real contra novas ameaças criadas;
- Deve possuir pelo menos duas engines de antivírus independentes e de diferentes fabricantes para a detecção de malware, podendo ser configuradas isoladamente ou simultaneamente;
- Deve permitir o bloqueio de vulnerabilidades;
- Deve permitir o bloqueio de exploits conhecidos;
- Deve detectar e bloquear o tráfego de rede que busque acesso a contact command servidores de controle utilizando múltiplas camadas de dns, afc e firewall;
- Deve incluir proteção contra-ataques de negação de serviços;
- Ser imune e capaz de impedir ataques básicos como: syn flood, icmp flood, udp flood, etc.
- Suportar bloqueio de arquivos por tipo;
- Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- Os eventos devem identificar o país de onde partiu a ameaça;
- Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseados em políticas de segurança considerando uma das opções ou a combinação de todas elas: usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de ips, sendo essas políticas por usuários, grupos de usuários, origem, destino, zonas de segurança;
- O firewall deve ter capacidade para contratação futura de módulo de proteção de firewall web (waf) que deverá ter a função de reverse proxy, com a função de url hardening realizando deep-linking e prevenção dos ataques de path traversal ou directory traversal;
- O firewall de aplicação web (waf) deverá realizar cookie signing com assinaturas digitais, roteamento baseado por caminho, autenticações reversas e básicas para acesso do servidor;
- O firewall de aplicação web (waf) deverá possuir a função de balanceamento de carga de visitantes por múltiplos servidores, com a possibilidade de modificação dos parâmetros de desempenho do waf e permissão e bloqueio de ranges de ip. Proteção pelo menos contra os seguintes ataques, mas não limitado a: sql injection e cross-site scripting;
- Controle e proteção de aplicações;
- Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 07, utilizando portas padrões (80 e 443), portas não padrões, port hopping e túnel através de tráfego ssl encriptado;
- Reconhecer pelo menos 1.000 (um mil) aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, serviços de rede, voip, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de softwares;
- Reconhecer pelo menos as seguintes aplicações: 4shared file transfer, active directory/smb, citrix ica, dhcp protocol, dropbox download, easy proxy, facebook graph api, firefox update, freegate proxy, freevpn proxy, gmail video, chat streaming, gmail webchat, gmail webmail, gmail-way2sms webmail, gtalk messenger, gtalk messenger file transfer, gtalk-way2sms, http tunnel proxy, httport proxy, logmein remote access, ntp, oracle database, rar file download, redtube streaming, rpc over http proxy, skydrive, skype, skype services, skyzip, snmp trap, teamviewer conferencing e file transfer, tor proxy, torrent

clients p2p, ultrasurf proxy, ultravpn, vnc remote access, vnc web remote access, whatsapp, whatsapp file transfer e whatsapp web;

- Deve realizar o escaneamento e controle de micro app incluindo, mas não limitado a: facebook (applications, chat, commenting, events, games, like plugin, message, pics download e upload, plugin, post attachment, posting, questions, status update, video chat, video playback, video upload, website), freegate proxy, gmail (android application, attachment), google drive (base, file download, file upload), google earth application, google plus, linkedin (company search, compose webmail, job search, mail inbox, status update), skydrive file upload e download, twitter (message, status update, upload, website), yahoo (webmail, webmail file attach) e youtube (video search, video streaming, upload, website);
- O escaneamento de micro app deverá ser habilitado via console gráfica (gui) e via comando de linha (cli);
- Para tráfego criptografado ssl, deve decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- Atualizar a base de assinaturas de aplicações automaticamente;
- Reconhecer aplicações em ipv6;
- Limitar a banda usada por aplicações (traffic shaping);
- Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft active directory, sem a necessidade de instalação de agente no domain controller, nem nas estações dos usuários;
- Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
- Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuírem acesso a estes aplicativos devem ter a utilização bloqueada;
- Deve permitir especificar política de navegação web por tempo, ou seja, a definição de regras para um determinado dia da semana e horário de início e fim, permitindo a adição de múltiplos dias e horários na mesma definição de política por tempo. Esta regra de tempo pode ser recorrente ou em uma única vez;
- Deve ser possível a criação de políticas por usuários, grupos de usuários, ips e redes;
- Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais urls através da integração com serviços de diretório, autenticação via ldap, active directory, radius, e-directory e base de dados local;
- Permitir popular todos os logs de url com as informações dos usuários conforme descrito na integração com serviços de diretório;
- Possuir pelo menos 80 categorias de urls;
- Suportar a capacidade de criação de políticas baseadas no controle por url e categoria de url;
- Deve ser capaz de forçar o uso da opção safe search em sites de busca;
- Deve ser capaz de categorizar as urls a partir de base ou cache de urls locais ou através de consultas dinâmicas na nuvem do fabricante, independentemente do método de classificação a categorização não deve causar atraso na comunicação visível ao usuário;
- Suportar a criação categorias de urls customizadas;
- Suportar a opção de bloqueio de categoria http e liberação da categoria apenas em https;
- Permitir a customização de página de bloqueio;
- Suportar a inclusão nos logs do produto de informações das atividades dos usuários;
- Deverão salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado;
- Deve realizar caching do conteúdo web;
- Deve realizar filtragem por mime-type, extensão e tipos de conteúdo ativos, tais como, mas não limitado a: activex, applets e cookies;
- Identificação de usuários;
- Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticando via ldap, active

directory, radius, edirectory, tacacs+ e via base de dados local, para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

- Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (captive portal);
- Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço ip em ambientes citrix e Microsoft terminal server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- Deve permitir autenticação em modos: transparente, autenticação proxy (ntlm e kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, Mac OS x e Linux 32/64;
- Deve possuir a autenticação single sign-on para, pelo menos, os sistemas de diretórios active directory e edirectory;
- Deve possuir portal do usuário para que os usuários tenham acesso ao uso de internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução;
- Qualidade de serviço – QOS;
- Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações;
- A solução deverá suportar traffic shaping (qos) e a criação de políticas baseadas em categoria web e aplicação por: endereço de origem. endereço de destino. usuário e grupo do ldap/ad;
- Deve ser configurado o limite e a garantia de upload/download, bem como ser priorizado o tráfego total e bitrate de modo individual ou compartilhado;
- Suportar priorização real-time de protocolos de voz (voip);
- Redes virtuais privadas – VPN;
- Suportar vpn site-to-site e cliente-to-site;
- Suportar ipsec vpn;
- Suportar acesso remoto ssl, ipsec e vpn cliente para android e iphone/ipad;
- Deve ser disponibilizado o acesso remoto ilimitado, até o limite suportado de túneis vpn pelo equipamento, sem a necessidade de aquisição de novas licenças e sem qualquer custo adicional para o licenciamento de clientes para estações Windows;
- Deve possuir um portal encriptado baseado em html5 para suporte pelo menos a: rdp, http, https, ssh, telnet e vnc, sem a necessidade de instalação de clientes vpn nas estações de acesso;
- A vpn ipsec deve suportar: des e 3des, autenticação md5 e sha-1. diffie-hellman group 1, group 2, group 5 e group 14. algoritmo internet key exchange (ike). aes 128, 192 e 256 (advanced encryption standard). sha 256, 384 e 512. autenticação via certificado pki (x.509) e pre-shared key (psk);
- Deve possuir interoperabilidade com os seguintes fabricantes: cisco, check point, dell sonicwall, fortinet, huawei, juniper, palo alto networks e sophos;
- Deve permitir criar políticas de controle de aplicações, ips, antivírus, anti-malware e filtro de url para tráfego dos clientes remotos conectados na vpn ssl;
- Suportar autenticação via ad/ldap, token e base de usuários local;
- Permitir estabelecer um túnel vpn com uma solução de autenticação via ldap, active directory, radius, edirectory, tacacs+ e via base de dados local;
- Gerência administrativa centralizada;
- Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos através de uma única console central, com administração de privilégios e funções;
- O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;
- Estar licenciada para gerenciar as soluções de firewall de próxima geração;
- Deve ser centralizada a gerência de todas as políticas do firewall e configurações para as soluções de firewall de próxima geração, sem necessidade de acesso direto aos equipamentos.
- Deve possuir indicadores do estado de equipamentos e rede;

- Deve emitir alertas baseados em thresholds customizáveis, incluindo também alertas de expiração de subscrição, mudança de status de gateways, uso excessivo de disco, eventos atp, ips, ameaças de vírus, navegação, entre outros;
- Deve permitir a criação de grupos de equipamentos por nome, modelo, firmware e regiões.
- Deve ter controle de privilégios administrativos, com granularidade de funções (vpn admin, app e web admin, ips admin, etc);
- Deve ter controle das alterações feitas por usuários administrativos, comparar diferentes versões de configurações e realizar o processo de roll back de configurações para mudanças indesejadas;
- Deve ter logs de auditoria de uso administrativo e atividades realizadas nos equipamentos;
- Deve ter integração com a solução de logs e relatórios, habilitando o provisionamento automático de novos equipamentos e a sincronização dos administradores da centralização da gerência com a centralização de logs e relatórios;
- Gerência de logs e relatórios centralizados;
- Deve possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução através de uma única console central;
- Estar licenciada para gerenciar as soluções de firewall de próxima geração;
- Devem ser fornecidas soluções em cloud desde que obedeçam a todos os requisitos desta especificação, com armazenamento mínimo de 07 (sete) dias sem limite de volume e expansível até 1TB de dados;
- Deverá prover relatórios baseados em usuários, com visibilidade sobre acesso a aplicações, navegação, eventos atp, downloads e consumo de banda, independente em qual rede ou ip o usuário esteja se conectando;
- Devem possibilitar a identificação de ataques como a identificação de malware identificados pelos eventos atp, usuários suspeitos, tráfegos anômalos incluindo tráfego icmp e consumo não-usual de banda;
- Deve conter relatórios pré-configurados, pelo menos de: aplicações, navegação, web server (waf), ips, atp e vpn;
- Deve fornecer relatórios históricos para análises de mudanças e comportamentos;
- Deve conter customizações dos relatórios para inserção de logotipos próprios;
- Deve fornecer relatórios de compliance, hipaa e pci;
- Deve permitir a exportação via pdf ou excel;
- Deve fornecer relatórios sobre os acessos de procura no google, yahoo, bing e wikipedia;
- Deve fornecer relatórios de tendências;
- Deve fornecer logs em tempo real, de auditoria e arquivados;
- Deve possuir mecanismo de procura de logs arquivados;
- Deve ter acesso baseado em web com controles administrativos distintos;
- Instalação, suporte e monitoramento; e
- O equipamento deverá ser compatível com os já existentes de modo a possibilitar o gerenciamento central de todos eles.

A empresa vencedora deverá oferecer e instalar sem custos durante todo período de contrato, ferramenta de monitoramento de rede em plataforma Windows com pelo menos 100 (cem) sensores para gerenciamento proativo da solução, com capacidade para monitorar snmp, wmi e contadores de desempenho do Windows, ssh para sistemas linux/unix, fluxos e sniffing de pacotes, solicitações http, qualquer rest api retornando xml ou json, ping e sql com geração de relatórios e envio de alertas via e-mail e sms. Capacidade de monitorar os indicadores do firewall next generation oferecido na proposta com os seguintes indicadores: cpu, memória, portas de comunicação, data de expiração da licença serviço dns, smtp e status do modulo de antivírus.

A segurança corporativa a ser implantada através do equipamento de segurança firewall de próxima geração deverá ser fornecidos pela contratada com os devidos licenciamentos e atualizações de versões contínuas durante a vigência contratual em comodato.

Impreterivelmente, a Solução de serviços de segurança para controle de ameaças virtuais “appliance utm firewall de Borda” deverá ser fornecido por um único fabricante Sophos Ltd e ter total compatibilidade e operar em conjunto com os **Itens-3 e 4**.

O serviço de instalação do ambiente deverá ser executado presencialmente nas dependências da contratante por, no mínimo, dois profissionais certificados pelo fabricante da solução. Todas as atividades de configuração, bem como a migração e/ou criação de regras, deverão ser realizadas de forma a não interferir no funcionamento da infraestrutura atual das Unidades Essenciais (**UPA e PALP**). A entrada definitiva em operação do equipamento deverá ocorrer somente após a completa validação e realização de testes pela Contratada que comprovem o seu pleno funcionamento. Eventuais procedimentos que possam ocasionar pausa ou interrupção dos serviços deverão ser executados em data e hora a ser definida pela Diretoria de Tecnologia da Informação juntamente com as Unidades Essenciais tendo em vista a alta demanda das referidas localidades, sendo inclusive necessário a realização em horários de baixo fluxo de atendimento (após as 22:00 horas por exemplo), de modo a garantir o mínimo impacto possível na infraestrutura tecnológica e na continuidade da prestação de serviço de ambos os locais.

Ao término da implantação, instalação e realização de todas as configurações necessárias para o pleno funcionamento do Firewall, a empresa contratada deverá realizar treinamento presencial destinado à reciclagem de conhecimentos, atualização técnica e capacitação de novos integrantes da equipe, por profissional certificado pelo fabricante. O treinamento deverá ter duração mínima de 04 (quatro) horas e será realizado obrigatoriamente nas dependências da contratante, voltado à equipe de Tecnologia da Informação, contemplando, no mínimo, os procedimentos de instalação, administração e utilização da solução. O horário de realização será definido pela Diretoria de Tecnologia da Informação (DIRTI), podendo, quando necessário, ser estabelecido que a prestação do serviço ocorra fora do horário de expediente do órgão. A Transferência de conhecimento deverá ser realizada por profissional certificado pelo fabricante da solução, incluindo-se técnicas de execução, gerenciamento e monitoramento.

Como referência técnica para fornecimento deste **Item-5**, informamos que, atualmente a municipalidade, através da Diretoria de TI, faz uso da solução: 02 (dois) equipamentos de hardware firewall de borda appliance UTM licenciamento de firewall, ips, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para appliance de firewall de próxima geração com suporte e atualização de versões, instalados na **UPA e PALP** como **FIREWALL DE BORDA PARA UNIDADES COM SERVIÇOS ESSENCIAIS** para a realização da segurança da rede de computadores nesses prédios públicos essenciais, esta solução, tem garantido a esta municipalidade, eficiência e constância no gerenciamento da segurança contra invasões a estas redes ao longo dos anos, estabelecendo-se um padrão de usabilidade. Dessa maneira, informa-se que a solução atual já descrita deverá ser mantida com a mesma especificação técnica mínima exigida de modelo/ marca da **SOPHOS LTD.**

O suporte técnico deverá ser prestado em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, com prazo máximo de atendimento presencial em até 06 (seis) horas após a abertura de chamado para incidentes críticos conforme exposto nas **Tabelas 14 e 15.**

4.7 DESCRIÇÃO TECNICA (ITEM-6)
FERRAMENTA DE SOFTWARE DE SISTEMA PARA SUPORTE REMOTO TIPO “HELP DESK”

A solução de ferramenta de software de sistema para suporte remoto “Help Desk” contemplará as seguintes especificações técnicas:

Objeto: Ferramenta de software de sistema para suporte remoto tipo “Help Desk”.
Produto: Ferramenta de software de sistema para suporte remoto “Help Desk” compatível com os sistemas operacionais em uso, compreendendo: 01 (uma) licença para até 06 (seis) analistas e licenças para usuários ilimitados, usável em navegador de internet com comunicação através deste serviço – 2000 (dois mil) hosts.
Implantação: Serviços de Implantação, configuração e instalação de software para suporte remoto – Pagamento Único.
Suporte: Suporte por 12 (doze) meses.

Tabela 6 - Descritivos dos Itens 06 e 06.a

A solução de software de sistema para suporte remoto “Help Desk” contemplará: softwares para 06 (seis) canais de atendimento de suporte técnico e ilimitados usuários, todos os bens e serviços inerentes, deverão ser fornecidos pela contratada com os devidos licenciamentos e atualizações de versões contínuas durante a vigência contratual, podendo ser instaladas em no mínimo 2000 (dois mil) hosts.

4.7.1 A SOLUÇÃO DE SOFTWARE DE SISTEMA PARA SUPORTE REMOTO “HELP DESK” DEVE TER AS SEGUINTES CARACTERÍSTICAS MÍNIMAS

- Gerencie remotamente computadores e equipamentos controlados por computador;
- Gerencie usuários e dispositivos da através de um Management Console;
- Forneça suporte de plataforma cruzada Windows e Linux;
- Permita o acesso remoto sem abertura de portas em firewalls;
- Relatórios detalhados de conexão para formar uma base de informações precisas;
- Número ilimitado de clientes com uma única licença;
- Priorize e atribua pedidos de suporte através da fila de serviço;
- Não necessite instalar o software para os clientes solicitarem e receberem suporte;
- Transferência de arquivo; e
- Ferramentas de suporte com reinicialização remota, impressão remota e VPN.

4.7.2 POSSUIR A CAPACIDADE DE ORGANIZAR REUNIÕES E APRESENTAÇÕES PARA ATÉ 25 PARTICIPANTES EM UMA REUNIÃO COM

- Bate-papo, vídeo, VoIP, teleconferência;
- Agendar e gravar reuniões;
- Possuir ferramentas de colaboração como quadro branco, controle de transferência, funções da reunião; e
- Conectividade multiplataforma.

4.7.3 O HELP DESK DEVE CONTER FUNÇÕES PARA

- Possibilitar a customização da marca/logo;
- Possuir integrações pré-incorporadas para Outlook, MS Teams;
- Possibilitar integração a outros sistemas via API; e
- Possua capacidade de conexões a partir de dispositivos móveis iOS e Android.

4.7.4 POSSUIR GERENCIAMENTO DE ADMINISTRAÇÃO COM AS SEGUINTES CARACTERÍSTICAS

- Políticas de configuração centralizadas;
- Gerenciamento do usuário;
- Controles detalhados de acesso do cliente e configurações avançadas do cliente;
- Implementação em massa (MSI, Android, Host);
- Possua relatório de conexão do usuário e conexão de dispositivo;
- Permita visualizar todas as conexões de entrada rapidamente em um painel central para visualizar quem está se conectando aos dispositivos; e
- Compatível com as plataformas Windows, Mac, Linux, iOS e Android.

O software deve oferecer uma console de gerenciamento central baseado na web para gerenciar contatos e registrar as conexões. Além disso, deve oferecer funções para gerenciar várias contas e gerenciá-las através de uma conta administrativa. Possibilitar ser acessado através da Internet usando um navegador da Web.
Gerenciamento centralizado de várias contas em um nível de organização.
Permitir criar módulos personalizados com a opção de adicionar logotipo, modificar cores e textos adequados à identidade corporativa.
Gerenciamento de dispositivo confiável para informar os dispositivos e endereços IP em que foi confiado.

Recurso para os administradores poderem visualizar todos os dispositivos confiáveis da empresa e removê-los facilmente em caso de emergência.
Possuir recurso de redefinição de senha forçada em caso de comportamento incomum.
Possuir criptografia com troca de chaves pública/privada RSA e criptografia de sessão AES (256 bits).
Possuir capacidade de autenticação de duplo fator.
Capacidade mínima de 2.000 (dois mil) dispositivos gerenciados para licenças do tipo estações de trabalho e 20 (vinte) licenças do tipo servidor de rede windows/linux.
Deverá ser realizada pela Contratada e/ou caso seja necessário, a exportação de hosts do atual licenciamento e/ou reinstalação do software em TODAS as estações de trabalho (Anexo III – Lista de locais) e no ambiente de gerenciamento da DIRTI para os servidores de rede.
Ao término da implantação, instalação e realização de todas as configurações necessárias para o pleno funcionamento da ferramenta, a empresa contratada deverá realizar treinamento presencial destinado à reciclagem de conhecimentos, atualização técnica e capacitação de novos integrantes da equipe. O treinamento deverá ter duração mínima de 04 (quatro) horas e será realizado obrigatoriamente nas dependências da contratante, voltado à equipe de Tecnologia da Informação, contemplando, no mínimo, os procedimentos de instalação, administração e utilização da solução. O horário de realização será definido pela Diretoria de Tecnologia da Informação (DIRTI), podendo, quando necessário, ser estabelecido que a prestação do serviço ocorra fora do horário de expediente do órgão.
Como referência técnica para fornecimento dos **Item-6**, informa-se que, atualmente a municipalidade, através da Diretoria de TI, faz uso da ferramenta **"TEAM VIEWER"**, nas versões cliente para o gerenciador e cliente para todos os usuários de rede dos prédios públicos nos ambientes de TI da municipalidade. Informamos ainda que a prefeitura, através da Diretoria de TI, possui histórico de uso de vários anos da ferramenta atual, o que ao longo do tempo estabeleceu um padrão de usabilidade, o que tem garantindo a eficiência adequada na prestação de assistência técnica remota aos usuários das redes da prefeitura. Dessa maneira, informa-se que a solução atual já descrita deverá ser mantida com a mesma especificação técnica mínima exigida de modelo/ marca para a nova contratação de forma que, tecnicamente possa ser garantido o atendimento remoto eficiente que tem garantido alto padrão na eficiência e na rapidez para a solução de problemas de TI.
O suporte técnico deverá ser prestado em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, com prazo máximo de atendimento presencial em até 06 (seis) horas após a abertura de chamado para incidentes críticos conforme exposto nas **Tabelas 14 e 15.**

4.8 DESCRIÇÃO TECNICA (ITEM-7)
SOFTWARE DE SISTEMA ANTIVÍRUS CORPORATIVO PARA CONTROLE DE AMEAÇAS DIGITAIS NOS EQUIPAMENTOS DA REDE DE COMPUTADORES E SEGURANÇA
ESPECIFICAÇÕES TÉCNICAS

Objeto: Software de sistema antivírus corporativo para controle de ameaças digitais nos equipamentos da rede de computadores e segurança.
Produto: Sistema de software de antivírus corporativo: licenças para estações de trabalho e servidores de rede, compatível com todos os sistemas operacionais legados com console de gerenciamento WEB incluso, 2000 (duas mil) licenças para estações de trabalho e 20 (vinte) licenças para servidores de rede.
Implantação: Serviços de implantação de antivírus corporativo para todas as estações de trabalho e servidores de rede – Pagamento Único.
Suporte: Suporte por 12 (doze) meses.

