MUNICÍPIO DE REBOUÇAS

SECRETARIA DE ADMINISTRAÇÃO

ESTUDO TÉCNICO PRELIMINAR N° 80/2026

REBOUÇAS – PR

2026

INTRODUÇÃO

O presente documento caracteriza a primeira etapa da fase de planejamento conforme Decreto nº 285/2023 com base na nova Lei de Licitação nº 14.133/2021, de forma a apresentar os devidos estudos para a contratação de solução que atenderá à necessidade abaixo especificada.

A presente análise tem por objetivo demonstrar a viabilidade técnica e econômica para a contratação de empresa especializada na prestação de serviços de Tecnologia da Informação, contemplando o fornecimento, na modalidade de locação, de solução de firewall corporativo, serviços de migração da infraestrutura tecnológica local e remota, implementação e gerenciamento de solução de backup local e em nuvem, fornecimento de licenças de antivírus para estações de trabalho e servidores, bem como a prestação de serviços continuados de suporte técnico especializado, manutenção preventiva e corretiva e monitoramento contínuo (24x7) da infraestrutura de TI da Administração Municipal.

O objetivo principal é estudar detalhadamente a necessidade e identificar no mercado a melhor solução para supri-la, em observância às normas vigentes e aos princípios que regem à Administração Pública, avaliando todos os aspectos necessários e suficientes à contratação.

I. DESCRIÇÃO DA NECESSIDADE

A Administração Municipal necessita garantir a continuidade, segurança e eficiência dos serviços públicos, os quais dependem diretamente da adequada infraestrutura de Tecnologia da Informação. Atualmente, grande parte das atividades administrativas, operacionais e de atendimento à população é realizada por meio de sistemas informatizados, redes de dados e plataformas digitais, tornando a TI um elemento essencial para o funcionamento do Município.

Verifica-se, contudo, que a infraestrutura tecnológica existente apresenta fragilidades relevantes, especialmente no que se refere à segurança da informação. No mês de novembro de 2025, o ambiente computacional da Administração foi alvo de ataque cibernético, ocasionando prejuízos à estrutura tecnológica e atrasos na tramitação de processos internos, evidenciando a vulnerabilidade do sistema atualmente utilizado.

Além disso, o ambiente atual opera com soluções limitadas, sem monitoramento contínuo, sem rotinas adequadas de backup em nuvem e sem mecanismos eficazes de prevenção, detecção e resposta a ameaças cibernéticas. Soma-se a isso a inexistência de suporte técnico especializado contínuo e de ferramentas modernas de gestão, o que compromete a disponibilidade dos sistemas e eleva o risco de novas ocorrências.

Diante desse cenário, torna-se necessária a contratação de empresa especializada para fornecimento de solução integrada de tecnologia da informação, contemplando segurança de rede, backup, antivírus, suporte técnico e monitoramento contínuo, visando garantir a integridade, confidencialidade e disponibilidade das informações, bem como a continuidade e eficiência dos serviços públicos prestados à população.

1.1 DIAGNÓSTICO DA SITUAÇÃO ATUAL DA INFRAESTRUTURA DE TI

A infraestrutura de Tecnologia da Informação da Administração Municipal apresenta limitações estruturais e operacionais que comprometem a segurança, a disponibilidade e a eficiência dos serviços prestados.

Atualmente, a proteção de rede é realizada por meio de solução baseada em pfSense, instalada em equipamento não dedicado e sem aderência plena às boas práticas de segurança da informação, o que reduz significativamente sua efetividade na prevenção, detecção e resposta a ameaças cibernéticas.

No mês de novembro de 2025, o ambiente computacional do Município foi alvo de ataque cibernético, ocasionando prejuízos à estrutura tecnológica e impactando diretamente a continuidade dos serviços, com registro de atrasos na tramitação de processos internos, evidenciando a vulnerabilidade da infraestrutura existente.