Tabela 7 – Descritivos dos Itens 07 e 07.a

4.8.1 SOLUÇÕES DOS SOFTWARES DE SISTEMAS ANTIVÍRUS CORPORATIVO PARA ESTAÇÕES DE TRABALHO E SERVIDORES DE REDE – REQUISITOS

Para as ferramentas de antivírus corporativo para servidores de rede e estações de trabalho, as soluções, deverão cumprir os requisitos a seguir:

- Os softwares que compõem a solução dos softwares de sistemas de antivírus para servidores de rede e estações de trabalho deverão ser totalmente gerenciáveis através da mesma console de gerenciamento centralizado e de forma que todos os produtos sejam monitorados através desta;
- A solução deverá possuir ferramentas de varredura, detecção, análise e remoção de malwares, riskwares, spywares e demais formas de vírus e códigos maliciosos conhecidos, bem como modulo para controle do firewall windows, controle de aplicativos, verificação de tráfego web, modulo de atualização de softwares e proteção contra ransonware. Estas devem ser totalmente integradas, instaladas através de um único pacote sem a necessidade de instalação de módulos adicionais;
- Prover solução de monitoramento remoto com utilização de interface Web, para administração, monitoração e gerenciamento da solução ofertada;
- A solução de gerenciamento Web deverá ser em nuvem do fabricante da solução;
- O servidor de gerenciamento deve possibilitar a administração dos hosts, via internet, inclusive com a capacidade de fazer upgrade da versão instalada remotamente;
- O fabricante do antivírus deve possuir site próprio para coleta de amostras de arquivos infectados e falsos positivos;
- Permitir a criação de usuários para acesso a console de gerenciamento web, com opção de usuário administrador e usuário para leitura (read only);
- Manter um registro de acessos realizados pelos administradores no sistema de gerenciamento da solução de segurança;
- Prover comunicação segura entre os servidores de gerenciamento e clientes gerenciados através de protocolo https para a comunicação entre hosts gerenciados e servidor de gerenciamento;
- Atualização de listas, vacinas, mecanismos de rastreamento e desinfecção através da internet via protocolo http ou https, disponibilizando estas para todas as demais ferramentas que compõem a solução de antivírus automaticamente sem a intervenção do administrador;
- As atualizações devem ser incrementais, inclusive o download, este deve ser gerenciado de forma que baixe somente a parte que lhe falta e do ponto onde foi interrompido;
- Permitir a alteração das configurações dos agentes antivírus nos clientes de maneira remota;
- Bloquear as configurações nas estações de trabalho sem a necessidade de senha, evitando que os usuários alterem as configurações do produto;
- Atualizar automaticamente as políticas de prevenção a partir da console de gerenciamento;
- Estabelecer políticas em caso de epidemia de vírus criando-se regras de bloqueio com hash SHA-1/SHA-256 contra os ataques até que a vacina seja criada para as plataformas do ambiente da contratante;
- Gerar relatórios que contenham informações sobre as infecções e atualizações da solução;
- Exportar relatórios para csv;
- Permitir a visualização contendo as seguintes informações: status on-line, perfil atribuído, nome do SO, versão do software, status de proteção, data de registro, endereço IP, status do bitlocker, endereço MAC;
- Manter histórico de infecções;
- Manter dados do host (sistema operacional e versão do mesmo, status da vida útil do SO, host name, dns name, ip, endereço MAC, status RDP, status bitlocker, versão do TPM);
- Listar dados de inventários com no mínimo os seguintes itens: modelo do hardware, fabricante da bios e versão, Nome e modelo da CPU, número de cores do processador, tipo de disco, tamanho de disco, espaço disponível na unidade de boot, quantidade de memória RAM e modelo, presença e versão do TPM, número de serie e endereço MAC da placa de rede.
- Possuir um dashboard com informações do estado geral da solução de segurança e hosts gerenciados;
- Ter recursos de Inteligência Artificial (IA) para auxílio aos administradores para análise de eventos de segurança, facilitando a interpretação e posterior ação de proteção do ambiente.
- A solicitação de verificação de atualização de vacinas e políticas de segurança deve ser originada a partir da estação de trabalho para o servidor de gerenciamento web;
- Utilizar protocolo seguro (https) para consulta/visualização de relatórios;

- Capacidade de gerenciar e aplicar as atualizações de softwares e patches disponibilizados para os sistemas operacionais Windows do ambiente de TI da contratante, bem como verificar a disponibilidade de atualizações e correções para softwares de terceiros de forma automática, através de configurações no console de gerenciamento central da solução de proteção para endpoints;
- Ter capacidade de aplicar as atualizações de software, sem a necessidade de intervenção do usuário;
- Aplicar as atualizações e correções de produtos de terceiros mesmo quando o usuário logado não possui privilégios para a tarefa de instalação;
- Aplicar as atualizações e correções na plataforma Windows de produtos de terceiros mesmo quando o computador estiver bloqueado ou quando não houver usuário conectado (em logoff);
- Ser o repositório web das atualizações de software do ambiente cliente/servidor da contratante;
- Possibilitar a importação de novos computadores em perfil específico, baseado em parâmetros pelo menos de IP, host, DNS, Unidade Organizacional do MS Active Directory, aplicando automaticamente rótulos e grupos durante a importação;
- Configurar grupos/tags distintos para atualização de software, dessa forma, podendo marcar quais grupos sofrerão atualização de software e quais não sofrerão;
- Agendar alertas sobre atualizações críticas de correções;
- Criar lista de programas para exclusão da verificação da necessidade de atualização de software;
- Possibilitar configurar os eventos do sistema operacional Windows que devem ser enviados ao console de gerenciamento web para análise de eventos de segurança correlatos como bloqueio de usuário, desbloqueio de usuário, criação de usuários, elevação de direitos administrativos, falha de logon, apagamento de dados de auditoria entre outros;
- Possibilitar a contratação de módulos de detecção e resposta para endpoint (EDR) em qualquer quantidade podendo ser menor que a quantidade de endpoints totais contratados, devendo ser gerenciado pelo mesmo ambiente de gerenciamento que os endpoints sem o modulo de EDR;
- Possuir a possibilidade de expansão do sistema de segurança com modulo de análise de vulnerabilidades integrado ao ambiente de gerenciamento usando a mesma console de gerenciamento de antivírus; e
- Atualizações e/ou reinstalações que venham a ser necessárias deverão ser realizadas pela CONTRATADA, nas dependências da Prefeitura Municipal de Campo Mourão e todas as suas demais localidades.

4.8.2 SOLUÇÃO DE SEGURANÇA PARA ESTAÇÕES DE TRABALHO DA REDE

As interfaces dos clientes antivírus e anti-spyware para estações de trabalho da rede devem ter a opção de ser instalada em português do Brasil nas plataformas de sistemas operacionais existentes no ambiente de TI da CONTRATANTE e devem contemplar as seguintes funcionalidades:

- A solução end-point security deve permitir ser instalada, no mínimo, através das seguintes opções: remotamente via GPO e através de scripts;
- Permitir instalação “silenciosa”;
- Permitir atualizações da versão da solução de segurança (programa end-point security) através de login script, internet/intranet, cd-rom e arquivo offline;
- Permitir instalação remota sem forçar a reinicialização da máquina;
- Agrupar estações de trabalho por perfil;
- Configuração diferenciada para cada perfil;
- Monitoramento e gerenciamento em interface centralizada, contemplando clientes da rede a partir de um servidor central web, criando-se configurações específicas para cada perfil de clientes, atendendo os requisitos de sistemas operacionais;
- Atualizar listas de vírus, vacinas e mecanismos de rastreamento automaticamente através da internet para as plataformas de todos os clientes do ambiente de TI da CONTRATANTE;
- O módulo de atualização automática deve suportar serviço de proxy;
- Ter capacidade de rastreamento em tempo real, manual ou agendada, tomando as seguintes ações: limpar, apagar, colocar em quarentena o arquivo infectado;

- Permitir que o rastreamento agendado seja configurado pelo administrador da rede, com frequência diária, em horário definido podendo escolher baixa prioridade para minimizar o impacto nos hosts;
- Rastreamento manual com interface gráfica em português do Brasil;
- No rastreamento manual, possuir capacidade de indicar a prioridade do rastreamento em normal ou segundo plano;
- Detectar cookies potencialmente indesejáveis no sistema;
- Possuir módulo anti-ransonware que monitore pastas (diretórios) impedindo aplicações potencialmente perigosas de modificar os arquivos contidos nestas pastas para proteção contra ransonware e similares;
- Possuir módulo zero day, para detecção de ameaças ainda desconhecidas, com opção de inserção de lista de exceções. Para maior segurança, a identificação do arquivo a ser excluído do módulo zero day deve ser efetuada através de hash ou caminho do arquivo;
- Para redução do tráfego de dados em segmentos de rede a solução deve possuir servidores proxy para servidores Windows e Linux ilimitados, para a entrega de vacinas de antivírus e atualização de softwares de terceiros, com capacidade de indicar quais hosts devem usar o repositório web e quais devem usar os servidores proxy;
- Rastrear arquivos compactados no mínimo nos seguintes formatos: zip, arj, lzh, rar, cab, bz2, tar, tgz, jar e gz em ambiente Windows e/ou Linux;
- Criar lista de exclusão de pastas ou arquivos que não devem ser rastreados;
- Possuir módulo firewall integrado à ferramenta e gerenciado pelo mesmo console dos módulos antivírus e antispyware para administração do firewall do Windows;
- Bloquear em estações, portas tcp e udp comuns e específicas;
- Permitir a criação de serviços que utilizam portas específicas e protocolos tcp e udp;
- Possuir a funcionalidade de mudança de perfil automático do firewall, de acordo com o ambiente de rede em que o usuário se encontra (Ex.: perfil de escritório, perfil de local público, perfil em ambiente residencial etc.);
- Possuir sistema de detecção de configuração de local de trabalho por endereço IP, rede local, gateway, IP do DHCP, IP do Servidor DNS para alterar os parâmetros de segurança da estação de trabalho habilitando ou desabilitando os seguintes itens: filtro de conteúdo, controle de conteúdo da internet, verificação de trafego da internet, proxy da de atualização e podendo usar um endereço distinto no proxy de atualização, (por exemplo um endereço interno quando na rede segura ou um endereço externo quando em outras redes desconhecidas;
- Possuir módulo de controle de aplicativos configurável, para as ações de rodar um aplicativo, instalar, iniciar um processo e carregar uma biblioteca. Nas seguintes situações com capacidade de parametrização por: caminho do arquivo, hash, nome do fabricante, nome do arquivo, empresa, reputação e versão. Que permita tomar as ações de bloquear, permitir ou registrar conforme parametrização;
- Possuir módulo para varredura do tráfego http durante a navegação via browser analisando o tráfego em busca de códigos maliciosos;
- Possuir a capacidade de bloqueio de endereços de internet nos protocolos http e https;
- Possuir módulo de proteção de tráfego de internet de sites desconhecidos, com capacidade de bloqueio de aplicativos flash, java, activex, executáveis e silverlight;
- Conter um filtro de reputação web, alertando o usuário e bloqueando a página web quando esta for suspeita. O filtro de reputação deve identificar durante a pesquisa nos principais sites de busca, sites suspeitos, assinalando-os com um carimbo de confiável, indeterminado ou não confiável;
- Possuir controle de conteúdo web, com no mínimo 28 (vinte e oito) categorias diferentes, sem necessidade de criar ou customizar nova categoria, entre eles: serviços de pagamento, fraude, ilegais, downloads de software, streaming média, redes sociais, adulto, drogas, namoro, bancos, compras, web mail, sites para invasão, jogos e desconhecidos, podendo bloquear ou liberar uma lista de sites específicos;
- Permitir a configuração por perfis, podendo o administrador determinar, por perfil, quais categorias serão permitidas ou não e se o controle estará ativado para aquele perfil ou não;

- Possuir a funcionalidade gestão de conexões, quando for detectado que foi aberta uma conexão bancária ou conexão a informações confidenciais, devendo poder ser configurado para bloquear durante a conexão segura a execução de scripts, acesso remoto ao computador e limpar a área de trabalho quando finalizado a conexão;
- Gerar notificações para o usuário em caso de detecção de vírus, podendo ser suprimida a mensagem na interface do usuário local pelo administrador e apenas registrado no console web.
- Bloquear acesso às funções de configuração da solução de segurança nas estações de trabalho através do uso de senha e política de segurança para as funções locais, de forma remota, através da console de gerenciamento. Esta função deve permitir bloquear as configurações locais por perfil;
- Gerar notificações para o administrador de rede quando ocorrer uma epidemia de vírus (outbreak alert) através de e-mail;
- Desinstalar remotamente a solução de antivírus na estação;
- Prover atualização automática e incremental das listas de vírus;
- Procurar códigos maliciosos em arquivos pelo tipo em tempo real;
- Fornecer proteção e remoção contra spywares em tempo real;
- Efetuar armazenamento de log de ocorrência de vírus local e na web;
- Implantar políticas de uso para impedir a desinstalação não autorizada ou remoção do módulo residente em memória do cliente de antivírus;
- Possuir módulo para bloqueio de dispositivos;
- Permitir bloquear dispositivos no mínimo pelo hardware id, id do dispositivo, id compatível e classe guid;
- Capacidade de bloquear a escrita em dispositivos de armazenamento em massa, permitindo somente a leitura;
- Capacidade de bloquear a execução de binários (executáveis) a partir de dispositivos de armazenamento em massa;
- Permitir bloquear dispositivos como e no mínimo, modens 5g, dispositivos de armazenamento em massa, câmeras de vídeo embutidas e móveis, CD-ROM, leitores de cartão, discos rígidos (hds), Bluetooth, impressoras, portas LPT e COM, floppy disk, dispositivos wireless podendo bloquear um único dispositivo e liberar todos os demais, bem como liberar um único dispositivo e bloquear os demais. Ex.: bloquear qualquer pendrive exceto um em um único computador;
- Possuir a possibilidade de emitir relatórios com id de dispositivos anexos ao computador, para eventual bloqueio;
- Emitir alertas de tentativa de uso de dispositivo bloqueado por ordem do administrador do sistema, contendo o id do dispositivo e a identificação da máquina que tentou utilizá-lo;
- Proteção ao arquivo de entrada de DNS local “host” do Windows;
- Modulo de criptografia de disco para gerenciamento do Bitlocker com capacidade de ativar ou desativar o recurso nos hosts e coletar e armazenar as chaves de recuperação do Bitlocker;
- Relatório de segurança dos hosts indicando pontos de configuração que podem levar ao comprometimento e vazamento de dados confidenciais, indicando os itens que estão ou não em conformidade com pelo menos quinze parâmetros críticos entre eles: comprimento de senha mínimo, bloqueio de conta, SO em fim de vida útil, RDP ativo, limite de bloquei de conta, unidade local compartilhada, excesso de uso de conta de administrador nos hosts;
- Possibilitar a coleta de dados do antivírus em formato de WMI;
- Possuir modulo anti-ransonware, detectando e bloqueando modificações de dados não autorizados por software desconhecidos. O modulo deve ter capacidade de reverter automaticamente os dados modificados pelos dados originais sem a intervenção do usuário; e
- Possuir o recurso de criação de cofres de dados, onde apenas as aplicações explicitamente autorizadas poderão criar e alterar dados nesses locais previamente definidos pelo administrador.

4.8.3 ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO DE SEGURANÇA PARA SERVIDORES DE REDE COM SUPORTE PARA AS PLATAFORMAS OPERACIONAIS WINDOWS

- Ser gerenciado pela mesma ferramenta de gerenciamento da solução de segurança para estações de trabalho;
- A instalação da solução de segurança deve permitir ser executada remotamente via GPO com arquivos msi;
- Permitir instalação “silenciosa”;
- Permitir atualizações através de login script, internet/intranet e arquivo offline;
- Permitir instalação remota sem forçar a reinicialização da máquina;
- Bloquear o acesso às configurações locais do software;
- Agrupar servidores por perfis;
- Capacidade de gerenciar e aplicar as atualizações de softwares e patches disponibilizados para os sistemas operacionais Windows do ambiente de TI da contratante, bem como verificar a disponibilidade de atualizações e correções para softwares de terceiros de forma automática, através de configurações no console de gerenciamento central da solução de proteção para end-points;
- Para a plataforma Windows possuir módulo de proteção de tráfego de internet de sites desconhecidos, com capacidade de bloqueio de aplicativos flash, java, activex, executáveis e silverlight;
- Em caso de ataques de rede o software deve possuir recurso de isolamento de rede do host Windows a partir da console de gerenciamento central;
- Possuir módulo anti-ransonware que monitore pastas (diretórios) impedindo aplicações potencialmente perigosas de modificar os arquivos contidos nestas pastas para proteção contra ransonware e similares;
- Possuir módulo de monitoramento do firewall do Windows com capacidade de criação de múltiplos perfis;
- Permitir configuração diferenciada para cada perfil de servidores;
- Efetuar monitoramento e gerenciamento através de uma console web para todos os servidores de rede, possibilitando a criação de configurações específicas para cada perfil;
- Atualizar a lista de vírus, mecanismo de rastreamento, desinfecção automaticamente, a partir de um local específico na rede e site do fabricante na internet;
- Atualização automática através de serviço de proxy e sem necessidade autenticação;
- Realizar rastreamento em tempo real e de forma manual e agendada nos servidores da rede;
- Efetuar rastreamento em tempo real na entrada e saída de (gravação e leitura) de arquivos no servidor;
- Ter capacidade de rastreamento em tempo real, manual e agendada, tomando as seguintes ações: limpar, apagar, colocar em quarentena o arquivo infectado;
- Permitir que o rastreamento agendado seja configurado pelo administrador da rede, com frequência diária, em horário definido, para um perfil específico;
- Possuir módulo zero day na plataforma Windows, para detecção de ameaças ainda desconhecidas, com opção de inserção de lista de exceções. Para maior segurança, a identificação do arquivo a ser excluído do módulo zero day deve ser efetuada através de hash;
- Ferramenta de detecção e remoção de vírus, trojans, spyware e rootkits;
- Rastrear arquivos compactados no mínimo nos seguintes formatos: zip, arj, lzh, rar, cab, bz2, tar, tgz, jar e gz em ambiente Windows e/ou Linux;
- Permitir a exclusão de pastas e arquivos que não devem ser rastreados;
- Permitir a exclusão de extensões de arquivos que não devem ser rastreados;
- Gerar relatório de incidente centralizado;

- Detectar e bloquear conteúdo malicioso (sobre o protocolo http) para fornecer proteção adicional contra malware durante a navegação; e
- Possuir recurso nos servidores Windows para bloquear temporariamente, usuários mal-intencionados que gravam arquivos infectados nos compartilhamentos do servidor. O sistema deve permitir configurar o tempo mínimo de 5 minuto e máximo de pelo menos 24 horas para garantir o tempo de correção pelo administrador.

4.8.4. ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO DE SEGURANÇA PARA SERVIDORES DE REDE COM SUPORTE PARA AS PLATAFORMAS OPERACIONAIS LINUX

- Ser gerenciado pela mesma ferramenta de gerenciamento da solução de segurança para estações de trabalho;
- A instalação da solução de segurança deve permitir ser executada via pacotes deb e rpm.
- Agrupar servidores por perfis;
- Permitir configuração diferenciada para cada perfil de servidores;
- Efetuar monitoramento e gerenciamento através de uma console web para todos os servidores da rede, possibilitando a criação de configurações específicas para cada perfil;
- Atualizar a lista de vírus, mecanismo de rastreamento, desinfecção automaticamente, a partir de um local específico na rede e site do fabricante na internet;
- Atualização automática através de serviço de proxy e sem necessidade autenticação;
- Realizar rastreamento em tempo real e de forma manual e agendada nos servidores da rede;
- Ter capacidade de rastreamento em tempo real, manual e agendada, tomando as seguintes ações: apagar ou renomear;
- Permitir que o rastreamento agendado seja configurado pelo administrador da rede, com frequência diária, em horário definido, para um perfil específico;
- Ferramenta de detecção e remoção de malwares;
- Possuir recursos de verificação de arquivos desconhecidos em sistema cloud do fabricante da solução de segurança;
- Rastrear arquivos compactados;
- Possuir recurso de verificação de integridade de arquivos com integração a gerenciadores de pacotes APT e DNF;
- Permitir a exclusão de pastas e arquivos que não devem ser rastreados; e
- Gerar relatório de incidente centralizado.

4.8.5 SERVIÇOS DE INSTALAÇÃO E SUPORTE

O serviço de instalação das ferramentas de administração inicial do ambiente deverá ser executado nas instalações da contratante de forma presencial, por pelo menos dois profissionais certificados pelo fabricante, e instalado em 100% (cem por cento) do parque de computadores locais (cerca de 1500 equipamentos), em conjunto com os técnicos da contratante, removendo a atual solução de segurança e instalando o novo software conforme Anexo III – TABELA DE LOCAIS E ENDEREÇOS respeitando o horário de funcionamento de cada localidade que de forma geral tem funcionamento das 08:00 as 11:30 e das 13:30 as 17:00 horas.

Ao término da implantação, instalação e realização de todas as configurações necessárias para o pleno funcionamento da Ferramenta, a empresa contratada deverá realizar treinamento presencial destinado à reciclagem de conhecimentos, atualização técnica e capacitação de novos integrantes da equipe, por profissional certificado pelo fabricante. O treinamento deverá ter duração mínima de 08 (oito) horas e será realizado obrigatoriamente nas dependências da contratante, voltado à equipe de Tecnologia da

Informação, contemplando, no mínimo, os procedimentos de instalação, administração e utilização da solução. O horário de realização será definido pela Diretoria de Tecnologia da Informação (DIRTI), podendo, quando necessário, ser estabelecido que a prestação do serviço ocorra fora do horário de expediente do órgão.
Como referência técnica para fornecimento do **Item-7**, informa-se que, atualmente a municipalidade, através da Diretoria de TI, faz uso da ferramenta **"WITHSECURE ELEMENTS PREMIUM"**, antiga **"F-SECURE"** nas versões **CLIENT** para estações de trabalho Windows e **SERVER** para servidores de rede "Windows e Linux" para a realização dos serviços de segurança de dados e informações em todos os ambientes de rede da municipalidade. Informamos ainda que a prefeitura, através da Diretoria de TI, possui armazenada extensa biblioteca de dados históricos de LOGs de defesas contra ameaças digitais com cobertura sobre um período de vários anos, o que ao longo do tempo estabeleceu um padrão de usabilidade da ferramenta atual, o que tem garantindo a eficiência e a segurança adequadas ao lidar-se com o gerenciamento da segurança de dados e informações no ambiente de TI em mais de 100 (cem) prédios públicos da prefeitura. Dessa maneira, informa-se que a ferramenta atual já descrita deverá ser mantida com a mesma especificação técnica mínima exigida de modelo/ marca para a nova contratação de forma que, tecnicamente possa ser garantida a segurança digital de dados e informações.
O suporte técnico deverá ser prestado em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, com prazo máximo de atendimento presencial em até 06 (seis) horas após a abertura de chamado para incidentes críticos conforme exposto nas **Tabelas 14 e 15.**

4.9 DESCRIÇÃO DETALHADA (ITEM-8)
LICENÇA DE SOFTWARE PARA COLETA E ARMAZENAMENTO DE LOGS (SYSLOG)

A solução de software para coleta e armazenamento de log centralizados (syslog) em ambiente Windows que deverão ser fornecidos pela contratada com os devidos licenciamentos e atualizações de versões contínuas durante a vigência contratual.
Especificações técnicas:

Objeto: Licença de Software para coleta e armazenamento de Logs (Syslog).
Produto: Software para coleta e armazenamento de log's centralizados (Syslog) em ambiente Windows para 01 (um) servidor.
Implantação: Serviços de implantação e configuração de software de coleta de logs – Pagamento Único.
Suporte: Suporte por 12 (doze) meses.

Tabela 8 – Descritivos dos Itens 08 e 08.a

Software para coleta e armazenamento de log centralizados (syslog) em ambiente Windows deverá preencher no mínimo os requisitos a seguir:
- Originadores syslog ilimitados com mensagens ilimitadas por hora;
- Console de visualização de Logs em tempo real com parâmetros de número de registros, tempo de refresh com ou sem rolamento automático;
- Filtro rápido com opção de severidade, facilidade, fonte, origem, TAG e mensagem;
- Manutenção de armazenamento de base de dados com opção de limpeza e compactação;
- Busca de LOG por período com filtros severidade, facilidade, fonte, origem, TAG e mensagem;
- Exportação de LOGs com formato proprietário, CSV, XML, TXT JSON com filtro de datas e critérios de severidade, facilidade, fonte, origem, TAG e mensagem;
- Exportação de LOGs via interface ODBC com filtro de datas e critérios severidade, facilidade, fonte, origem, TAG e mensagem;
- Importação de dados via em formato syslog;
- Geração de relatórios em HTML com as seguintes características:
  - ✓ Distribuição de mensagens pelo período selecionado;
  - ✓ Estatísticas por dia da semana;
  - ✓ Estatísticas por hora;
  - ✓ Distribuição por severidade e facilidade;

✓ Estatísticas por fonte; e
✓ 50 mensagens mais comuns.
➢ Agendamento de Backup da base de dados dentro da própria ferramenta com seleção de dia, hora e caminho de rede;
➢ Capacidade de encaminhamento de syslog para outros servidores de syslog (relay);
➢ Envio de alertas por e-mail com critérios de severidade, facilidade, fonte, origem, TAG e mensagem;
➢ Capacidade de fornecer acesso remoto ao servidor de SYSLOG;
➢ Os softwares devem ser instalados com todos os recursos solicitados pela administração no local designado; e
➢ Ao término da implantação, instalação e realização de todas as configurações necessárias para o pleno funcionamento da Ferramenta, a empresa contratada deverá realizar treinamento presencial destinado à reciclagem de conhecimentos, atualização técnica e capacitação de novos integrantes da equipe. O treinamento deverá ter duração mínima de 04 (quatro) horas e será realizado obrigatoriamente nas dependências da contratante, voltado à equipe de Tecnologia da Informação, contemplando, no mínimo, os procedimentos de instalação, administração e utilização da solução. O horário de realização será definido pela Diretoria de Tecnologia da Informação (DIRTI), podendo, quando necessário, ser estabelecido que a prestação do serviço ocorra fora do horário de expediente do órgão.
O suporte técnico deverá ser prestado em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, com prazo máximo de atendimento presencial em até 06 (seis) horas após a abertura de chamado para incidentes críticos conforme exposto nas **Tabelas 14 e 15.**

4.10 DESCRIÇÃO DETALHADA DO (ITEM-9)
SOFTWARE DE SISTEMA DETECÇÃO E RESPOSTA PARA ENDPOINT (EDR) NOS EQUIPAMENTOS DA REDE DE COMPUTADORES

Objeto: Licenças de uso de ferramenta de software de sistema para detecção e resposta endpoint EDR (ENDPOINT DETECTION AND RESPONSE/DETECÇÃO E RESPOSTA DE ENDPOINT).
Produto: Licenças de uso de ferramenta de software de sistema para detecção e resposta endpoint EDR (ENDPOINT DETECTION AND RESPONSE/DETECÇÃO E RESPOSTA DE ENDPOINT) para implementar solução de segurança cibernética avançada e monitorar continuamente dispositivos finais para detectar comportamentos suspeitos, investigar ameaças em tempo real e responder automaticamente a incidentes como ransonware e malware em 25 (vinte e cinco) equipamentos estações de trabalho da rede (computadores) a serem elencados pela DIRTI.
Implantação: Serviços de implantação, configuração e instalação de software de sistema para detecção e resposta endpoint EDR (ENDPOINT DETECTION AND RESPONSE/DETECÇÃO E RESPOSTA DE ENDPOINT), pagamento único.
Suporte: Suporte por 12 (doze) meses.

Tabela 9 – Descritivos dos Itens 09 e 09.a

Este item refere-se a ferramenta de software de sistema para detecção e resposta endpoint **EDR (ENDPOINT DETECTION AND RESPONSE/DETECÇÃO E RESPOSTA DE ENDPOINT)** para implementar solução de segurança cibernética avançada e monitorar continuamente dispositivos finais para detectar comportamentos suspeitos, investigar ameaças em tempo real e responder automaticamente a incidentes como ransonware e malwares em equipamentos estações de trabalho da rede (computadores);
As soluções dos softwares de EDR para estações de trabalho e servidores de rede deverão cumprir os requisitos a seguir:
➢ Os softwares devem se integrar a atual solução de antivírus corporativo para estações e servidores;
➢ Deverá ser entregue pelo mesmo instalador via MSI ou EXE durante a instalação nas estações de trabalho;
➢ Possuir tempo de retenção de eventos de no mínimo 12 (doze) meses;

- Os softwares que compõem a solução dos softwares de sistemas de antivírus para servidores de rede, estações de trabalho e EDR deverão ser totalmente gerenciáveis através da mesma console de gerenciamento centralizado Web e de forma que todos os produtos sejam monitorados através desta;
- Prover solução de monitoramento remoto com utilização de interface Web, para administração, monitoração e gerenciamento da solução ofertada;
- A solução de gerenciamento Web deverá ser em nuvem do fabricante da solução;
- O servidor de gerenciamento deve possibilitar a administração dos hosts, via internet, inclusive com a capacidade de fazer upgrade da versão instalada remotamente;
- Manter um registro de acessos realizados pelos administradores no sistema de gerenciamento da solução de segurança;
- Prover comunicação segura entre os servidores de gerenciamento e clientes gerenciados através de assinatura digital, utilizando protocolo https para a comunicação entre hosts gerenciados e servidor de gerenciamento;
- Exportar relatórios para o formato csv;
- Utilizar protocolo seguro (https) para consulta/visualização de relatórios;
- Possibilitar a contratação de módulos de detecção e resposta para endpoint (EDR) em qualquer quantidade podendo ser menor que a quantidade de endpoints totais contratados;
- A solução deve incluir análise comportamental e inteligência artificial, treinada pelos especialistas em segurança cibernética da marca, detectando todas as ameaças conhecidas e desconhecidas. O aprendizado de máquina deve melhorar as detecções reconhecendo novas táticas, técnicas e procedimentos emergentes com lançamentos de processos, conexões de rede e tipos de aplicativos associados; e
- A solução EDR precisará usar a automação de processos para interromper e conter ameaças imediatamente. Você também precisará fornecer uma visualização do ataque com todos os pontos de extremidade afetados e diretrizes sobre como isolar e corrigir a ameaça.
- Deve ter um console de gerenciamento 100% (cem por cento) web e acesso seguro via HTTPS e/ou com autenticação de dois fatores onde deve ser gerenciado e visualizado, entre outras coisas:
  - ✓ Número de hosts gerenciados;
  - ✓ O número total de eventos processados nas últimas 24 (vinte e quatro) horas e nos últimos 30 (trinta) dias;
  - ✓ Número de eventos suspeitos detectados;
  - ✓ Número de detecções detectadas;
  - ✓ Quantidade real de detecção detectada pelo sistema de análise da solução;
  - ✓ A análise de causa raiz da detecção;
  - ✓ A lista de computadores, bem como o inventário de aplicativos usados em cada um dos endpoints;
  - ✓ A análise detalhada da detecção com a lista de endereços de arquivos, processos, URLs, eventos e outras ações que a detecção executou;
  - ✓ Integração com Virustotal.com análise de malware para verificação automática de assinaturas de arquivos na plataforma;
  - ✓ Deve permitir que os eventos detectados sejam correlacionados;
  - ✓ Deve permitir o isolamento do equipamento afetado; e
  - ✓ Deve permitir que as ameaças sejam filtradas de acordo com o risco: Baixo, Médio, Alto e Grave.
- Deve permitir notificar por e-mail o incidente detectado que deve ser incluído no referido relatório:
  - ✓ Hosts afetados;
  - ✓ O tipo de detecção;
  - ✓ O nível de risco;
  - ✓ O tipo de segurança do incidente; e
  - ✓ O nível de importância crítica do incidente.
- A solução deve fornecer ações imediatas para resposta a incidentes, permitindo que administradores de segurança contenham ameaças e previnam a propagação de ataques;
- A solução deve permitir isolamento imediato do dispositivo afetado da rede, evitando movimentação lateral da ameaça;

➢ A solução deve oferecer mecanismos para alertar os usuários dos dispositivos comprometidos por e-mail ou outro canal de comunicação;
➢ A solução deve possibilitar a execução de uma varredura detalhada no endpoint comprometido para identificar e remover ameaças;
➢ A solução deve permitir coleta de pacotes forenses, capturando informações detalhadas do dispositivo afetado para análise posterior;
➢ A solução deve permitir respostas automáticas para detecções específicas, otimizando a resposta a incidentes;
➢ A solução deve fornecer uma visualização da arvore de processos, permitindo que analistas investiguem como o ataque se desenvolveu, incluindo:
✓ Processos envolvidos na detecção;
✓ Origens dos comandos executados;
✓ Correlação com atividades suspeitas anteriores;
✓ A solução deve oferecer uma tabela de eventos correlacionados, permitindo que analistas comparem incidentes idênticos ou semelhantes dentro do mesmo ambiente nos últimos 30 dias;
✓ A solução deve permitir inserção de comentários e anotações em cada incidente, garantindo a rastreabilidade das ações tomadas pela equipe de segurança;
✓ A solução deve permitir que analistas encerram incidentes de acordo com a análise realizada, categorizando-os corretamente; e
✓ A solução deve permitir armazenamento e arquivamento de incidentes encerrados, garantindo rastreabilidade e documentação para auditoria e conformidade.
Como referência técnica para fornecimento do **Item-9**, que refere-se a ferramenta de software de sistema para detecção e resposta endpoint **EDR (ENDPOINT DETECTION AND RESPONSE/DETECÇÃO E RESPOSTA DE ENDPOINT)** para implementar solução de segurança cibernética avançada e monitorar continuamente dispositivos finais para detectar comportamentos suspeitos, investigar ameaças em tempo real e responder automaticamente a incidentes como **ransonware** e **malwares** em equipamentos estações de trabalho da rede (computadores). Nesse sentido, informa-se que esta ferramenta é parte integrante da solução **"WITHSECURE ELEMENTS PREMIUM"**, antiga **"F-Secure"** e que por isso é ferramenta primordial contra ameaças digitais para o gerenciamento de segurança de dados e informações em computadores específicos de ambientes de TI em camada avançada de proteção digital. Com isso, informa-se que a ferramenta atual já descrita deverá ser mantida para a nova contratação de forma que, tecnicamente possa ser garantida a segurança digital de dados e informações.
O suporte técnico deverá ser prestado em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, com prazo máximo de atendimento presencial em até 06 (seis) horas após a abertura de chamado para incidentes críticos conforme exposto nas **Tabelas 14 e 15.**

4.10.1 SERVIÇOS DE INSTALAÇÃO E SUPORTE

➢ Deverá ser ofertado treinamento local gratuito em todos os produtos ofertados para a equipe de informática da contratante, incluindo: instalação, administração e uso das ferramentas fora do horário de trabalho do contratante. O curso deverá ser presencial, ministrado nas instalações do licitante;
➢ O serviço de instalação das ferramentas de administração inicial do ambiente deverá ser executado nas instalações da contratante de forma presencial, e instalado em 100% (cem por cento) do parque de computadores locais, em conjunto com os técnicos da contratante, removendo a atual solução de segurança e instalando o novo software;
➢ As empresas participantes deverão comprovar que dispõe de equipe técnica qualificada, composta por no mínimo 03 (três) profissionais, e estes deverão ser certificados pelo fabricante de pelo menos as Soluções de **ANTIVÍRUS, FIREWALL e EDR**, aptos a prestar atendimento especializado durante toda a vigência contratual;
➢ A comprovação deverá ocorrer mediante demonstração de vínculo profissional ou contratual que assegure a efetiva disponibilidade dos técnicos para execução do objeto;
➢ Ao término da implantação, instalação e realização de todas as configurações necessárias para o pleno funcionamento das Ferramentas, a empresa contratada deverá realizar treinamento presencial

destinado à reciclagem de conhecimentos, atualização técnica e capacitação de novos integrantes da equipe, por profissional certificado pelo fabricante. O treinamento deverá ter a duração mínima apontada em cada item, sendo de no mínimo 04 (quatro) horas e será realizado obrigatoriamente nas dependências da contratante, voltado à equipe de Tecnologia da Informação, contemplando, no mínimo, os procedimentos de instalação, administração e utilização da solução. O horário de realização será definido pela Diretoria de Tecnologia da Informação (DIRTI), podendo, quando necessário, ser estabelecido que a prestação do serviço ocorra fora do horário de expediente do órgão.
O suporte técnico deverá ser prestado em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, com prazo máximo de atendimento presencial em até 06 (seis) horas após a abertura de chamado para incidentes críticos conforme exposto nas **Tabelas 14 e 15.**

4.11 DESCRIÇÃO DETALHADA DO (ITEM-10)
FERRAMENTA DE SOFTWARE DE SISTEMA WEB PARA ABERTURA DE CHAMADOS TIPO "HELP DESK"

A ferramenta de software de sistema web para abertura de chamados tipo "Help Desk" para solicitações internas e gerenciador de tarefas em cloud e que deverá preencher no mínimo os requisitos a seguir:

Objeto: Ferramenta de software de sistema web para abertura de chamados de suporte técnico tipo "Help Desk".
Produto: Ferramenta de software de sistema web para abertura de chamados de suporte técnico tipo "Help Desk", solicitações internas e gerenciador de tarefas em cloud para 20 (vinte) analistas.
Implantação: Serviços de implantação, configuração e instalação de ferramenta de software de sistema web para abertura de chamados de suporte técnico tipo "Help Desk", pagamento único.
Suporte: Suporte por 12 (doze) meses.

Tabela 10 – Descritivos dos Itens 10 e 10.a

- Help Desk/ Service Desk multi-entidades, isto é, uma equipe de analistas atende várias entidades (setores) diferentes com seus usuários respectivos;
- Possibilitar a abertura de tickets com dados de usuário/cliente, setor, categoria, classificação e status;
- Possuir campo previsão com hora e data;
- Permitir estabelecer prioridades em pelo menos 03 (três) níveis de gravidade;
- Na abertura do chamado permitir anexar arquivos, agendar compromisso, incluir um checklist de tarefa e anexar formulários customizados;
- Fazer o registro de todas as interações e não permitir a exclusão de informações após a gravação para integridade e auditoria;
- Possibilitar a alteração ao longo do atendimento do setor, categoria, classificação, analista e previsão, registrado as alterações;
- Após a conclusão permitir registrar a avaliação do cliente final ao ticket de chamado;
- Possuir filtros para pesquisa dos tickets pelos campos número, usuário, cliente, setor, categoria, classificação, status, abertos, lidos, tickets lidos sem interação, datas de abertura / alteração / conclusão / previsão / interações;
- Os campos de filtro de datas devem possuir a capacidade de filtragem por pelo menos, período (de/até podendo ser filtrado com ou sem hora), hoje, amanhã, ontem, N dias a frente e N dias passados;

4.11.1 ATENDIMENTO ONLINE/ CHAT

- ✓ Possibilitar alterar o status de on-line e off-line pelo operador;
- ✓ Selecionar setor do colaborador para atendimento;
- ✓ Possuir painel com fila de espera;
- ✓ Lista de operadores; e
- ✓ Mensagens rápidas.
- Atendimento via Whatsapp integrado;

4.11.2 ATENDIMENTO TELEFÔNICO

✓ Possuir campos para registro de usuário, cliente, data do chamado telefônico com hora de início e fim, setor, categorias e classificação**;**

✓ Possibilitar o registro da queixa e da solução no atendimento; e

✓ Possuir menu de acesso rápido para consulta de histórico do cliente e do usuário, novo ticket e nova tarefa com os dados do atendimento em tela**.**

4.11.3 GESTÃO DO CONHECIMENTO

✓ Capacidade de estruturar os temas por arvore com pastas;

✓ Categorizar as pastas por pelo menos Informações Gerais, Q&A, central de arquivos e listas de pendências; e

✓ Permitir armazenar arquivos em cloud ou criar atalhos de rede para consulta aos dados.

4.11.4 CONTROLE DE HORAS

✓ Permitir o registro e controle de gastos de horas por tarefas com classificação de tipos, classificação, data, colaborador Valor Hora, horas usadas com minutos e descrição.

4.11.5 GESTÃO DE TAREFAS E PROJETOS

✓ Permitir criação de projetos com dados dos participantes, gerente do projeto data de início e fim e status; e

✓ Permitir controle de tarefas com informação de projeto, colaborador, prioridade agendamento, assunto, cliente.

4.11.6 SOLICITAÇÕES INTERNAS

✓ Possibilitar a abertura de solicitações internas com dados de usuário/cliente, setor, categoria, classificação e status;

✓ Possuir campo previsão com hora e data;

✓ Permitir estabelecer prioridades em pelo menos 3 níveis de gravidade;

✓ Na abertura do chamado permitir anexar arquivos, agendar compromisso, incluir um checklist de tarefa e anexar formulários customizados;

✓ Fazer o registro de todas as interações e não permitir a exclusão de informações após a gravação para integridade e auditoria; e

✓ Possibilitar a alteração ao longo do atendimento do setor, categoria, classificação, analista e previsão, registrado as alterações.

➢ Possuir filtros para pesquisa dos chamados pelos campos número, usuário, cliente, setor, categoria, classificação, status, abertos, lidos, tickets lidos sem interação, datas de abertura / alteração / conclusão / previsão / interações;

➢ Os campos de filtro de datas devem possuir a capacidade de filtragem por pelo menos, período (de/até podendo ser filtrado com ou sem hora), hoje, amanhã, ontem, N dias a frente e N dias passados;

4.11.7 COMUNICADOR INTERNO

✓ Permitir a troca de mensagens rápida entre os colaboradores por departamento; e

✓ Possibilitar além da troca de texto o envio de anexos com retenção de dados de pelo menos 24 (vinte e quatro) horas do envio.

4.11.8 SISTEMA DE RECADOS

✓ Permitir envio de recados pela plataforma com opção de envio de anexos de rede ou de arquivos em cloud;

✓ Os recados podem ser enviados com opção de privacidade para leitura apenas do recebedor; e

✓ Possibilitar o arquivamento de recados e a marcação como favorito.

4.11.9 AGENDA CORPORATIVA

✓ Possuir agenda compartilhada com vários tipos de calendários setorizados por equipes;
✓ Possuir os campos assunto, local, notas sobre a agenda; e
✓ Permitir disparar alertas programados aos participantes com agendamento de alertas múltiplos, por pop-up, sms e whatsapp.

4.11.10 RELATÓRIOS GERAIS

✓ Chamados abertos por período por analista, colaborador, setor com data de abertura, fechamento e status;
✓ Listagem de chamados com interação por analista e colaborador;
✓ Análise de tempo de resposta por chamado com a primeira resposta, última resposta e tempo de chamado total;
✓ Avaliação dos atendimentos por analista;
✓ Chamados pendentes;
✓ Análise de Tickets abertos x fechados;
✓ Análise de previsão dos chamados;
✓ Estatísticas dos chamados abertos por mês e por hora de chamado;
✓ Análise de tempo de duração; e
✓ Avaliação dos atendimentos.
➢ Todos os relatórios devem possuir pelo menos os seguintes filtros: ticket, setor, categoria, classificação, status, assunto, operador, interação por operador, prioridade, tickets abertos, data de abertura, última alteração data de conclusão, data de previsão;
➢ Os campos de filtro de datas nos relatórios devem possuir a capacidade de filtragem por pelo menos, período (de/até podendo ser filtrado com ou sem hora), hoje, amanhã, ontem, N dias a frente e N dias passados; e
➢ Ao término da implantação, instalação e realização de todas as configurações necessárias para o pleno funcionamento da Ferramenta, a empresa contratada deverá realizar treinamento presencial destinado à reciclagem de conhecimentos, atualização técnica e capacitação de novos integrantes da equipe. O treinamento deverá ter duração mínima de 04 (quatro) horas e será realizado obrigatoriamente nas dependências da contratante, voltado à equipe de Tecnologia da Informação, contemplando, no mínimo, os procedimentos de instalação, administração e utilização da solução. O horário de realização será definido pela Diretoria de Tecnologia da Informação (DIRTI), podendo, quando necessário, ser estabelecido que a prestação do serviço ocorra fora do horário de expediente do órgão.
O suporte técnico deverá ser prestado em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, com prazo máximo de atendimento presencial em até 06 (seis) horas após a abertura de chamado para incidentes críticos conforme exposto nas **Tabelas 14 e 15.**

4.12. DESCRIÇÃO DETALHADA DO (ITEM-11)

IMPLANTAÇÃO DE REDUNDÂNCIA FÍSICA E LÓGICA DE (AD E FILE SERVER)

Objeto: Serviço de implantação física e lógica de redundância de servidores de rede (AD e File Server).
Produto: Serviço de implantação física e lógica de redundância de servidores de rede (AD e File Server), pagamento único sob demanda.

Configuração de replicação/espelhamento do Microsoft Active Directory em servidor secundário e replicação de dados do sistema de arquivos para redundância em Local a ser definido pela Diretoria de Tecnologia da Informação da Prefeitura Municipal de Campo Mourão – PR.
Deverá incluir a Controlador de Domínio adicional, sincronização completa das bases (AD DS, DNS integrado e demais serviços correlatos) e validação do funcionamento do ambiente em alta disponibilidade.
Implementação de replicação de dados do sistema de arquivos (File Server), deverá garantir a redundância das informações institucionais em local a ser definido pela Administração, com utilização

de mecanismos nativos do sistema operacional ou solução tecnicamente adequada à arquitetura existente.
Equipamentos para a montagem da estrutura redundante será disponibilizado pela DIRTI, pois já pertence ao parque de tecnológico do Município.
A Contratada será responsável pela instalação física, lógica e de sistema Operacional conforme estrutura pré-existente, desmontagem, montagem, configuração, parametrização, testes, documentação e entrada em operação do ambiente redundante.
Criação dos Jobs de backup do novo ambiente no atual software de backup da com replicação das novas máquinas virtuais.

4.13. DESCRIÇÃO DETALHADA DO (ITEM-12)
IMPLEMENTAÇÃO DE PLANO DE DISASTER RECOVERY/ RECUPERAÇÃO DE DESASTRES

Objeto: Implementação e implantação de plano de Disaster Recovery/Recuperação de Desastres.
Implantação: Implementação de plano de Disaster Recovery/Recuperação de Desastres, englobando planejamento e diagnostico, Desenho/Projeto da solução de DR, implementação, testes, validação, documentação e treinamento, pagamento único após entrega, prazo de até 180 (cento e oitenta) dias, pagamento único pós-implantação.
Suporte: Suporte e Sustentação pós-implantação de Plano de Disaster Recovery/Recuperação de Desastres – Pagamento Único Após Entrega do **Item-12**.

Tabela 11 – Descritivos dos Itens 12 e 12.a

A Prefeitura Municipal de Campo Mourão - PR possui sistemas e dados críticos ao negócio, cuja indisponibilidade pode causar impactos operacionais, financeiros, legais e reputacionais. Este projeto visa estabelecer uma estratégia robusta de Disaster Recovery, alinhada às melhores práticas de mercado (Ex.: ISO 22301, ISO 27031, ITIL, NIST), assegurando níveis adequados de resiliência e recuperação.
Deverá ser realizado o Planejamento e Diagnóstico da Estrutura da Prefeitura Municipal de Campo Mourão a partir do Levantamento do ambiente atual: infraestrutura, aplicações, dados e dependências. Classificação de sistemas críticos. Elaboração ou revisão de BIA – Business Impact Analysis. Definição de RTO (Recovery Time Objective) e RPO (Recovery Point Objective) por serviço.
Em seguida a Empresa contratada deverá apresentar o Desenho/ projeto da solução de DR através da apresentação de uma Arquitetura de Disaster Recovery (on-premises, cloud ou híbrida). Estratégias de replicação, backup e restauração. Definição do site de contingência (ativo-ativo, ativo-passivo, warm site, cold site). Requisitos de segurança da informação e conformidade.
Na fase de Implementação, deverá ser realizada a Configuração/conferência de ferramentas de backup e replicação. Implementação de ambientes de contingência. Integração com sistemas existentes e a Criação de runbooks de recuperação (guia passo a passo que descreve como executar tarefas operacionais ou reagir a incidentes).
Após implementado deve-se prossegui com a realização de Testes e Validação onde devem ser realizados o Planejamento e execução de testes de DR (parciais e completos). Simulações de cenários de desastre. e apresentado o Relatório de resultados e ajustes necessários.
Deve ser realizado em seguida a Documentação e treinamento, com a realização de Documentação técnica e operacional completa. entrega do Manual do Plano de Disaster Recovery. e Treinamento da equipe técnica e gestores.
Deve-se manter ainda até o fim do contrato o Suporte e Sustentação que inclui Suporte pós-implantação. Acompanhamento periódico e testes recorrentes. A empresa vencedora deverá semestralmente revisar e atualizar os procedimentos desenhadas na solução de DR e atualizar a documentação. Tais revisões deverão ser realizadas após visita in-loco das dependências do licitador com a equipe de tecnologia.
Requisitos técnicos mínimos: Aderência a normas e boas práticas reconhecidas (LGPD e ISO 27001).

O prazo para execução do objeto descrito no **Item-12** será de 180 (cento e oitenta) dias, contados a partir da data da emissão da Ordem de Serviço. Durante esse período, a Contratada deverá realizar integralmente a entrega do serviço, compreendendo as seguintes fases:

- Planejamento e Diagnóstico da Estrutura;
- Desenho e Projeto da Solução de Disaster Recovery (DR);
- Implementação da Solução;
- Execução de Testes e Validação Técnica do Ambiente;
- Elaboração da Documentação Técnica Completa; e
- Treinamento da Equipe Técnica da DIRTI.

Concluído o prazo de 180 (cento e oitenta) dias, e após a validação formal de todas as fases pela DIRTI, será autorizado o pagamento em parcela única do **Item-12**, condicionado à emissão do Termo de Aceite Definitivo.

A Contratada permanecerá responsável pela prestação dos serviços de Suporte e Sustentação da solução implementada, até o término da vigência contratual, que será de 12 (doze) meses, contados da data da emissão da Ordem de Serviço, observadas as condições, níveis de serviço e demais obrigações estabelecidas no instrumento contratual.

O pagamento do **Item-12a** - Suporte e Sustentação pós-implantação fica expressamente condicionado à conclusão integral do **Item-12**, compreendendo todas as fases previstas no escopo contratual, bem como à validação formal pela DIRTI e à emissão do correspondente Termo de Aceite Definitivo.

Não será admitido pagamento antecipado, parcial, proporcional ou por etapa do **Item-12a**, ficando sua quitação vinculada, de forma inequívoca, ao aceite definitivo do **Item-12**.

O suporte técnico e a sustentação deverão ser prestados em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, com prazo máximo de atendimento presencial em até 06 (seis) horas após a abertura de chamado para incidentes críticos conforme exposto nas **Tabelas 14 e 15.**

4.14. DESCRIÇÃO TÉCNICA DO (ITEM-13)
AUDITORIA E CONSULTORIA TÉCNICA DO AMBIENTE
ESPECIFICAÇÕES TÉCNICAS

Objeto: Auditoria e Consultoria Técnica do Ambiente
Produto: Prestação de serviços continuados de processamento de dados e segurança da informação no ambiente da contratante, compreendendo atividades especializadas de monitoramento, operação assistida no ambiente de tecnologia da informação e segurança da informação, com visita técnica presencial trimestral de 04 (quatro) horas para verificação do ambiente, análise de conformidade e de vulnerabilidades e apoio técnico operacional com emissão de relatório técnico. O serviço contempla: monitoramento de segurança; criação, suporte e execução de upgrades no ambiente de virtualização, Storages, Servidores físicos, Ativos de rede, Active Directory (Ms-ad), Servidores de arquivos (file server) e Sistemas de armazenamento nas (12 meses).
Suporte: Suporte por 12 (doze) meses.

4.14.1. CARACTERÍSTICAS DOS SERVIÇOS

Prestação de serviços continuados de processamento de dados e segurança da informação no ambiente da contratante, compreendendo atividades especializadas de monitoramento, operação assistida no ambiente de tecnologia da informação e segurança da informação, com visita técnica presencial trimestral de 04 (quatro) horas para verificação do ambiente, análise de conformidade e de vulnerabilidades e apoio técnico operacional com emissão de relatório técnico. O serviço contempla: monitoramento de segurança; criação, suporte e execução de upgrades no ambiente de virtualização, Storages, Servidores físicos, Ativos de rede, Active Directory (Ms-ad), Servidores de arquivos (file server) e Sistemas de armazenamento nas (12 meses). As visitas deverão ser trimestrais, agendadas com a equipe de TI contratante, em horário comercial, podendo em situações extraordinárias serem executados fora do horário de trabalho de contratante.

O tempo de visita deverá ser de pelo menos 04 (quatro) horas, podendo se estender caso o profissional da contratada avalie sua necessidade.

Deverá será entregue mensalmente para a administração de TI da contratante um parecer técnico mensal referente as soluções de segurança contratadas, recomendações para sua melhoria e outros que julgar relevantes para manter o ambiente em padrões de segurança adequados
Os serviços deverão contemplar monitoramento, análise, manutenção preventiva, suporte técnico especializado e recomendações de melhoria contínua do ambiente de TI, abrangendo servidores, virtualização, armazenamento, diretório de usuários, servidores de arquivos (File Server) e demais componentes da infraestrutura tecnológica, incluindo:

- Monitoramento e gestão de ativos de TI: Monitoramento da disponibilidade e desempenho do Storage, servidores físicos e virtuais; monitoramento CPU, memória, armazenamento e rede; identificação de falhas e degradação de desempenho; acompanhamento e gestão de ativos de TI;
- Administração e suporte ao ambiente virtualizado: Monitoramento e suporte a plataforma de virtualização (VMWare); gerenciamento e acompanhamento de máquinas virtuais (Vms); análise de desempenho e otimização de recursos do ambiente virtual; recomendações de melhorias na arquitetura virtual;
- Administração de Storage, servidores físicos e/ou virtuais, ativos de Rede: suporte e acompanhamento do Storage, servidores físicos e/ou virtuais, ativos de rede; atualização de patches de segurança; configurações; análise de eventos, logs e falhas do sistema; apoio na resolução de incidentes e indisponibilidades;
- Gerenciamento do Active Directory (MS-AD), políticas de domínio e autenticação: administração do ambiente MS-AD primário e secundário; Verificação de políticas de grupo (GPOs); monitoramento de autenticação, permissões e controle de acesso;
- Administração de sistemas de armazenamento próprios (NAS): monitoramento de sistemas NAS ou demais soluções de armazenamento; configuração de rotinas de backup para esses equipamentos; análise de capacidade, desempenho e disponibilidade; expansão ou reorganização do armazenamento;
- Segurança da Informação: Análise de logs e eventos de segurança; Verificação de vulnerabilidades e recomendações de mitigação; Apoio técnico na resolução de incidentes de segurança ou indisponibilidade de serviços; Avaliação de desempenho e disponibilidade dos sistemas; Orientações para boas práticas de segurança da informação;
- Elaboração de relatórios técnicos periódicos contendo diagnóstico do ambiente, ações realizadas e recomendações de melhorias; Avaliação da necessidade de upgrades tecnológicos; eventuais falhas ou vulnerabilidades identificadas; e
- Todas as despesas relacionadas a deslocamento, transporte, alimentação e hospedagem necessárias à execução dos serviços deverão estar integralmente incluídas no valor apresentado pela contratada, não sendo permitido qualquer tipo de cobrança adicional durante a vigência contratual.

O suporte técnico deverá ser prestado em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, com prazo máximo de atendimento presencial em até 06 (seis) horas após a abertura de chamado para incidentes críticos conforme exposto nas **Tabelas 14 e 15.**

5. DESCRIÇÃO DA SOLUÇÃO COMPLETA, CONSIDERANDO-SE TODO O CICLO DE VIDA DO OBJETO

A solução deverá ser executada considerando-se o objeto desta contratação mediante as especificações mínimas exigidas no instrumento convocatório, para as fases do ciclo de vida a seguir.

5.1. ANÁLISE DO AMBIENTE

A Contratada deverá realizar diagnóstico técnico detalhado do ambiente tecnológico existente, identificando riscos, vulnerabilidades, dependências e necessidades operacionais. Deverá ser apresentado Documento Técnico contendo a metodologia de implantação, plano de integração com o ambiente atual e cronograma de execução da solução contratada, considerando-se obrigatoriamente a manutenção da continuidade operacional de toda a infraestrutura durante o processo de implantação. O documento deverá ser submetido à aprovação da Diretoria de Tecnologia da Informação antes do início da fase seguinte.

5.2. IMPLANTAÇÃO

Compreende registro e ativação das licenças no ambiente tecnológico existente, integrando-se aos sistemas e equipamentos já em operação, mediante instalação, configuração e integração de todos os equipamentos e sistemas previstos. Implantação dos firewalls e importação/configuração de políticas de segurança pré-existentes. Implantação das soluções de backup local e em nuvem. Implantação da redundância de serviços críticos (AD e arquivos). Implementação do plano de recuperação de desastres. Instalação das soluções de antivírus, EDR, gerenciamento de logs e Help Desk.

5.3. CAPACITAÇÃO

Deverá ser realizado treinamento técnico à equipe designada pela Administração, contemplando: operação, administração e as boas práticas de utilização das soluções de TI implantadas. A Realização do repasse de conhecimento deverá ser executada de forma presencial com carga horaria específica para cada item licitado conforme descritivo técnico.

5.4. OPERAÇÃO

A Contratada deverá acompanhar de forma contínua o funcionamento de todas as soluções implantadas, realizando monitoramento preventivo do ambiente, análise de desempenho, verificação de disponibilidade, acompanhamento de alertas de segurança e atuação proativa na mitigação de incidentes. Deverá também promover revisões periódicas das políticas de segurança, regras de firewall, parâmetros de backup, retenção de dados, integridade das replicações, funcionamento do ambiente de alta disponibilidade (HA), desempenho das soluções de antivírus e EDR, consistência da coleta e armazenamento de logs, bem como o correto funcionamento do sistema de Help Desk e suporte remoto. Realização de Visitas Técnicas Presenciais Mensais. Caberá ainda à Contratada apoiar a Administração na análise de eventos críticos, recomendações de ajustes técnicos, aplicação de boas práticas de segurança da informação, emissão de relatórios gerenciais periódicos e orientação técnica para melhoria contínua do ambiente, assegurando estabilidade, desempenho e aderência às políticas institucionais de segurança e continuidade operacional.

5.5. MANUTENÇÃO

Compreende a atualização de versões, aplicação de patches de segurança, correção de falhas, substituição de equipamentos em caso de defeito (quando em comodato) e prestação de suporte técnico, auditoria durante todo o período de vigência contratual, garantindo eficiência, disponibilidade e segurança das soluções implementadas: Encerramento, Transição e Disponibilidade e Portabilidade de Dados.

Ao final do contrato e/ou em caso de rescisão ou revogação, a Contratada deverá prestar apoio técnico para exportação integral de dados, usuários, regras, políticas, configurações e demais informações necessárias, de forma estruturada e documentada, possibilitando futura importação, migração ou consulta pela Prefeitura Municipal de Campo Mourão – PR.

A transição deverá ocorrer sem prejuízo à integridade, confidencialidade e disponibilidade das informações, e sem ônus adicional dentro da vigência contratual.

6. REQUISITOS DA CONTRATAÇÃO

O fornecedor deverá entregar os itens no prazo estipulado no Termo de Referência, bem como informar a contratada sobre as intercorrências de problemas com o referido prazo.

Não será admitida a subcontratação dos objetos contratuais.

A contratada deverá preencher todos os requisitos de regularidade jurídica, fiscal, técnica e econômico-financeira, previstos na Lei nº 14133/2021.

6.1. ATESTADO DE CAPACIDADE TÉCNICA

O atestado de capacidade técnica deverá ser fornecido por pessoa jurídica de direito público ou privado, devidamente assinado pelo responsável preferencialmente por assinatura eletrônica, para fins de auditoria, nos termos da legislação vigente.

Para fins de comprovação, serão considerados contratos vigentes ou encerrados nos últimos 05 (cinco) anos. A comprovação deverá demonstrar experiência em serviços compatíveis com o objeto da contratação, abrangendo, no mínimo: **Itens 1, 1.a, 2, 2.a** (Serviços de Backups); **Itens 3, 3.a, 4, 4.a e 5, 5.a** (Serviços de Segurança via Equipamentos de Firewalls); e os **Itens 7, 7.a e 9, 9.a** (Antivírus Corporativo e EDR).

Informamos ainda, para todos os fins que as empresas proponentes deverão apresentar atestados perfazendo um total mínimo de 50% (cinquenta por cento) do teto máximo de quantitativos indicados no objeto mediante os itens em epígrafe, que ainda assim estarão aprovados conforme previsto na legislação pertinente a matéria, conforme transcrito no Termo de Referência, no Edital de Licitações e seus Anexos.

6.2. DECLARAÇÃO DE VIABILIDADE DE ATENDIMENTO TÉCNICO

Este documento referente a "**Declaração de Viabilidade de Atendimento Técnico"**, refere-se ao ateste da capacidade da empresa proponente como prestadora de serviços de TI, onde compromete-se e garante técnica e juridicamente que possui os recursos necessários para fazer frente ao que preconiza o item em epígrafe, visando-se atender a todas demandas de chamados técnicos abertos pela Diretoria de TI e demais setores, dentro do prazo estabelecido no SLA do instrumento convocatório, que é de 24x7x6. Com isso, tem-se que a apresentação deste documento no credenciamento das empresas, durante o certame licitatório, é obrigatória.

6.3. Os serviços técnicos especializados que farão parte da implementação da solução completa e deverão seguir as especificações técnicas detalhadas no Termo de Referência, no Edital de Licitações e seus Anexos.

6.4. Os bens de Tecnologia da Informação deverão ser entregues instalados, configurados e testados para pleno uso conforme previsto no instrumento convocatório.

6.5. É mandatária a apresentação de Marca/Modelo dos Equipamentos/ Licenças dos Softwares que serão ofertados nas propostas pelos possíveis fornecedores no Certame Licitatório.

6.6. Atualmente a Prefeitura Municipal de Campo Mourão dispõe da solução de Appliance UTM firewall concentrador Sophos, adotada como solução padrão de firewall para o controle de ameaças digitais em sua rede com 04 (quatro) equipamentos já instalados. Todo esse conjunto é gerenciado por um servidor central. A solução vem sendo utilizadas com elevada taxa de sucesso tendo reduzido a praticamente zero o número de incidentes ataques virtuais em nossa rede, além de gerar maior visibilidade à rede. Com isso faz-se necessário a ampliação de uso destas licenças de forma a padronizar as configurações e uniformizar o gerenciamento da solução.

6.7. Sendo assim fica estabelecido os requisitos para contratação dos **Itens-3, 4 e 5** (Firewall Concentrador Paço Municipal, Firewall Concentrador Redundante em (HA) e Firewall de Borda para Unidades Essenciais), impreterivelmente a Solução de serviços de segurança para controle de ameaças virtuais "appliance utm firewall concentrador" deverá ser fornecido por um único fabricante **Sophos Ltd.** Ou seja, a solução a ser adotada deverá ser a mesma já utilizada anteriormente pelo Órgão, a manutenção da solução atualmente adotada justifica-se pela necessidade de padronização tecnológica, garantia de interoperabilidade com o ambiente já implantado em 3 (três) unidades administrativas — que atendem a mais de uma centena de computadores — e preservação da eficiência administrativa. Tal medida encontra fundamento no art. 40, §1º, inciso I, da Lei nº 14.133/2021, que admite a indicação de marca ou modelo quando tecnicamente justificada a padronização, conforme demonstrado no Estudo Técnico Preliminar, para a garantia da padronização tecnológica, interoperabilidade com o ambiente existente e preservação da eficiência administrativa.
Ressalte-se ainda que os produtos atuais tem atendido tecnicamente a todos os requisitos previstos para a solução de serviços de segurança para controle de ameaças virtuais Appliance UTM firewall

((concentrador, redundante em (HA) e Firewalls de Borda)) e com qualidade técnica demonstrada no ambiente real de produção, o que tem dado a tranquilidade necessária aos órgãos para operar de forma protegida das ameaças virtuais existentes e daquelas que surgem a cada dia.
Todas as regras de Firewall, Regras NAT, lista de URLs, Políticas e demais configurações pré-existentes na estrutura deverão ser migradas, exportadas e/ou refeitas para que não haja impacto na Estrutura como um todo.
A escolha da continuidade de uso dessas soluções em conjunto se dá também pelo fato de que a Prefeitura Municipal de Campo Mourão já possui em sua estrutura pré-estabelecidas diversas regras de navegação, regras de firewall, políticas de autenticação, regras de NAT, listas de URLs e categorias entre outras funcionalidades, logo, a sua substituição poderá gerar prejuízos à economicidade e à eficiência dos processos e procedimentos do órgão, com a mácula inclusive do interesse público. Uma eventual substituição acarretaria um novo processo de implantação, treinamento, adaptação, estabelecimento e criação de todas regras e políticas que ocorreria em um longo período de tempo, isso porque o novo objeto contratado ainda abrangerá a TODOS os Prédios do Município, além de nova capacitação da equipe técnica completa para gerir a solução (software) contratada.
A continuidade da solução permite, ainda, o aproveitamento do conhecimento técnico prévio já consolidado por parte da equipe operacional, otimização do suporte técnico e manutenção do gerenciamento centralizado, evitando retrabalho, riscos de descontinuidade e custos adicionais decorrentes de eventual substituição integral da plataforma, entendimento este alinhado à jurisprudência do Tribunal de Contas da União, inclusive conforme consolidado na Súmula nº 270.
A manutenção da solução assegurará otimização e padronização ao ambiente da Prefeitura Municipal de Campo Mourão, sendo mais vantajoso em termos de custo, uma vez que já existe um conhecimento técnico prévio das funcionalidades da solução e da sua administração.
Ainda no que diz respeito aos **Itens-3 e 4** a implantação e as instalações deverão ser realizadas por profissional certificado pelo fabricante de forma presencial nas dependências da Prefeitura Municipal de Campo Mourão – PR em data e hora a ser definida pela DIRTI (Diretoria de Tecnologia da Informação), de modo a não interromper o funcionamento geral da rede, tendo em vista que a necessidade de Alta disponibilidade que o órgão possui por ser o Concentrador. Com relação ao **Item-5** – a implantação e as instalações deverão ser realizadas por profissional certificado pelo fabricante de forma presencial nas dependências das Unidades Essenciais (**UPA e PALP**) tendo em vista a alta demanda das referidas localidades, deverá ser realizado em horários de baixo fluxo de atendimento (após as 22:00 horas por exemplo) com agendamento prévio em data e hora a ser definida pela DIRTI (Diretoria de Tecnologia da Informação), de modo a não interromper o funcionamento da rede e garantir o mínimo impacto possível na infraestrutura tecnológica e na continuidade da prestação de serviço de ambos os locais.
Como referência técnica para fornecimentos dos **Itens 3, 4 e 5**, informamos que, atualmente a municipalidade, através da Diretoria de TI, faz uso das soluções: 01 (um) equipamento de hardware firewall concentrador appliance UTM (Unified Threat Management) com licenciamento de firewall concentrador, ips, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para appliance de firewall de próxima geração com suporte e atualização de versões durante a vigência contratual, instalado no local como **FIREWALL CONCENTRADOR PAÇO MUNICIPAL (Item-1)**; 01 (um) equipamento de hardware firewall concentrador appliance UTM (Unified Threat Management) com licenciamento de firewall concentrador redundante de Alta Disponibilidade (HA), ips, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para appliance de firewall de próxima geração com suporte e atualização de versões durante a vigência contratual, instalado no local como **FIREWALL CONCENTRADOR PAÇO MUNICIPAL em (HA)**; e 02 (dois) equipamentos de hardware firewall de borda appliance UTM licenciamento de firewall, ips, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para appliance de firewall de próxima geração com suporte e atualização de versões, instalados na **UPA** e **PALP** como **FIREWALL DE BORDA PARA UNIDADES COM SERVIÇOS ESSENCIAIS**. Todas estas soluções operacionalizam a segurança da rede de computadores em mais de 100 (cem) prédios públicos contra invasões nos ambientes de TI que possam culminar no sequestro de dados e informações em todos estes locais municipalidade, como o caso do **ransonware e malware**.

Dessa maneira, informa-se que a solução atual já descrita e justificada acima, deverá ser mantida com a mesma especificação técnica mínima exigida de modelo/ marca **SOPHOS LTD**.
As empresas participantes deverão comprovar que dispõe de equipe técnica qualificada, composta por no mínimo 03 (três) profissionais certificados pelo fabricante da solução ofertada, aptos a prestar atendimento especializado durante toda a vigência contratual.
A comprovação deverá ocorrer mediante demonstração de vínculo profissional ou contratual que assegure a efetiva disponibilidade dos técnicos para execução do objeto.
O suporte técnico deverá ser prestado em regime 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, com prazo máximo de atendimento presencial em até 06 (seis) horas após a abertura de chamado para incidentes críticos conforme exposto nas **Tabelas 14 e 15.**

6.8. Requisitos da Contratação – **Item-6** - Atualmente a Prefeitura Municipal de Campo Mourão dispõe das licenças da Ferramenta de Suporte Remoto "Help Desk", sendo utilizadas para acesso a Equipamentos Lotados nos diversos Prédios da Prefeitura de Campo Mourão. A solução vem sendo utilizadas com elevada taxa de sucesso permitindo a resolução de Chamados Técnicos sem a necessidade de deslocamento dos Técnicos da Diretoria de Tecnologia da Informação. Com a Unificação de todo Corpo Técnico que compõe a Diretoria de Tecnologia da Informação e a Unificação da Prestação de Atendimento Técnico dos mais de 100 (cem) prédios do Município, dessa forma a utilização do Suporte Remoto se tornou imprescindível para a otimização e rapidez no atendimento, dessa forma faz-se necessário a ampliação de uso destas licenças de forma a padronizar as configurações e uniformizar o gerenciamento da solução.
A solução a ser adotada será a mesma já adquirida, como forma de manter a compatibilidade técnica e a padronização da solução já instalada em mais de uma centena de computadores/locais, o que permite um melhor aproveitamento do conhecimento técnico já adquirido pelo corpo técnico operativo destes órgãos e da capacidade consultiva e de suporte, suporte tal medida encontra fundamento no art. 40, §1º, inciso I, da Lei nº 14.133/2021, que admite a indicação de marca ou modelo quando tecnicamente justificada a padronização, conforme demonstrado no Estudo Técnico Preliminar, para a garantia da padronização tecnológica e preservação da eficiência administrativa.
Ressalte-se ainda que o produto atual tem atendido tecnicamente a todos os requisitos previstos para a solução de Suporte Remoto "Help Desk" e com qualidade técnica demonstrada no ambiente real de produção.
A escolha da continuidade de uso dessa ferramenta se dá também pelo fato de que a Prefeitura Municipal de Campo Mourão já possui grande parte do seu parque computacional instalado por estas soluções totalizando mais de 1800 (mil e oitocentos) equipamentos instalados, logo, a sua substituição poderá gerar prejuízos à economicidade e à eficiência dos processos e procedimentos do órgão, com a mácula inclusive do interesse público. Uma eventual substituição acarretaria um novo processo de implantação, instalação nas máquinas clientes, treinamento e adaptação que ocorreria em um longo período de tempo, devido ao tamanho da rede e a quantidade de localidades atendidas por ela, nova capacitação da equipe técnica para gerir a nova ferramenta (software), além da necessidade de treinamento dos usuários finais os quais serão atendidos de forma remota.
A renovação da manutenção das soluções assegurará otimização, agilidade e padronização ao ambiente da Prefeitura Municipal de Campo Mourão, sendo mais vantajoso em termos de custo, uma vez que já existe um conhecimento técnico e dos usuários finais das funcionalidades da solução.
Sendo assim impreterivelmente, o Software de sistema para suporte remoto "Help Desk" deverá ser fornecido por um único fabricante **TEAM VIEWER.**
O suporte técnico deverá ser prestado em regime 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana por semana, com prazo máximo de atendimento presencial de até 06 (seis) horas, conforme exposto nas **Tabelas 14 e 15.**

6.9. Requisitos da Contratação – **Item-7** - Atualmente a Prefeitura Municipal de Campo Mourão dispõe das licenças da solução de antivírus **WITHSECURE ELEMENTS PREMIUM** (antiga **F-SECURE**), adotada como solução padrão de antivírus corporativo para o controle de ameaças digitais nos

servidores de rede e estações de trabalho cujo módulo possui mais de 1500 (mil e quinhentas) licenças instaladas. Todo esse conjunto é gerenciado por um servidor central.
A solução vem sendo utilizadas com elevada taxa de sucesso tendo reduzido a praticamente zero o número de incidentes devido a vírus e outras ameaças virtuais nas estações de trabalho e servidores, além de gerar maior visibilidade à rede. Com isso faz-se necessário a ampliação de uso destas licenças de forma a padronizar as configurações e uniformizar o gerenciamento da solução.
A solução a ser adotada será a mesma já adquirida, como forma de manter a compatibilidade técnica e a padronização da solução já instalada em mais de uma centena de computadores/locais, o que permite um melhor aproveitamento do conhecimento técnico já adquirido pelo corpo técnico operativo destes órgãos e da capacidade consultiva e de suporte tal medida encontra fundamento no art. 40, §1º, inciso I, da Lei nº 14.133/2021, que admite a indicação de marca ou modelo quando tecnicamente justificada a padronização, conforme demonstrado no **Estudo Técnico Preliminar**, para a garantia da padronização tecnológica e preservação da eficiência administrativa.
Ressalte-se ainda que o produto atual tem atendido tecnicamente a todos os requisitos previstos para a solução de segurança e com qualidade técnica demonstrada no ambiente real de produção, o que tem dado a tranquilidade necessária aos órgãos para operar de forma protegida das ameaças virtuais existentes e daquelas que surgem a cada dia.
A escolha da continuidade de uso destas suítes de proteção contra códigos maliciosos e visibilidade se dá também pelo fato de que a Prefeitura Municipal de Campo Mourão já possui o seu parque computacional protegido e instalado por estas soluções, logo, a sua substituição poderá gerar prejuízos à economicidade e à eficiência dos processos e procedimentos do órgão, com a mácula inclusive do interesse público. Uma eventual substituição acarretaria um novo processo de implantação, treinamento e adaptação que ocorreria em um longo período de tempo, devido ao tamanho da rede e a quantidade de localidades atendidas por ela, além de nova capacitação da equipe técnica para gerir a nova ferramenta (software).
A renovação da manutenção das soluções assegurará otimização e padronização ao ambiente da Prefeitura Municipal de Campo Mourão, sendo mais vantajoso em termos de custo, uma vez que já existe um conhecimento técnico das funcionalidades da solução e da sua administração.
Impreterivelmente, todos os componentes que fazem parte da solução de segurança para servidores de rede e estações de trabalho deverão ser fornecidos por um único fabricante **WITHSECURE ELEMENTS PREMIUM** (antiga **F-Secure**) devendo o mesmo ser compatível para utilização em S.Os Windows ou Linux.
As empresas participantes deverão comprovar que dispõe de equipe técnica qualificada, composta por no mínimo 03 (três) profissionais certificados pelo fabricante da solução ofertada, aptos a prestar atendimento especializado durante toda a vigência contratual.
Exigir no momento do Credenciamento dos possíveis Fornecedores a apresentação de Carta do Fabricante apontando que a Empresa é autorizada e certificada para o fornecimento do Item.
A comprovação deverá ocorrer mediante demonstração de vínculo profissional ou contratual que assegure a efetiva disponibilidade dos técnicos para execução do objeto.
O suporte técnico deverá ser prestado em regime 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana por semana, com prazo máximo de atendimento presencial de até 06 (seis) horas, conforme exposto nas **Tabelas 14 e 15.**

6.10. Requisitos de contratação do **Item-9** – Software de sistema para detecção e resposta endpoint EDR (ENDPOINT DETECTION AND RESPONSE/DETECÇÃO E RESPOSTA DE ENDPOINT) para implementar solução de segurança cibernética avançada e monitorar continuamente dispositivos finais para detectar comportamentos suspeitos, investigar ameaças em tempo real e responder automaticamente a incidentes como ransonware e malwares em equipamentos estações de trabalho da rede (computadores), sendo 25 (vinte e cinco) equipamentos por 12 (doze) meses. O EDR é parte integrante e adicional do **Item-7**, assim deverão ser fornecidos por um único fabricante **WITHSECURE ELEMENTS PREMIUM** (antiga **F-Secure**) devendo o mesmo ser compatível para utilização em S.O.s Windows ou Linux. Será exigido no momento do credenciamento dos possíveis fornecedores a

apresentação de Carta do Fabricante apontando que a Empresa é autorizada e certificada para o fornecimento do item do objeto do Edital de Licitações.
As empresas participantes deverão comprovar que dispõem de equipe técnica qualificada, composta por no mínimo 03 (três) profissionais certificados pelo fabricante da solução de **EDR** ofertada, aptos a prestar atendimento especializado durante toda a vigência contratual.
O suporte técnico deverá ser prestado em regime 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana por semana, com prazo máximo de atendimento presencial de até 06 (seis) horas, conforme exposto nas **Tabelas 14 e 15.**

6.11. Requisitos de contratação do **Item-10** – Software de sistema para abertura de chamados tipo "Help Desk" para solicitações internas e gerenciador de tarefas, deverá ser operacionalizado em nuvem. O suporte técnico deverá ser prestado em regime 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana por semana, com prazo máximo de atendimento presencial de até 06 (seis) horas, conforme exposto nas **Tabelas 14 e 15.**
6.12. Requisitos de contratação do **Item-11** – A prestação dos serviços de implantação física e lógica de redundância de servidores de rede (AD e File Server) ocorrerá sob demanda, mediante solicitação da CONTRATANTE, por meio de abertura de chamado técnico, conforme a necessidade da Administração. O pagamento será realizado apenas pelo serviço efetivamente executado.

6.13. Requisitos de contratação do **Item-12** – A implementação do plano de DR – Disaster Recovery no que tange o planejamento e o diagnóstico, ocorrerá em até 180 (cento e oitenta) dias, implementação, de verá cumprir as etapas de testes, validação, documentação e treinamento. A posteriori, os demais 180 (cento e oitenta) dias de prazo contratual serão utilizados para suporte e sustentação pós-implantação de plano de Disaster Recovery/Recuperação de Desastres. O suporte técnico e a sustentação (**Item 12.a**) deverão ser prestados em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, com prazo máximo de atendimento presencial em até 06 (seis) horas após a abertura de chamado para incidentes críticos conforme exposto nas Tabelas 14 e 15.

6.14. Requisitos de contratação do **Item-13** – Prestação de serviços continuados de processamento de dados e segurança da informação no ambiente da CONTRATANTE preconizará a verificação, análise de conformidade e orientação técnica especializada, com emissão de relatório técnico. O serviço contempla: monitoramento de segurança, suporte e execução de upgrades no ambiente de virtualização (incluindo a Criação de Novas Vms), storages, servidores físicos, ativos de rede, Active Directory (MS-AD), servidores de arquivos (File Server) e sistemas de armazenamento NAS. O suporte técnico deverá ser prestado em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, com prazo máximo de atendimento presencial em até 06 (seis) horas após a abertura de chamado para incidentes críticos conforme exposto nas Tabelas 14 e 15.

6.15. Nesse sentido, a escolha das ferramentas/equipamentos apresentadas baseia-se em critérios estritamente técnicos e operacionais, visando assegurar a continuidade, a eficiência e a economicidade, sem prejuízo à competitividade do certame.

6.16. Requisitos Gerais da Contratação (comuns a TODOS os Itens):
Deverá ser disponibilizada pela Contratada, ferramenta de abertura de chamados (help desk) com acesso Web para registro das solicitações da Equipe da Diretoria de Tecnologia da Informação e caso necessário dos diversos órgãos da contratante em ambiente on-line na web com uso de navegadores de internet diversos, com as seguintes características mínimas:
Possibilitar abertura de chamados com acompanhamento pelos técnicos da contratante com dados do operador do chamado, número do chamado, assunto, data de abertura, status do chamado com envio dos chamados via e-mail. Quando solicitados pela contratante o software deve possuir capacidade de geração de relatórios com os seguintes itens mínimos:

- Chamados abertos por período por analista, colaborador, setor com data de abertura, fechamento e status;

- Listagem de chamados com interação por analista e colaborador;
- Análise de tempo de resposta por chamado com primeira resposta, última resposta e tempo de chamado total;
- Avaliação dos atendimentos por analista;
- Chamados pendentes; e
- Estatísticas dos chamados abertos por mês e por hora de chamado.

Para a manutenção da segurança de dados e senhas usadas no ambiente da contratante a contratada deverá comprovar possuir software de gerenciamento de senhas corporativas para uso de todos os seus funcionários com autenticação de dois fatores, relatórios de atividades para auditoria de segurança e console de administrador, devendo a licitante armazenar todas as informações de login e senha que a licitadora fornecer, nessa plataforma criptografada.

A contratada deverá possuir estrutura para atendimento emergencial presencial, bem como ferramenta de acesso remoto compatível com ambientes Windows e Linux, que utilize criptografia de dados segura (256 bits) ou superior, Acesso através de firewalls e rede em nat sem necessidade de criação de regras internas na rede, deverá possibilitar múltiplas conexões simultâneas, com capacidade de registro das sessões (gravação) para fins de auditoria e operação em ambientes protegidos por firewall e NAT, sem comprometer a segurança da rede.

Devido à necessidade de que a implantação e a configuração dos objetos da nova solução ocorram de forma simultânea à operação da infraestrutura atualmente em funcionamento, garantindo a continuidade dos serviços e evitando interrupções no ambiente produtivo, a contratada será integralmente responsável pelo fornecimento de todos os materiais, acessórios, dispositivos e demais recursos necessários para viabilizar a instalação, integração e testes da solução durante o período de transição. Essa responsabilidade inclui, quando necessário, o fornecimento de cabos de rede, patch cords, módulos de conexão, adaptadores, transceptores, equipamentos auxiliares, racks provisórios, dispositivos de interligação, ferramentas técnicas, bem como quaisquer outros componentes ou insumos indispensáveis para a realização das atividades de instalação, configuração, testes, migração e validação do ambiente.

A disponibilização desses materiais deverá permitir que a nova solução seja implantada e testada paralelamente à estrutura atualmente em operação, possibilitando a realização de todos os procedimentos técnicos necessários sem comprometer o funcionamento da estrutura existente. O objetivo é assegurar que todo o processo de implantação, validação e preparação para entrada em produção ocorra de forma controlada, segura e sem impactos à continuidade dos serviços prestados pela Prefeitura.

Todos os materiais utilizados durante essa fase deverão atender às especificações técnicas compatíveis com a infraestrutura da contratante e com os equipamentos implantados, garantindo desempenho adequado, confiabilidade e segurança na operação. Eventuais recursos utilizados temporariamente para viabilizar a implantação da estrutura paralela poderão ser removidos ou quando necessário incorporados de forma adequada ao ambiente definitivo sem custos adicionais a Contratante, conforme orientação da equipe técnica da Diretoria de Tecnologia da Informação (DIRTI), após a conclusão da etapa de migração e ativação definitiva da solução.

O suporte técnico deverá ser prestado em regime 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana por semana, com prazo máximo de atendimento presencial de até 06 (seis) horas, conforme exposto nas **Tabelas 14 e 15.**

7. MODELO DE EXECUÇÃO DO OBJETO

A CONTRATADA deverá prestar os serviços, durante o período de 12 (doze) meses.

A CONTRATADA deverá se apresentar, ao Gestor e/ou Fiscais da CONTRATANTE, em até 05 (cinco) dias úteis após a emissão da Ordem de Serviço:

Um preposto administrativo/gerencial, com poder de gestão e facilidade de localização (indicando, no mínimo, nome, endereço eletrônico e telefone de contato), responsável por representar a CONTRATADA, prestar esclarecimentos e atender às reclamações que eventualmente surgir em durante a execução do contrato.

Canais de contato (indicando, no mínimo, endereço eletrônico e telefone, inclusive telefone móvel plantonista) a serem utilizados pela CONTRATANTE para solicitações relativas aos serviços.
- Início da execução do objeto será no prazo de até 10 (dez) dias, contados do recebimento da Ordem de Serviço.
- O serviço de implantação, instalação e configuração da solução deverá ser executado presencialmente nas dependências da contratante por profissionais da empresa contratada. A entrada definitiva em produção da solução somente poderá ocorrer após o encerramento dos contratos atualmente vigentes, de modo a garantir a continuidade dos serviços e evitar sobreposição contratual.
Com o objetivo de assegurar a adequada transição entre as soluções, permitir a realização de testes, ajustes de configuração, migração de regras e validação do funcionamento do ambiente, a contratada deverá concluir as atividades de implantação da solução contratada com prazo de até 45 (quarenta e cinco) dias a partir da emissão da Ordem de Serviço.
Durante esse período de transição, todas as atividades de instalação, configuração, parametrização, testes e validações deverão ser realizadas sem interferir no funcionamento do ambiente atualmente em produção, não sendo permitida o desligamento da solução vigente antes da conclusão do pleno funcionamento, não ultrapassando o término do contrato atual.
A ativação definitiva da nova solução somente poderá ocorrer após a conclusão dos testes de funcionamento, validação pela equipe técnica da contratante e encerramento formal do contrato anterior, garantindo que a nova infraestrutura esteja plenamente operacional na data de término da vigência do contrato vigente.
Caso a empresa vencedora do certame seja a mesma atualmente responsável pelos equipamentos e serviços já em operação, a contratação destes poderá ocorrer somente ao término da vigência contratual atualmente vigente, de forma a evitar sobreposição contratual e prejuízo à Administração.

8. PRAZOS PARA A EXECUÇÃO DOS SERVIÇOS – ACORDO DE NÍVEL DE SERVIÇO (SLA)

Para a realização dos atendimentos a **CONTRATANTE** através dos serviços especializados de suporte técnico, a **CONTRATADA**, deverá seguir os seguintes conceitos pré-definidos:

8.1 TEMPO DE INÍCIO DE ATENDIMENTO

Prazo decorrido entre a abertura do chamado efetuada pela PREFEITURA MUNICIPAL DE CAMPO MOURÃO à prestadora de serviço e o efetivo início dos trabalhos de assistência técnica.

8.2 TEMPO DE SOLUÇÃO DE ATENDIMENTO

Prazo decorrido entre a abertura do chamado pela PREFEITURA MUNICIPAL DE CAMPO MOURÃO e o restabelecimento da solução em pleno estado de funcionamento, garantindo a normalização do serviço afetado. Os níveis de criticidade do atendimento serão definidos conforme segue.

8.3 NÍVEL CRÍTICO

Representa um incidente crítico que possa tornar inoperante qualquer serviço de Tecnologia da Informação envolvido nesta Contratação essencial à manutenção dos sistemas e da atividade finalística da PREFEITURA MUNICIPAL DE CAMPO MOURÃO.

8.4 NÍVEL URGENTE

Representa um incidente que está causando ou irá causar uma degradação do ambiente operacional. Apesar da degradação, continuam em operação os serviços essenciais para a manutenção dos sistemas e da atividade finalística da PREFEITURA MUNICIPAL DE CAMPO MOURÃO.

8.5 NÍVEL ROTINA

Representam falhas mínimas que não estão afetando o desempenho, serviço ou operação dos sistemas e da atividade finalística da PREFEITURA MUNICIPAL DE CAMPO MOURÃO, ou ainda a função afetada só é usada eventualmente ou temporariamente.

8.6 MÉTRICAS PARA ACOMPANHAMENTO DE SLA

De acordo, então, como os níveis de criticidade apresentados durante a abertura do chamado, fica então definidos os prazos de atendimento e de solução pela CONTRATADA, contados a partir da data e horada abertura do chamado pela CONTRATANTE, conforme a Tabela a seguir:

8.6.1 ANÁLISES DAS CRITICIDADES E PRAZOS DE ATENDIMENTOS

Nível de Criticidade	Prazos de Atendimentos
Crítico	Prazo de 06 (seis) horas para início do atendimento presencial. Prazo de 12 (doze) horas para solução definitiva do incidente.
Urgente	Prazo de 08 (oito) horas para início do atendimento presencial. Prazo de 16 (dezesseis) horas para solução definitiva do incidente.
Rotina	Prazo de 48 (quarenta e oito) horas para início do atendimento presencial. Prazo de 96 (noventa e seis) horas para solução de definitiva do incidente.

Tabela 14 – Níveis de Criticidade x Prazos de Atendimentos

Nos casos em que não seja possível a solução definitiva dentro do prazo estabelecido, a contratada deverá apresentar solução de contorno (workaround) que restabeleça temporariamente o funcionamento do serviço afetado, devendo a solução definitiva ser implementada no menor prazo possível, mediante alinhamento com a equipe técnica da contratante.
A empresa contratada deverá fornecer por escrito (e-mail ou portal Web), independente da forma de abertura do chamado utilizada pela DIRTI da PREFEITURA MUNICIPAL DE CAMPO MOURÃO, comprovante da solicitação de chamado, onde devem estar claramente indicados a data e o horário de abertura do chamado e o problema relatado.
O não cumprimento dos prazos estabelecidos no Acordo de Nível de Serviço (SLA) caracterizará descumprimento contratual, sujeitando a CONTRATADA à aplicação de penalidades, sem prejuízo das demais sanções previstas na legislação vigente e no contrato.
Sempre que houver descumprimento dos prazos de início de atendimento ou de solução estabelecidos para os chamados classificados nos níveis de criticidade definidos neste instrumento, será aplicada multa proporcional no valor do item do contrato, garantindo-se o contraditório e a ampla defesa, conforme os seguintes critérios:

8.6.2 ANÁLISES DAS CRITICIDADES E PENALIDADES POR OCORRÊNCIAS

Nível de Criticidade	Penalidade por Ocorrência
Crítico	Desconto de 5% do valor do item(s) de contrato por ocorrência
Urgente	Desconto de 3% do valor do item(s) de contrato por ocorrência
Rotina	Desconto de 1% do valor do item(s) de contrato por ocorrência

Tabela 12 – Níveis de Criticidade por Ocorrências x Penalidades

Durante a vigência contratual, a CONTRATADA através da Diretoria de Tecnologia da Informação, efetuará a aferição dos níveis de serviços conforme estipulado no SLA descrito no instrumento convocatório. Nesse sentido, ressalta-se que para os casos de penalidades cumulativas, será considerado como teto máximo para aplicação de multas, o valor percentual de 20% (vinte por cento) sobre o valor correspondente ao total do contrato de prestação de serviços.

9. VISITA TÉCNICA

É facultada ao licitante a visita e verificação do (s) Ambiente(s) onde os equipamentos e a prestação de serviço será executada, caso haja a realização da visita a LICITANTE PROPONENTE deverá apresentar ATESTADO DE VISITA TÉCNICA (Modelo Anexo IV), emitido pela fiscalização da

CONTRATANTE, atestando que a licitante realizou visita técnica no local da prestação dos serviços, visando ao perfeito conhecimento dos objetos ora licitados ou, alternativamente caso a empresa venha a se eximir da realização da visita deverá incluir a DECLARAÇÃO FORMAL DE DISPENSA DE VISITA (Modelo Anexo V) assinada pelo responsável legal da proponente, sob as penalidades da lei, de que tem pleno conhecimento das condições e do grau de dificuldade existentes, assumindo total responsabilidade por esse fato e informando que não o utilizará para quaisquer questionamentos futuros que ensejem avenças técnicas ou financeiras com a contratante.
Tendo em vista a faculdade da realização de vistoria, os licitantes não poderão alegar o desconhecimento das condições e do grau de dificuldade existentes como justificativa para se eximirem das obrigações assumidas.
A Visita Técnica deverá ser previamente agendada, por e-mail depti@campomourao.pr.gov.br, e/ou telefones (44)35181139 / (44) 35181173, em horário comercial, com pelo menos 3 (três) dias úteis de antecedência.

10. MODELO DE GESTÃO DO CONTRATO

As comunicações entre a contratante e a contratada devem ser realizadas por escrito ou via chamado sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica ou plataforma de abertura de chamados própria da Contratada para esse fim.
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.
A execução do Contrato deverá ser acompanhada e fiscalizada pelo Gestor e Fiscal.

11. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

Após o fornecimento dos objetos contratados, a empresa contratada deverá emitir nota fiscal em nome do Município de Campo Mourão (CNPJ n.º 75.904.524/0001-06) e/ou do Fundo Municipal de Saúde (CNPJ n.º 09.253.109/0001-05), a depender do órgão solicitante, de maneira que deverá ser indicado ainda no corpo da nota o número do empenho, o número e nome do banco, agência e número da conta, na qual deverá ser feito o pagamento.
O pagamento ocorrerá até o 15º (décimo quinto) dia útil após a apresentação da nota fiscal, desde que os produtos tenham sido aprovados e atestados pela Diretoria de Tecnologia da Informação, e será feito por transferência bancária na conta corrente da contratada.
Os valores das notas fiscais estão sujeitos às retenções tributárias e previdenciárias na forma da lei.
O pagamento pelos serviços contratados somente será realizado mediante a efetiva prestação dos serviços, devidamente comprovada e atestada pelo fiscal ou gestor do contrato, após a verificação do cumprimento das obrigações contratuais pela contratada. Não haverá pagamento por serviços não executados, executados parcialmente ou em desacordo com as especificações estabelecidas no Termo de Referência e no contrato, podendo a Administração reter valores ou aplicar multas proporcionalmente ao serviço não prestado ou prestado de forma inadequada.

12. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO GLOBAL do lote. Regime de execução
O regime de execução do contrato será por empreitada por preço global.
De acordo com o art. 6º, inciso XLI, da Lei nº 14.133, de 2021, esta licitação deve ser realizada na modalidade de Pregão, na forma eletrônica, com julgamento pelo critério de menor preço global por lote.
A fundamentação pauta-se na premissa que a contratação de serviços se baseia em padrões de desempenho e qualidade objetivamente definidos no Termo de Referência, por meio de especificações reconhecidas e usuais do mercado, caracterizando-se como “serviços comuns” conforme art. 6º, inciso XIII, da Lei nº 14.133, de 2021.
Da caracterização do objeto como serviço de prestação continuada.

Nos termos da Lei nº 14.133/2021, Art. 6º, incisos XI e XV, os serviços que se intenta contratar são considerados de prestação continuada, por se tratar de serviços contratados pela Administração Pública para a manutenção da atividade administrativa, decorrentes de necessidades permanentes ou prolongadas.

13. DA SUBCONTRATAÇÃO
Não é admitida a subcontratação do objeto contratual.

14. VALOR DA CONTRATAÇÃO
O custo estimado para a contratação é de R$ 410.381,87 (Quatrocentos e Dez Mil, trezentos e oitenta e um reais e oitenta e sete centavos).- ANEXO I – PLANILHA DE VALOR

15. ADEQUAÇÃO ORÇAMENTÁRIA E COMPATIBILIDADE COM PPA E LOA
15.1 Para custear o fornecimento dos produtos objeto do presente termo, as dotações encontram-se elencadas abaixo e no bojo da Requisição de Compras:
Órgão: 06 - [Secretaria Municipal de Administração - SEADM]
Unidade: 005 - [Gerência de Tecnologia da Informação - GTI]
Tipo Ação: Atividade - Ação: 2045 - Funcional: 0004.0126.0002 - [Manter as Atividades da Gerência de Tecnologia da Informação - GTI]
Elemento: 3339040000000000000 - [Serviços de tecnologia da informação e comunicação - pessoa jurídica]
127 00000 Recursos Ordinários (Livres)

16. DA ENTREGA DOS PRODUTOS OU FORMA DE FORNECIMENTO E/OU PRESTAÇÃO DO SERVIÇOS
A entrega dos produtos e a prestação dos serviços deverão ocorrer de acordo com as condições estabelecidas neste Termo de Referência, observando-se as especificações técnicas, prazos, requisitos de qualidade e demais condições necessárias para o pleno atendimento das necessidades da CONTRATANTE.
Os equipamentos, licenças, softwares, componentes e demais itens previstos no objeto deverão ser entregues em perfeitas condições, devidamente acondicionados e acompanhados da documentação técnica pertinente, incluindo-se manuais, certificados de garantia, licenças de uso, registros de série e quaisquer outros documentos necessários à comprovação da originalidade e regularidade dos produtos fornecidos.
Caso sejam identificadas inconsistências, defeitos, incompatibilidades ou qualquer não conformidade com as especificações estabelecidas neste Termo de Referência, a contratada deverá promover, sem ônus adicional para a CONTRATANTE, a correção ou substituição dos itens ou serviços no prazo a ser definido pela Diretoria de TI, garantindo-se o pleno atendimento às condições contratuais.

17. PRAZO DE CONTRATO E REAJUSTE
Os preços são fixos e irreajustáveis no prazo inferior a 12 (doze) meses. Será admitida a sua prorrogação na forma e prazo nos termos da Lei n° 14.133/21, até o limite de 120(cento e vinte) meses, mediante acordo celebrado entre as partes. Após o primeiro ano de contrato, o cálculo de reajuste anual, deverá ser baseado em tabela IPCA/IBGE.
A prorrogação é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com a CONTRATADA, em razão do fato de que o prazo contratual pode ser prorrogado é compreendido que os equipamentos sofrerão depreciação, defasagem tecnológica que poderá ocasionar queda na qualidade dos serviços, riscos à segurança da informação, desta forma, tais equipamentos deverão ser substituídos/atualizados após prévia deliberação estabelecida pela CONTRATANTE em acordo com a CONTRATADA, tendo em vista que o hardware e o software fornecidos não podem constar, em listas de end-of-support, end-of-engineering-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade

de fornecimento, suporte ou vida, para manter o pleno funcionamento das atividades dos locais durante toda a vigência contratual.
No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o Contratante pagará ao Contratado a importância calculada pela última variação conhecida.

18. DAS OBRIGAÇÕES DA CONTRATADA

Durante a vigência do contrato a contratada deverá:

- Manter, durante toda a vigência da ata de registro de preço, regularidade relativa à seguridade social e ao fundo de garantia por tempo de serviço – FGTS;
- Comunicar à unidade requisitante, qualquer anormalidade que impeça o fornecimento dos produtos/ou prestação dos serviços;
- Manter as condições de habilitação desde a licitação até o término da vigência contratual;
- Indicar o responsável que responderá perante a administração por todos os atos e comunicações formais;
- Arcar com o pagamento de todos os tributos e encargos que incidam sobre o produto fornecido ou prestação dos serviços, bem como pelo seu transporte, até o local determinado para a sua entrega.
- Fornecer a seus colaboradores, todas as informações necessárias para coerente entrega dos produtos ou prestação dos serviços;
- Efetuar a prestação de Serviço de acordo com as especificações e demais condições estipuladas no termo de referência. A empresa também será responsável pelas despesas de deslocamento, hospedagem, alimentação e demais gastos eventuais de seus funcionários durante o período da prestação de serviço/treinamentos; e
- A Contratada se obriga a fornecer todos os cabos, conectores e demais componentes necessários à operação e manutenção das soluções contratadas.

19. DAS OBRIGAÇÕES DA CONTRATANTE

Constituem obrigações da contratante:

- Designar fiscal e gestor do contrato;
- Acompanhar e fiscalizar a execução do objeto;
- Disponibilizar informações técnicas e acessos necessários à execução dos serviços;
- Garantir acesso à infraestrutura física e lógica para instalação e funcionamento das soluções;
- Analisar e aprovar documentos e entregas técnicas;
- Efetuar os pagamentos nos prazos estabelecidos;
- Realizar a abertura de chamados técnicos conforme SLA;
- Comunicar formalmente eventuais irregularidades e descumprimento contratual que venha a incidir Multa;
- Indicar equipe técnica para interação com a contratada;
- Participar dos treinamentos previstos; e
- Zelar pela adequada utilização dos equipamentos eventualmente fornecidos em comodato.

20. DOS RESULTADOS PRETENDIDOS

A presente contratação tem por objetivo assegurar a continuidade, disponibilidade e segurança da infraestrutura tecnológica no que diz respeito a toda a Segurança da Informação da Prefeitura Municipal de Campo Mourão – PR, mediante a manutenção, atualização e ampliação das soluções de segurança da informação já implantadas. Busca-se garantir a padronização tecnológica e a interoperabilidade com o ambiente existente, reduzindo riscos de indisponibilidade dos serviços públicos digitais por meio da implementação de alta disponibilidade, rotinas adequadas de backups e plano de recuperação de desastres. Pretende-se, ainda, fortalecer a proteção contra ameaças cibernéticas mediante monitoramento contínuo e mitigação proativa de incidentes, assegurando-se a integridade, confidencialidade e disponibilidade das informações institucionais. A contratação visa também proporcionar suporte técnico especializado, com melhoria no tempo de resposta a incidentes, além de otimizar a aplicação dos recursos públicos, evitando-se custos adicionais decorrentes de substituição de plataforma, retrabalho técnico e descontinuidade técnica operacional.

21. DO CATÁLOGO/PORTFÓLIO

No momento da apresentação da proposta, as empresas licitantes deverão obrigatoriamente apresentar **catálogo técnico, datasheet, ficha técnica oficial do fabricante ou documentação equivalente** que comprove de forma clara e objetiva que o equipamento ou solução ofertada atende integralmente às especificações técnicas exigidas neste Termo de Referência. Essa documentação deverá conter informações suficientes para análise técnica, tais como características do produto, funcionalidades, capacidade, interfaces, padrões suportados, desempenho e demais especificações pertinentes.
A ausência da documentação técnica exigida, bem como a apresentação de material que não permita a verificação clara das especificações solicitadas, poderá ensejar a desclassificação da proposta, por impossibilitar a adequada análise de conformidade técnica do item ofertado.

22. DA POLÍTICA ANTIFRAUDE E DE ANTICORRUPÇÃO

Licitantes e o contratado devem observar e fazer observar, por seus fornecedores e subcontratados, se admitida subcontratação, o mais alto padrão de ética durante todo o processo de licitação, de contratação e de execução do objeto contratual.
Para os propósitos neste item, definem-se as seguintes práticas:

- “prática corrupta”: oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação de servidor público no processo de licitação ou na execução de contrato.
- “prática fraudulenta”: a falsificação ou omissão dos fatos, com o objetivo de influenciar o processo de licitação ou de execução de contrato.
- “prática conluiada”: esquematizar ou estabelecer um acordo entre dois ou mais licitantes, com ou sem o conhecimento de representantes ou prepostos do órgão licitador, visando estabelecer preços em níveis artificiais e não competitivos.
- “prática coercitiva”: causar dano ou ameaçar causar dano, direta ou indiretamente, às pessoas ou sua propriedade, visando influenciar sua participação em um processo licitatório ou afetar a execução do contrato.
- “prática obstrutiva”: (I) destruir, falsificar, alterar ou ocultar provas em inspeções ou fazer declarações falsas aos representantes do organismo financeiro multilateral, com o objetivo de impedir materialmente a apuração de alegações de prática prevista acima. (II) atos cuja intenção seja impedir materialmente o exercício do direito de o organismo financeiro multilateral promover inspeção.

Na hipótese de financiamento, parcial ou integral, por organismo financeiro multilateral, mediante adiantamento ou reembolso, este organismo imporá sanção sobre uma empresa ou pessoa física, inclusive declarando-a inelegível, indefinidamente ou por prazo determinado, para a outorga de contratos financiados pelo organismo se, em qualquer momento, constatar o envolvimento da empresa, diretamente ou por meio de um agente, em práticas corruptas, fraudulentas, colusivas, coercitivas ou obstrutivas ao participar da licitação ou da execução um contrato financiado pelo organismo.
Considerando os propósitos neste item, as LICITANTES deverão concordar e autorizar que, na hipótese de o contrato vir a ser financiado, em parte ou integralmente, por organismo financeiro multilateral, mediante adiantamento ou reembolso, o organismo financeiro e/ou pessoas por ele formalmente indicadas possam inspecionar o local de execução do contrato e todos os documentos, contas e registros relacionados à licitação e à execução do contrato.

23. DA PREVISÃO NO PCA

PCA n° 122/2025 SEADM /GTI CONTRATAÇÃO DE EMPRESA DE SEGURANÇA CORPORATIVA.

24. DO GESTOR CONTRATUAL E FISCAL CONTRATUAL

Com base no Decreto Municipal nº 10.625/2023, cada Unidade da Administração, deve designar Gestores e Fiscais de contrato, sendo para tanto a seguinte designação:
A Gestão ficará a cargo do Servidor Fábio Cesar do Carmo e Silva, Diretor de Tecnologia da Informação e sua suplente a servidora Roselle Thomé Frare Tonete, Gerente de Tecnologia da Informação. No tocante a fiscalização, será atribuída ao servidor Juliano Valério e seu suplente Jonas Angelo Lauber.

Assinado eletronicamente por: ROSELLE THOME FRARE TONETE 081.905.909-95 15/06/2026 14:22:40 Assinatura digital avançada. Roselle Thomé Frare Tonete **Gerente de Tecnologia da Informação**	Assinado eletronicamente por: JONAS ANGELO LAUBER 695.949.459-15 15/06/2026 16:48:11 Assinatura digital avançada. Jonas Angelo Lauber **Chefe da Divisão de Sistemas**
Nome dos responsáveis pela elaboração do Termo de Referência.	
Maria José Pereira da Silva **Secretaria Municipal de Administração**	
Fábio Cesar do Carmo e Silva Gestor de Contrato **Diretor de Tecnologia da Informação**	Juliano Valério **Fiscal de Contrato** **Chefe da Divisão de Infraestrutura**

PREFEITURA DE CAMPO MOURÃO
CAMPO MOURÃO | CIDADE ESCOLA

ANEXO I – PLANILHA RESUMIDA DE FORMAÇÃO DE PREÇOS

PLANILHA DE PRECIFICAÇÃO										
ITEM	QTDE.	ESPECIFICAÇÕES/OBJETOS	PLAT. BANCO DE PREÇOS	CONTRATAÇÕES SEMELHANTES				PRECIFICAÇÃO DIRETA		FORMA DE PRECIFICAÇÃO
				CONTRATO 128/2023- PREGÃO 71/2023 PREFEITURA MUN. DE CAMPO MOURAO - PR (VALOR PROPORCIONAL 12 MESES)	CONTRATO 73/2022 PREGÃO 37/2022 - PREFEITURA MUN. DE CAMPO MOURAO - PR (VALOR PROPORCIONAL 12 MESES)	EDITAL Nº PCE 11/2025 EDITAL Nº PCE 11/2025 CAMARA MUNICIPAL DE CAMPO MOURAO (VALOR PROPORCIONAL 12 MESES)	UASG 389087 - CONSELHO REG. DE ENGENHARIA E AGRONOMIA - SC PREGÃO 90014/2025	RENATO CALONEGO	SECURETE GATE	MÉDIA
1	1	Serviços de fornecimento de software de sistema de backup de dados e informações de arquivos digitais em ambiente virtualizado – BACKUP VIRTUAL LOCAL, incluídos: suporte e atualização de versões para 04 (quatro) servidores físicos de rede com 02 (dois) processadores cada, até 15 (quinze) máquinas virtuais e suporte a Tape Library LTO, 12 (doze) meses.	R$ 12.553,73	R$ 8.133,24		R$ 14.400,00		R$ 18.562,00	R$ 19.320,00	**R$ 15.150,52**

1.a	1	Serviços de implantação e configuração de solução de backup de dados em ambiente virtualizado, pagamento único.		R$ 2.483,63				R$ 1.800,00	R$ 2.000,00	
TOTAL			**R$ 12.553,73**	**R$ 10.616,87**	**-**	**R$ 14.400,00**		**R$ 20.362,00**	**R$ 21.320,00**	
2	1	Serviços de fornecimento de ferramenta de backup de dados e informações on-line operacionalizado em datacenter especializado com no mínimo 5000Gb de espaço para armazenamento de arquivos digitais em nuvem – BACKUP CLOUD, para usuários ilimitados e computadores com softwares inclusos para o período da vigência contratual de 12 (doze) meses.	R$ 4.831,73		R$ 21.676,38	R$ 10.000,00		R$ 5.577,00	R$ 6.100,00	**R$ 10.493,02**
2.a	1	Serviços de implantação e configuração de ferramenta de BACKUP CLOUD, pagamento único.			R$ 480,00			R$ 1.800,00	R$ 2.000,00	
TOTAL			**R$ 4.831,73**	**-**	**R$ 22.156,38**	**R$ 10.000,00**	**-**	**R$ 7.377,00**	**R$ 8.100,00**	

3	1	Serviços de segurança, incluindo-se: 01 (um) equipamento de hardware firewall concentrador appliance UTM (Unified Threat Management) com licenciamento de firewall concentrador, ips, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para appliance de firewall de próxima geração com suporte e atualização de versões durante a vigência contratual, em comodato, 12 (doze) meses. Local: FIREWALL CONCENTRADOR PAÇO MUNICIPAL.			R$ 77.415,63			R$ 59.466,00	R$ 63.500,00	**R$ 75.527,21**
3.a	1	Serviços de implantação de firewall e adaptação de rede e ambiente de segurança com MS-AD de solução de firewall concentrador, pagamento único.			R$ 22.400,00			R$ 1.800,00	R$ 2.000,00	
TOTAL			**-**		**R$ 99.815,63**			**R$ 61.266,00**	**R$ 65.500,00**	
4	1	Serviços de segurança, incluindo-se: 01 (um) equipamento de hardware firewall concentrador appliance UTM (Unified Threat Management) com licenciamento de firewall concentrador redundante de Alta Disponibilidade (HA), ips, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para appliance de firewall de próxima geração com suporte e atualização de versões durante a vigência contratual, em comodato, 12 (doze) meses. Local: FIREWALL CONCENTRADOR REDUNDANTE PAÇO MUNICIPAL em (HA).		R$ 68.777,52				R$ 28.190,00	R$ 31.800,00	**R$ 45.612,54**

4.a	1	Serviços de implantação de firewall concentrador redundante em (HA), pagamento único.		R$ 3.870,10				R$ 1.800,00	R$ 2.400,00	
TOTAL			**-**	**R$ 72.647,62**			**R$ 0,00**	**R$ 29.990,00**	**R$ 34.200,00**	
5	2	Serviços de segurança, incluindo-se: 01 (um) equipamento de hardware firewall de borda appliance UTM licenciamento de firewall, ips, antivírus, anti-spyware, filtro de web, proteção contra ameaças avançadas e firewall de aplicação web para appliance de firewall de próxima geração com suporte e atualização de versões, em comodato, 12 (doze) meses.Local: FIREWALL DE BORDA PARA UNIDADES COM SERVIÇOS ESSENCIAIS.		R$ 9.814,44				R$ 7.823,00	R$ 8.250,00	**R$ 10.368,52**
5.a	2	Serviços de Implantação e configuração de solução de firewall de borda, pagamento único.		R$ 1.418,13				R$ 1.800,00	R$ 2.000,00	
TOTAL				**R$ 11.232,57**	**R$ 0,00**		**R$ 0,00**	**R$ 9.623,00**	**R$ 10.250,00**	
6	1	Ferramenta de software de sistema para suporte remoto tipo “Help Desk” compatível com os sistemas operacionais em uso na CONTRATANTE, compreendendo: 01 (uma) licença para até 06 (seis) analistas e licenças para usuários ilimitados, usável em navegador de internet com comunicação através deste serviço, 2000 (dois mil) hosts por 12 (doze) meses.			R$ 25.802,20			R$ 46.025,00	R$ 54.500,00	**R$ 43.129,07**

6.a	1	Serviços de implantação, configuração e instalação de ferramenta de software de sistema para suporte remoto tipo “Help Desk”, pagamento único.			R$ 960,00			R$ 900,00	R$ 1.200,00	
TOTAL					**R$ 26.762,20**			**R$ 46.925,00**	**R$ 55.700,00**	
7	1	Sistema de software de antivírus corporativo: licenças para estações de trabalho e servidores de rede, compatível com todos os sistemas operacionais legados com console de gerenciamento WEB incluso, 2000 (duas mil) licenças para estações de trabalho e 20 (vinte) licenças para servidores de rede, por 12 (doze) meses.			R$ 55.597,32		596.000,00 *	R$ 160.460,00	R$ 178.000,00	**R$ 135.539,11**
7.a	1	Serviços de implantação, configuração e instalação de antivírus para todas as estações de trabalho e servidores de rede, pagamento único.			R$ 960,00			R$ 5.400,00	R$ 6.200,00	
TOTAL			**R$ 0,00**	**R$ 0,00**	**R$ 56.557,32**	**R$ 0,00**	**596.000,00***	**R$ 165.860,00**	**R$ 184.200,00**	
8	1	Software para coleta e armazenamento de log’s centralizados (Syslog) em ambiente Windows para 01 (um) servidor, 12 (doze) meses. .			R$ 2.397,74	R$ 4.300,00		R$ 6.142,00	R$ 7.950,00	**R$ 6.523,25**
8.a	1	Serviços de implantação e configuração de software de coleta de log’s, pagamento único.			R$ 380,00			R$ 1.200,00	R$ 1.500,00	
TOTAL					**R$ 2.777,74**			**R$ 7.342,00**	**R$ 9.450,00**	

9	1	Software de sistema para detecção e resposta endpoint EDR (ENDPOINT DETECTION AND RESPONSE/DETECÇÃO E RESPOSTA DE ENDPOINT) para implementar solução de segurança cibernética avançada e monitorar continuamente dispositivos finais para detectar comportamentos suspeitos, investigar ameaças em tempo real e responder automaticamente a incidentes como ransonware e malwares em equipamentos estações de trabalho da rede (computadores), 25 (vinte e cinco) equipamentos, 12 (doze) meses.						R$ 6.497,00	R$ 6.900,00	**R$ 7.448,50**
9.a	1	Serviços de implantação, configuração e instalação de software de sistema para detecção e resposta endpoint EDR (ENDPOINT DETECTION AND RESPONSE/DETECÇÃO E RESPOSTA DE ENDPOINT), pagamento único.						R$ 600,00	R$ 900,00	
TOTAL								**R$ 7.097,00**	**R$ 7.800,00**	
10	1	Ferramenta de software de sistema web para abertura de chamados de suporte técnico tipo “Help Desk” para solicitações internas e gerenciador de tarefas em cloud para 20 (vinte) analistas, 12 (doze) meses.			R$ 17.640,00			R$ 29.568,00	R$ 34.500,00	**R$ 28.076,53**
10.a	1	Serviços de implantação, configuração e instalação de ferramenta de software de sistema web para abertura de chamados de suporte técnico tipo “Help Desk”, pagamento único.			R$ 421,60			R$ 600,00	R$ 1.500,00	

TOTAL					**R$ 18.061,60**			**R$ 30.168,00**	**R$ 36.000,00**	
11	1	Serviço de implantação física e lógica de redundância de servidores de rede (AD e File Server), pagamento único sob demanda.		R$ 2.401,75				R$ 3.600,00	R$ 5.000,00	**R$ 3.667,25**
TOTAL				**R$ 2.401,75**				**R$ 3.600,00**	**R$ 5.000,00**	
12	1	Implementação de plano de Disaster Recovery/Recuperação de Desastres, englobando planejamento e diagnostico, Desenho/Projeto da solução de DR, implementação, testes, validação, documentação e treinamento, prazo de até 180 (cento e oitenta) dias, pagamento único pós-implantação.	R$ 30.282,43					R$ 6.000,00	R$ 9.000,00	**R$ 17.794,14**
12a	1	Suporte e sustentação pós-implantação de plano de Disaster Recovery/ Recuperação de Desastres, pagamento único.						R$ 3.600,00	R$ 4.500,00	
TOTAL			**R$ 30.282,43**					**R$ 9.600,00**	**R$ 13.500,00**	

13	1	Prestação de serviços continuados de processamento de dados e segurança da informação no ambiente da contratante, compreendendo atividades especializadas de monitoramento, operação assistida no ambiente de tecnologia da informação e segurança da informação, com visita técnica presencial trimestral de 04 (quatro) horas para verificação do ambiente, análise de conformidade e de vulnerabilidades e apoio técnico operacional com emissão de relatório técnico. O serviço contempla: monitoramento de segurança; criação, suporte e execução de upgrades no ambiente de virtualização, Storages, Servidores físicos, Ativos de rede, Active Directory (Ms-ad), Servidores de arquivos (file server) e Sistemas de armazenamento nas (12 meses).	R$ 10.500,00		R$ 5.161,04	R$ 7.200,00		R$ 14.400,00	R$ 18.000,00	**R$ 11.052,21**
TOTAL			**R$ 10.500,00**		**R$ 5.161,04**	**R$ 7.200,00**		**R$ 14.400,00**	**R$ 18.000,00**	
OBSEERVAÇÃO: ALGUNS VALORES SOFRERAM AJUSTES PARA SE ADEQUAR PROPORCIONALMENTE AO NOVO QUANTITATIVO E/OU AO PERÍODO DE CONTRATAÇÃO - 12MESES.								**TOTAL**		**R$ 410.381,87**
*** VALOR DESCONSIDERADO NO CÁLCULO POR TER MUITA DISCREPANCIA EM COMPARAÇÃO ÀS DEMAIS PRECIFICAÇÕES**										

ANEXO II - CHECKLIST DOS ELEMENTOS OBRIGATÓRIOS DO TERMO DE REFERÊNCIA

Lei Federal nº. 14.133/2021
Art.70 Decreto Municipal nº. 10.672 de 01 de dezembro de 2023 (Regulamento Geral)

Descrição do requisito		Conformidade	Inconformidade	Não se aplica
I.	Definição do objeto, incluídos sua natureza, o prazo do contrato e, se for o caso, a possibilidade de sua prorrogação.			
II.	Fundamentação da contratação, que consiste na referência aos estudos técnicos preliminares correspondentes ou, quando não for possível divulgar esses estudos, no extrato das partes que não contiverem informações sigilosas.			
III.	Descrição da solução como um todo, considerado todo o ciclo de vida do objeto.			
V.	Requisitos da contratação e as especificações técnicas detalhadas do produto, preferencialmente conforme catálogo eletrônico de padronização, observados os requisitos de qualidade, rendimento, compatibilidade, durabilidade e segurança, para o pleno atendimento da necessidade que ensejou a contratação.			
V.	Modelo de execução do objeto, que consiste na definição de como o contrato deverá produzir os resultados pretendidos desde o seu início até o seu encerramento			
VI.	Modelo de gestão do contrato, que descreve como a execução do objeto será acompanhada e fiscalizada pelo órgão ou entidade			
VII.	Critérios de medição e de pagamento			
III.	Forma e critérios de seleção do fornecedor: 1. Justificativa para exigência de habilitação econômico-financeira e/ou técnica, se for o caso, para que: 2. Demonstrem a necessidade da exigência (ex: risco de inadimplemento, complexidade do objeto, alto valor envolvido). 3. Justifiquem a proporcionalidade dos parâmetros adotados. 4. O termo de referência possui capítulo que trata da contratação de microempresa e empresa de pequeno porte, inclusive avaliando o aspecto local e regional, cotas e subcontratação? (inciso XVI, do art. 70, do Regulamento Geral) *Não se aplica: Quando inexistentes itens menores do que R$ 80.000,00.			

**Conformidade: Quando existentes itens menores do que R$ 80.000,00 e capítulo do TR possuir informações da aplicação ou não dos benefícios para itens específicos. ***Inconformidade: Quando existentes itens menores do que R$ 80.000,00, mas 1) não há capítulo específico no TR, ou 2) que a unidade administrativa requisitante não justifica a não aplicação do benefício, em decorrência: • da natureza do produto • a inexistência na região de, pelo menos, 3 (três) fornecedores considerados de pequeno porte, • exigência de qualidade específica, • risco de fornecimento considerado alto ou qualquer outro aspecto impeditivo da participação de microempresas ou empresas de pequeno porte 5. O termo de referência que aponte a necessidade de se realizar licitação com restrição territorial local ou regional, está devidamente acompanhado de: I. amparada em uma política pública municipal com metas e indicadores estabelecidos por meio de plano de ação específico. II. amparada em ampla pesquisa para formação dos preços de referência que obrigatoriamente deverão se aproximar dos preços praticado no mercado. III. amparada na existência comprovada de, no mínimo, 03 (três) microempresas ou empresas de pequeno porte sediadas local ou regionalmente do ramo do objeto da licitação a ser realizada. IV. amparada pela previsão expressa no termo de referência indicando os itens e cotas nos quais serão aplicadas a restrição geográfica. *Conformidade: Quando preenchido todos os requisitos **Inconformidade: Quando não preenchido algum dos requisitos ***Não se aplica: Quando a unidade requisitante não tem interesse em se restringir territorialmente, nos termos do Decreto Municipal nº. 8.680/2020 É bem, serviço ou obra de natureza divisível? (Art. 11, do Decreto 8.680/2020) *Conformidade: Se tiver natureza divisível e haja reserva de cota para microempresa ou empresa de pequeno porte, de até 25% (vinte e cinco por cento) do objeto divisível.			

	*Conformidade: Se tiver natureza divisível, acompanhado de justificativa para não aplicar cota, com fundamento no prejuízo para o conjunto ou complexo do objeto. **Inconformidade: Caso o bem seja divisível e não haja reserva de cota ou justificativa. 6. Possibilidade de subcontratação e alteração subjetiva durante a execução contratual.			
X.	Valor da contratação, acompanhadas, quando couber, dos preços unitários referenciais, das memórias de cálculo e dos documentos que lhe dão suporte, com os parâmetros utilizados para a obtenção dos preços e para os respectivos cálculos, que devem constar de documento separado e classificado.			
X.	Adequação orçamentária com a fonte de recurso correspondente e compatibilidade com a Lei de Diretrizes Orçamentárias e com o Plano Plurianual.			
XI.	Especificações do produto e serviço: • Preferencialmente conforme catálogo eletrônico de padronização (qualidade, rendimento, compatibilidade, durabilidade e segurança) • Avaliação da necessidade de inserir como obrigação do contratado a execução de logística reversa.			
XII.	Da entrega dos produtos ou forma de fornecimento e/ou prestação dos serviços: • Indicação dos locais de entrega dos produtos e das regras para recebimentos provisório e definitivo, quando for o caso			
XIII.	Prazo do contrato e previsão de reajuste			
XV.	Especificação da garantia exigida e das condições de manutenção e assistência técnica, quando for o caso.			
XV.	Das obrigações da contratada			
XVI.	Das obrigações do contratante			
XVII.	Resultados pretendidos desde o início até o encerramento do contrato.			
XIII.	Exigência de catálogo, amostra ou prova de conceito			
XX.	Da política antifraude e anticorrupção			
XX.	Da previsão no PCA			
XXI.	Assinaturas e designação de servidores: • autoridade poítica competente (Prefeito ou Secretários ou Diretor-Presidente). • gestão e fiscalização do contrato com assinatura de ciência			

• Comissão técnica de análise de catálogo e amostra, se for o caso			

Anexo III – TABELA DE LOCAIS E ENDEREÇOS

ÓRGÃOS MUNICIPAIS	LOCALIDADES (SITES)	**ENDEREÇOS DOS (SITES)**
IPPLAN	IPPLAN	RUA DAS ANDORINHAS, 287 VILA TEIXEIRA
PROGE	PROCON	AVN COM. NORBERTO MARCONDES, 1314 CENTRO
SEADE	RESTAURANTE POPULAR DE CAMPO MOURÃO	AVN PREF. PEDRO VIRIATO DE SOUZA FILHO, 335 JD AEROPORTO
SEADE	SECRETARIA DE AGRICULTURA	AVN JOÃO BENTO, 1899 CENTRO
SEADM	BARRACÃO DO PATRIMÔNIO	PER TANCREDO DE ALMEIDA NEVES, 3258 JD SANTA NILCE
SEADM	CENTRO DE RECEBIMENTO E DISTRIBUIÇÃO MUNICIPAL (ALMOXARIFADO CENTRAL)	RUA BRASIL, 1555 CENTRO CEP 87.302-230.
SEADM	GERENCIA DE RECURSOS HUMANOS	RUA BRASIL, 1460 CENTRO
PREFEITURA	PAÇO MUNICIPAL	RUA BRASIL, 1487 CENTRO
PREFEITURA	PRAÇA DE ATENDIMENTO E SECRETARIAS DIVERSAS	RUA BRASIL, 1407 CENTRO
SEASO	CASA DE PASSAGEM INDÍGENA	RUA PITANGA, 1578 CENTRO
SEASO	CENTRO DA JUVENTUDE	RUA ROBSON DACIUK PAITACH, 179 JD AEROPORTO
SEASO	CENTRO DE INTEGRAÇÃO COLIBRI	RUA DOS CISNES, S/N CJ DR MILTON LUIZ PEREIRA
SEASO	CENTRO DE INTEGRAÇÃO ESPERANÇA	RUA PORFIRIO QUIRINO PEREIRA, 24 JD MODELO
SEASO	CENTRO DE INTEGRAÇÃO FORTUNATO PIACENTINI	RUA DEP. Q. MORAES, 1211 CJ. FORTUNATO PERDONCINI
SEASO	CENTRO DE INTEGRAÇÃO PRIMAVERA / CRAS CENTRAL	RUA DAS GARDÊNIAS, 224 CJ. PRIMAVERA
SEASO	CENTRO DE INTEGRAÇÃO TROPICAL	RUA DAS FLORES, S/N JD TROPICAL II
SEASO	CENTRO DIA - IDOSO	RUA PEABIRU, 558 CENTRO
SEASO	CONSELHO TUTELAR	RUA ANGELO AMARAL, S/N JD JOANA D'ARC
SEASO	CRAM - CENTRO DE REFERENCIA DE ATENDIMENTO A MULHER	AVN JOÃO BENTO, 2245 CENTRO
SEASO	CRAS – CENTRO DE REF EM ASSISTÊNCIA SOCIAL – REGIÃO OESTE	RUA DR NELSON BITENCOURT PRADO, 1180 JD PIO XII CEP 87.306-040
SEASO	CRAS – CENTRO DE REF. EM ASSISTÊNCIA SOCIAL – REGIÃO LESTE	RUA ALBERTO SPILKA, 84 VILA CORINTHIANS
SEASO	CREAS - CENTRO DE REF. EM ASSISTÊNCIA SOCIAL	RUA PREF. DEVETE DE PAULA XAVIER, 1309 CENTRO

SEASO	CREAS POP	RUA BRASIL, 1939 CENTRO CEP 87.302-230.
SEASO	SEASO – SEC DA AÇÃO SOCIAL	RUA SANTA CATARINA, 1682 CENTRO
SECED	CMEI AMOR PERFEITO	AVN MANOEL NOGUEIRA, 1622 JD LAR PARANÁ
SECED	CMEI DOCE MAGIA	RUA BRILHANTE, 115 CJ. DIAMANTE AZUL
SECED	CMEI DOM VIRGILIO DE PAULI	RUA PEDRO DA VEIGA, 1128 CJ. FORTUNATO PERDONCINI
SECED	CMEI DR. MILTON LUIZ PEREIRA	RUA PICA-PAU, 135 CJ. DR MILTON LUIS PEREIRA
SECED	CMEI ILHA BELA	RUA ILHA DO MEL, 136 CJ. ILHA BELA
SECED	CMEI MENINO JESUS	RUA JOSÉ F. DA SILVA, 301 VILA RIO GRANDE
SECED	CMEI MUNDO DA CRIANÇA	AVN ARMELINDO TROMBINI, 4669 JD ALBUQUERQUE
SECED	CMEI MUNDO ENCANTADO	RUA CARLOS HAKNER, 458 JD FLORA
SECED	CMEI NOSSA SENHORA APARECIDA	RUA ROCHA POMBO, 2595 VILA URUPÊS
SECED	CMEI NOSSA SENHORA DE FÁTIMA	RUA DR HUGO LISOT, 2630 JD PAULINO
SECED	CMEI PEQUENOS BRILHANTES	RUA PE. JOÃO VIECCELLI, 147 JARDIM MAIA
SECED	CMEI PINGO DE GENTE	RUA FAISÃO, 402 JD TROPICAL II
SECED	CMEI PIONEIRO AFONSO STANIZEWSKI	RUA SEVERO GOMES, S/Nº JD BATEL
SECED	CMEI PRIMEIROS PASSOS	RUA VALDOMIRO FERRARI, 922 CJ. AVELINO PIACENTINI
SECED	CMEI SAGRADA FAMÍLIA	RUA BRASIL, 567 JD LAURA
SECED	CMEI SANTA CRUZ	RUA PREF. DR HORÁCIO AMARAL, 292 JD SANTA CRUZ
SECED	CMEI SANTO ANTONIO	RUA PREF. JOSÉ ANTÔNIO DOS SANTOS, 1535 JD CIDADE NOVA
SECED	CMEI SÃO JOSÉ	RUA MANOEL SILVÉRIO PEREIRA, 136 JD ALVORADA
SECED	CMEI SOSSEGO DA MAMÃE	RUA LAURINDO BORGES, 2310 VILA URUPÊS
SECED	CMEI TANCREDO DE ALMEIDA NEVES	RUA DOS CISNES, 143 CJ. DR MILTON LUIZ PEREIRA
SECED	CMEI VERA LÚCIA COLLODEL	RUA LEMOS DO PRADO, 1046 JD INDIANÓPOLIS
SECED	ESCOLA BENTO MOSSURUNGA	RUA TEODORO METCHKO, 1129 JD COPACABANA
SECED	ESCOLA CIDADE NOVA	RUA PREF. JOSÉ ANTÔNIO DOS SANTOS, 1493 JD CIDADE NOVA
SECED	ESCOLA CLARINHA WENCEL CASIMIRO	RUA DA FLORES, 831 CJ. AVELINO PIACENTINI
SECED	ESCOLA CONSTANTINO L. DE MEDEIROS	RUA LEMOS DO PRADO, 215 JD LAR PARANÁ
SECED	ESCOLA DOMINGOS JOSÉ DE SOUZA	RUA FAISÃO, 496 JD TROPICAL I
SECED	ESCOLA ESPAÇO ABERTO	RUA SÃO JOSÉ, 2068 CENTRO
SECED	ESCOLA ETHANIL BENTO DE ASSIS	RUA VICENTE DOMANSKI, 1196 JD SANTA CRUZ
SECED	ESCOLA GURILANDIA	RUA EDMUNDO MERCER, 1323 CENTRO
SECED	ESCOLA MANOEL BANDEIRA	RUA MÁRIO SILVÉRIO PEREIRA, 151 JD ALVORADA
SECED	ESCOLA MARIA DO CARMO PEREIRA	RUA NELSON G. MONTEIRO, 499 JD PAULISTA

SECED	ESCOLA MÁRIO DE MIRANDA QUINTANA	RUA INT. MANOEL RIBAS, 2381 JD IONE
SECED	ESCOLA MONTEIRO LOBATO	RUA MÁRIO CASTALDELLI, 419 JD LAR PARANÁ
SECED	ESCOLA MUNICIPAL CAETANO MUNHOZ DA ROCHA	VILA ROBERTO BRZEZINSKI COMUNIDADE ALTO ALEGRE CEP 87.300-970
SECED	ESCOLA MUNICIPAL CASTRO ALVES	RUA Nº06, 596 VILA GUARUJÁ CEP 87.301-643
SECED	ESCOLA NARCISO SIMÃO	RUA JOSÉ PAULINO DE CARVALHO, 65 DISTRITO DE PIQUIRIVAÍ
SECED	ESCOLA NICON KOPKO	RUA CÉLIA SIMÃO BROZA, 2147 JD MODELO
SECED	ESCOLA PARIGOT DE SOUZA	RUA MATO GROSSO, 749 JD GUTIERREZ
SECED	ESCOLA PAULO VI	RUA DAS LONTRAS, 226 JD PIO XII
SECED	ESCOLA PROFESSOR ERONI MACIEL RIBAS	RUA CURIANGO, 339 JD LAR PARANÁ
SECED	ESCOLA PROFESSOR FLORESTAN FERNANDES	AVN ARMELINDO TROMBINI, 4669 JD ALBUQUERQUE
SECED	ESCOLA VILA URUPÊS	RUA LAURINDO BORGES, 2163 VILA URUPÊS
SECED	IMAPE	RUA DAS SAMAMBAIAS, 115 JD ARAUCÁRIA
SECED	SEDE SECRETARIA DA EDUCAÇÃO	AVN COM. NORBERTO MARCONDES, 1643 CENTRO
SECULT	BIBLIOTECA CIDADÃ	RUA ENGENHEIRO MERCER, 978 JD CONRADO
SECULT	BIBLIOTECA EGÝDIO MARTELLO	RUA FRANCISCO FERREIRA ALBUQUERQUE, 1158-1320 CENTRO
SECULT	CASA DA CULTURA E ESPAÇO MULTICULTURAL GURILANDIA/ ESCOLA MUN. DE ARTES CIRCENSES	AVN COM. NORBERTO MARCONDES, 684 CENTRO
SECULT	CASA DA MÚSICA	RUA DAS SERINGUEIRAS, 1055 JD ARAUCARIA
SECULT	MUSEU MUNICIPAL	AVN CAPITÃO ÍNDIO BANDEIRA, 1117 CENTRO
SECULT	TEATRO MUNICIPAL	AVN COM. NORBERTO MARCONDES, 684 CENTRO
SEIDEC	SEDE SECRETARIA DE DESENVOLVIMENTO ECONÔMICO	RUA SÃO PAULO, 1787 CENTRO
SEIMOB	AEROPORTO MUNICIPAL	AVN JOSÉ TADEU NUNES, 1370 JD NOSSA SENHORA APARECIDA
SEIMOB	DIRETRAN	PER TANCREDO DE ALMEIDA NEVES, 161 JD COPACABANA
SEIMOB	SEDE SECRETARIA DE OBRAS E SERVIÇOS PÚBLICOS	AVN JOSÉ TADEU NUNES, 150 JD NOSSA SENHORA APARECIDA
SEMA	ADMINISTRAÇÃO DO CEMITÉRIO MUNICIPAL	AVN NEY BRAGA, 1419 JD IZABEL
SEMA	SEDE SECRETARIA E MEIO AMBIENTE	RUA ARQ. HAMILTON TAVELA BORGES, 159 JD ALBUQUERQUE
SESAU	UBS PIQUIRIVAÍ (CARLOS ANTÔNIO)	RUA VIS. DO RIO BRANCO, 1161 DISTRITO DE PIQUIRIVAÍ
SESAU	ACADEMIA DA SAÚDE URUPÊS	RUA SÃO JOSÉ, 2152 CENTRO
SESAU	ACADEMIA DE SAÚDE COHAPAR	RUA GUARANI, 2537 CJ. DR MILTON LUIZ PEREIRA
SESAU	AMBULATÓRIO DE SAÚDE MENTAL	RUA COM. NORBERTO MARCONDES, 1673 CENTRO

SESAU	AMPARA	RUA FRANCISCO FERREIRA ALBUQUERQUE, 1779 CENTRO
SESAU	CAPS – CENTRO DE ATENÇÃO PSICOSSOCIAL II	RUA MATO GROSSO, 2622 CENTRO
SESAU	CAPS - IJ	RUA HARRISON JOSÉ BORGES, 692 CENTRO
SESAU	CENTRAL DE REGULAÇÃO	RUA FRANCISCO FERREIRA ALBUQUERQUE, 1999 CENTRO
SESAU	CENTRO DE ESPECIALIDADES	AVN MANOEL MENDES DE CAMARGO, 550 CENTRO
SESAU	PRONTO ATENDIMENTO LAR PARANÁ	RUA JOÃO VECCHI, 600 JD LAR PARANÁ
SESAU	COMPLEXO UBS CENTRO SOCIAL URBANO/ CAPS AD/ CEOCAM	RUA JUREMA POMPEU MIGUEL, 297 JD LURDES
SESAU	DIVISÃO DE SUPRIMENTOS / CENTRAL DE ASSISTÊNCIA FARMACÊUTICA	RUA NIVEA MATSUGUMA, S/Nº JD BELLA VISTA CEP 87307-425
SESAU	DIVISÃO DO SERVIÇO DE ATENDIMENTO ESPECIALIZADO – SAE- (AMBULATÓRIO DE INFECTOLOGIA E DST)	AVN GUILHERME DE PAULA XAVIER, 1844 CENTRO
SESAU	MODULO ODONTOLÓGICO VILA URUPÊS	AVN GUILHERME DE PAULA XAVIER, 2596 (FUNDOS) CENTRO
SESAU	POSTO DE ATENDIMENTO E MÓDULO ODONTOLÓGICO ALTO ALEGRE	ROD BR-272 SAÍDA P/ GOIOERÊ ALTO ALEGRE ZONA RURAL CEP 87.306-010
SESAU	POSTO DE ATENDIMENTO KM 128	ROD BR-487 SAÍDA P/ CRUZEIRO DO OESTE KM 128 ZONA RURAL CEP 87.305-380
SESAU	POSTO DE ATENDIMENTO SÃO BENEDITO	ROD BR-272 SAÍDA P/ FAROL SÃO BENEDITO ZONA RURAL CEP 87306-010
SESAU	SEDE SEC. DE SAÚDE	RUA FRANCISCO FERREIRA ALBUQUERQUE, 1999 CENTRO
SESAU	UBS ALVORADA	RUA MANOEL SILVÉRIO PEREIRA, 150 JD ALVORADA
SESAU	UBS AVELINO PIACENTINI (AUXILIA TRICE MARCHESE PIACENTINI)	RUA DAS FLORES, 945 CJ. AVELINO PIACENTINI
SESAU	UBS CIDADE NOVA	RUA PREF. JOSÉ ANTÔNIO DOS SANTOS, 1551 JD CIDADE NOVA
SESAU	UBS COHAPAR (UBS DR GERMANO TRAPLE)	RUA PICA-PAU, 181 CJ. DR MILTON LUIS PEREIRA
SESAU	UBS COPACABANA II (UBS DILMAR DALEFFE)	RUA FRANZ KAIZER, 641 JD COPACABANA II
SESAU	UBS DAMFERI (UBS DR SADAYOSHI SHIMIZU)	RUA LEMOS DO PRADO, 195 JD FERNANDO
SESAU	UBS EUROPA	RUA PROF. MARCOS ERHART, 474 JD EUROPA
SESAU	UBS FORTUNATO PERDONCINI (DR. MARTINHO FERNANDES DE MORAES)	RUA ARMANDO QUEIROZ DE MORAES, 1285 CJ FORTUNATO PERDONCINI
SESAU	UBS LAR PARANÁ (UBS DR DELBOS ZOLA LEODORO DA SILVA)	RUA NOSSA SENHORA APARECIDA, 267 VILA CÂNDIDA
SESAU	UBS MODELO (UBS BENEDITO PEREIRA DUARTE)	RUA ANA TEODORO DE LIMA, 681 JD MODELO

SESAU	UBS NEY BRAGA	AVN NEY BRAGA, 1362 JD SAN MARINO
SESAU	UBS PAULISTA (DR DIOGO FERRAZ SALVADOR)	AVN PREF. PEDRO VIRIATO DE SOUZA FILHO, 435 JD PAULISTA
SESAU	UBS PIO XII (MANOEL DE JESUS PEREIRA)	RUA DR NELSON BITTENCOURT DO PRADO, 1280 JD PIO XII
SESAU	UBS TROPICAL I (UBS DARCY DEITOS)	RUA ROUXINOL, 169 JD TROPICAL I
SESAU	UBS VILA URUPÊS	RUA SÃO JOSÉ, 2152 JD HORIZONTE
SESAU	UNIDADE BÁSICA DE SAÚDE DOMINGOS ZANRE (BARREIRO DAS FRUTAS)	ROD BR-272 SAÍDA P/ BARBOSA FERRAZ BARREIRO DAS FRUTAS ZONA RURAL CEP 87.300-490
SESAU	UNIDADE BÁSICA DE SAÚDE PEDRO DE FREITAS - RIO DA VÁRZEA	ROD BR-272 SAÍDA P/ BARBOSA FERRAZ (ESTRADA PARA O BARREIRO DAS FRUTAS KM-22) RIO DA VÁRZEA ZONA RURAL CEP 87.300-490
SESAU	UNIDADE DE SAÚDE VILA GUARUJÁ	RUA MARIO EPIFÂNIO, 391 VILA GUARUJÁ CEP 87.301-635
SESAU	UPA – UNIDADE DE PRONTO ATENDIMENTO 24 HORAS MARIA ZULEICA THEODORO	AVN PREF. PEDRO VIRIATO DE SOUZA FILHO, 172 JD PAULISTA
SESP	CENTRO ESPORTIVO E LAZER ANTÔNIO CARLOS SCARPIN	RUA BRASIL, S/N JD LAURA CENTRO
SESP	COMPLEXO ESPORTIVO ROBERTO BRZEZINSKI	AVN COM. NORBERTO MARCONDES, 286 CENTRO
SESP	ESTÁDIO MUNICIPAL JOSÉ CARLOS GALBIER (ESTÁDIO DOS AMADORES)	AVN JOSÉ TADEU NUNES, S/N JD ISABEL
SESP	GINÁSIO DE ESPORTES HAROLDO GONÇALVES NETO	RUA SANTA CRUZ, S/N VILA URUPÊS
SESP	GINÁSIO DE ESPORTES HORLEY CASALI	RUA ADÉLINO CONSTANTINO MIGUEL, 374-422 JD AEROPORTO
SESP	GINÁSIO DE ESPORTES JOÃO MARIA FERREIRA	AVN PREF. DR. HORÁCIO AMARAL, 509-597 JD SANTA CRUZ.
SESP	GINÁSIO DE ESPORTES JUSCELINO KUBITSCHEK	RUA ANGELO AMARAL, 02 JD JOANA D'ARC
SESP	PISCINA MUNICIPAL DO COMPLEXO ESPORTIVO ROBERTO BRZEZINSKI	RUA PITANGA, 1146 CENTRO
SESP	SECRETARIA DE ESPORTES	AVN PREF. PEDRO VIRIATO DE SOUZA FILHO, 303 PRAÇA DA JUVENTUDE

ANEXO IV

DECLARAÇÃO DE VISITA TÉCNICA

Objeto: Contratação de empresa de Tecnologia da Informação especializada na área de segurança corporativa digital e implantação de ambientes de salas de centrais de dados, para fornecimento de bens e serviços das seguintes soluções tecnológicas:

- Software de sistema de backup de dados e informações de arquivos digitais em ambiente virtualizado (Backup Virtual Local);

- Serviço para fornecimento de sistema de backup de dados e informações de arquivos digitais em nuvem (Backup Cloud);

- Equipamento e serviços para implantação de segurança virtual na rede de computadores para soluções de serviços de segurança para controle de ameaças virtuais na modalidade “Appliance do tipo UTM (Unified Threat Management) Firewall concentrador” em comodato – Firewall Concentrador Paço Municipal;

- Equipamento e serviços para implantação de segurança virtual na rede de computadores para controle de ameaças virtuais na modalidade “Appliance do tipo UTM (Unified Threat Management) Firewall concentrador redundante de alta disponibilidade (HA)” em comodato – Firewall Concentrador Redundante Paço Municipal em (HA);

- Firewall de borda para unidades com serviços essenciais em saúde pública municipal (UPA e PALP);

- Ferramenta de software de sistema para suporte remoto tipo “Help Desk”;

- Software de sistema antivírus corporativo para controle de ameaças digitais nos equipamentos da rede de computadores e segurança;

- Licença de uso de software para coleta e armazenamento de Logs (Syslog);

- Software de sistema para detecção e resposta endpoint EDR (ENDPOINT DETECTION AND RESPONSE/DETECÇÃO E RESPOSTA DE ENDPOINT) para implementar solução de segurança cibernética avançada e monitorar continuamente dispositivos finais para detectar comportamentos suspeitos, investigar ameaças em tempo real e responder automaticamente a incidentes como ransonware e malwares em equipamentos estações de trabalho da rede (computadores);

- Ferramenta de software de sistema web para abertura de chamados de suporte técnico tipo “Help Desk”;

- Serviço de implantação física e lógica de redundância de servidores de rede (AD e File Server).

- Implementação e implantação de plano de Disaster Recovery/Recuperação de Desastres; e

- Prestação de serviços continuados de processamento de dados e segurança da informação

Para todas as soluções, deverão ser incluídos treinamentos em níveis avançados especializados aos técnicos de tecnologia da informação da contratante para fins de atualização e reciclagem do conhecimento de forma presencial. Durante a vigência contratual deverá ser realizado upgrade nas soluções e prestação de serviços de suporte técnico especializado continuado no regime (24x7x6) conforme especificações técnicas e níveis de serviços mínimos exigidos constantes no Termo de Referência, no Edital de Licitações e seus Anexos, tendo como referência o disposto na lei federal n.º

14.133/2021 (nova lei de licitações) e os Regulamentos da Prefeitura Municipal de Campo Mourão – PR.

Eu, _____, portador(a) da Cédula de Identidade RG nº _____ e CPF nº _____, representante legal da empresa _____, inscrita no CNPJ sob nº _____, DECLARO, para os devidos fins, que realizei visita técnica nas dependências da Prefeitura Municipal de Campo Mourão – PR, tomando conhecimento de todas as condições locais, características técnicas, infraestrutura existente, peculiaridades operacionais, requisitos de execução dos serviços e demais informações necessárias à perfeita elaboração da proposta e execução contratual.

Declaro, ainda, que foram prestados todos os esclarecimentos considerados necessários e que a empresa possui pleno conhecimento das condições e dificuldades inerentes à execução do objeto licitado, não podendo alegar posteriormente desconhecimento de fatos, condições ou circunstâncias relacionadas à prestação dos serviços como fundamento para pleitos de alterações contratuais, reequilíbrios financeiros ou descumprimento das obrigações assumidas.

Por ser expressão da verdade, firmo a presente declaração para que produza os efeitos legais.

Campo Mourão – PR, ____ de _____ de 2026.

Representante Legal da Empresa

Nome:
CPF:
Cargo:

_____
Assinatura

VISTO DA PREFEITURA MUNICIPAL DE CAMPO MOURÃO

Certificamos que o representante acima identificado realizou visita técnica referente ao objeto da licitação, nas dependências indicadas pela Administração Municipal, na data ____ de _____ de 2026.

Servidor Responsável:
Nome:
Cargo:

_____
Assinatura

ANEXO V

MODELO DE DECLARAÇÃO DE DISPENSA DE VISITA TÉCNICA

Objeto: Contratação de empresa de Tecnologia da Informação especializada na área de segurança corporativa digital e implantação de ambientes de salas de centrais de dados, para fornecimento de bens e serviços das seguintes soluções tecnológicas:

- Software de sistema de backup de dados e informações de arquivos digitais em ambiente virtualizado (Backup Virtual Local);

- Serviço para fornecimento de sistema de backup de dados e informações de arquivos digitais em nuvem (Backup Cloud);

- Equipamento e serviços para implantação de segurança virtual na rede de computadores para soluções de serviços de segurança para controle de ameaças virtuais na modalidade “Appliance do tipo UTM (Unified Threat Management) Firewall concentrador” em comodato – Firewall Concentrador Paço Municipal;

- Equipamento e serviços para implantação de segurança virtual na rede de computadores para controle de ameaças virtuais na modalidade “Appliance do tipo UTM (Unified Threat Management) Firewall concentrador redundante de alta disponibilidade (HA)” em comodato – Firewall Concentrador Redundante Paço Municipal em (HA);

- Firewall de borda para unidades com serviços essenciais em saúde pública municipal (UPA e PALP);

- Ferramenta de software de sistema para suporte remoto tipo “Help Desk”;

- Software de sistema antivírus corporativo para controle de ameaças digitais nos equipamentos da rede de computadores e segurança;

- Licença de uso de software para coleta e armazenamento de Logs (Syslog);

- Software de sistema para detecção e resposta endpoint EDR (ENDPOINT DETECTION AND RESPONSE/DETECÇÃO E RESPOSTA DE ENDPOINT) para implementar solução de segurança cibernética avançada e monitorar continuamente dispositivos finais para detectar comportamentos

suspeitos, investigar ameaças em tempo real e responder automaticamente a incidentes como ransonware e malwares em equipamentos estações de trabalho da rede (computadores);

- Ferramenta de software de sistema web para abertura de chamados de suporte técnico tipo “Help Desk”;

- Serviço de implantação física e lógica de redundância de servidores de rede (AD e File Server).

- Implementação e implantação de plano de Disaster Recovery/Recuperação de Desastres; e

- Prestação de serviços continuados de processamento de dados e segurança da informação

Para todas as soluções, deverão ser incluídos treinamentos em níveis avançados especializados aos técnicos de tecnologia da informação da contratante para fins de atualização e reciclagem do conhecimento de forma presencial. Durante a vigência contratual deverá ser realizado upgrade nas soluções e prestação de serviços de suporte técnico especializado continuado no regime (24x7x6) conforme especificações técnicas e níveis de serviços mínimos exigidos constantes no Termo de

Referência, no Edital de Licitações e seus Anexos, tendo como referência o disposto na lei federal n.º 14.133/2021 (nova lei de licitações) e os Regulamentos da Prefeitura Municipal de Campo Mourão – PR.

Eu, _____ (representante do licitante), portador da Cédula de Identidade RG nº _____ e do CPF nº _____, na condição de representante legal devidamente constituído de _____ (identificação do licitante), inscrita no CNPJ sob o nº _____, para fins do disposto no Edital da presente Licitação, declaro, sob as penas da lei, em especial o art. 299 do Código Penal Brasileiro, que possuímos pleno conhecimento de todas as condições, peculiaridades inerentes à natureza dos trabalhos e do grau de dificuldade existentes pelo que não alegaremos desconhecimento como justificativa para se eximir das obrigações assumidas para com o Município, assumindo total responsabilidade por esse fato e informando que não o utilizaremos para quaisquer questionamentos futuros que ensejem avenças técnicas ou financeiras com a contratante.

Campo Mourão – PR, ... de ..... de 2026

_____

Carimbo e Assinatura do Representante Legal da Empresa