Verifica-se, ainda, a ausência ou insuficiência de mecanismos essenciais para a adequada gestão e proteção do ambiente de TI, destacando-se:

- Inexistência de solução estruturada de backup em nuvem, sendo adotado predominantemente backup local, o que eleva o risco de perda de dados;
- Ausência de monitoramento contínuo e centralizado da rede e dos ativos de TI;

- Inexistência de ferramentas avançadas de segurança, como sistemas de detecção e prevenção de intrusões;
- Deficiência na gestão de atualizações e correções de segurança (patch management);
- Ausência de solução corporativa de antivírus gerenciada de forma centralizada;
- Inexistência de políticas estruturadas de controle de acesso e segurança da informação.

Além disso, a inexistência de suporte técnico especializado contínuo e de rotinas formais de gerenciamento da infraestrutura contribui para a ocorrência de falhas operacionais, aumento do tempo de resposta a incidentes e risco de indisponibilidade dos serviços.

Diante desse cenário, conclui-se que a infraestrutura atual não atende de forma satisfatória às necessidades da Administração Municipal, sendo necessária a adoção de solução tecnológica integrada, moderna e segura, capaz de mitigar riscos, garantir a continuidade dos serviços e assegurar a proteção das informações institucionais.

1.2 PARQUE TECNOLÓGICO ATUAL

Paço Municipal	Outras Secretarias
40 computadores	45 computadores
10 reservas	10 reservas

1.3 INFRAESTRUTURA DE COMPUTADORES E UNIDADES ATENDIDAS

A infraestrutura tecnológica da Administração Municipal atende diversos prédios públicos, incluindo:

Paço municipal	Unidades esternas
50 computadores	50 computadores

Esses equipamentos estão distribuídos entre diversos setores da Administração, incluindo áreas como:

- Saúde
- Educação
- Assistência Social
- Administração
- Serviços operacionais

Diante do exposto e das informações apresentadas, justifica-se a necessidade de contratação de empresa especializada para a prestação dos serviços de Tecnologia da Informação, considerando a importância da manutenção de uma infraestrutura tecnológica estável, segura e eficiente para o funcionamento das atividades administrativas do Município.

Assim, a presente contratação visa assegurar a continuidade dos serviços públicos, a segurança das informações institucionais e o adequado funcionamento dos sistemas utilizados pelas diversas unidades administrativas do Município.

II. DOS REQUISITOS DA CONTRATAÇÃO

Para que o objeto seja contratado, é necessário o atendimento de alguns requisitos de acordo com as características do objeto, dentre eles os de qualidade e capacidade de execução pelo contratado, minimamente, os dispostos nos arts. 66, 67, 68 e 69, da Lei nº 14.133/2021. Sendo assim, quanto a documentação relativa à qualificação técnico-profissional e técnico-operacional e econômico-financeira serão os listados abaixo:

2.1. Habilitação técnico-profissional e técnico operacional:

2.2.1. Atestado de capacidade técnica expedido por pessoa jurídica de direito público ou privado, em nome da licitante, que comprove aptidão para o desempenho de atividade pertinente e compatível com o objeto deste estudo.

2.2.2. A comprovação deverá ser feita por meio de atestado, no ato da proposta, acompanhado de no mínimo 03 (três) Notas Fiscais consecutivas, para comprovar a execução do serviço mensal.

6.2. Habilitação econômico-financeira:

6.2.1 Certidão negativa de falência expedida pelo cartório distribuidor da sede da pessoa jurídica.

6.2.2. Apresentar Balanço Patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais; que comprovem a boa situação financeira da empresa, consubstanciada nos seguintes índices:

- Índice de Liquidez Geral (IGL) igual ou superior a 1,0 (um).
- Índice de Liquidez Corrente (ILC) igual ou superior a (um).
- Solvência Geral (SG) igual ou superior a 1,0 (um).

Os documentos referidos acima, limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.

Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), comprovados mediante a apresentação pelo licitante de balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais e obtidos pela aplicação das seguintes fórmulas:

$$LG = \frac{Ativo\ Circulante + Realizável\ a\ Longo\ Prazo}{Passivo\ Circulante + Passivo\ Não\ Circulante}$$

$$SG = \frac{Ativo\ Total}{Passivo\ Circulante + Passivo\ Não\ Circulante}$$

$$LC = \frac{Ativo\ Circulante}{Passivo\ Circulante}$$

- Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação patrimônio líquido mínimo de **10%** (dez por cento) do valor total estimado da contratação.
- As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).
- O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos. (Lei nº 14.133, de 2021, art. 69, §6º)

- **O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor. (Art. 69, § 1º da Lei 14.133/2021).**

2.2.3. JUSTIFICATIVA ÍNDICES CONTÁBEIS

Os índices financeiros indicados neste edital são Usuais de mercado e não caracterizam estrição a participação, de acordo com jurisprudência do Tribunal de Contas do Estado de Minas Gerais Representação n. 775.293. Rel. Conselheira Adriene Andrade Sessão do dia 17/0B/2009 Recurso Ordinário 808 260. Rel Conselheira Adriene Andrade. Sessão do dia 01/06/2011Tribunal Pleno).

Preliminarmente, foi realizada pesquisa na legislação específica e em órgãos que promovem procedimentos licitatórios, constatou-se a utilização dos seguintes índices contábeis, conclusivamente, os mais adotados no segmento de licitações.

Para os três índices colacionados (ILG, ILC e ISG), o resultado "> 1″ é indispensável à comprovação da boa situação financeira, sendo certo que, quanto maior o resultado (1,20; 1,30; 1,50; etc), melhor será a condição da empresa.

ÍNDICES CONTÁBEIS – Situação – ILC, ILG e ISG:

- < (menor) que 1,00: Deficitária;
- 1,00 a 1,35: Equilibrada;
- (maior) que 1,35: Satisfatória.

Diante de todo o exposto, conclui-se pela adoção dos índices que retratam situação financeira equilibrada e que aumentam consideravelmente o universo de competidores:

- ILG: maior ou igual a 1,00; e • ISG: maior ou igual a 1,00.

Portanto, o atendimento aos índices estabelecidos no Edital, demonstrará uma situação EQUILIBRADA da licitante. Caso contrário, o desatendimento dos índices, revelará uma situação DEFICITÁRIA da empresa, colocando em risco a execução do contrato. Ademais, os índices escolhidos foram democráticos, na medida em que estabelecem um "mínimo" de segurança na contratação.

2.3. REQUISITOS TÉCNICOS DA CONTRATAÇÃO

Para garantir a adequada execução dos serviços de suporte, monitoramento e gestão da infraestrutura de tecnologia da informação do Município, a empresa licitante deverá comprovar, no ato da habilitação, o atendimento a todos os requisitos mínimos de qualificação técnica e operacional, mediante a apresentação da documentação comprobatória exigida neste instrumento, sob pena de inabilitação.

- A empresa deverá possuir certificação válida em programas reconhecidos de qualidade de software ou serviços de tecnologia da informação, tais como International Organization for Standardization (ISO), CMMI Institute (CMMI) ou Associação para Promoção da Excelência do Software Brasileiro (MPS.BR), ou equivalente.
- Para garantir a dedicação, estabilidade e comprometimento dos profissionais alocados, será considerado vínculo empregatício válido somente aquele formalizado via Consolidação das Leis do Trabalho (CLT), ou quando o(s) mesmo(s) for(em) sócio ou diretor, o que deverá ser comprovado através da fotocópia do Contrato Social ou ata de assembleia. Essa exigência assegura a continuidade dos serviços, a conformidade com as normas trabalhistas vigentes e a disponibilidade dos profissionais conforme previsto no contrato. Não sendo aceitos vínculos em caráteres temporários, contratação terceirizada (PJ) e outros.
- A empresa deverá comprovar possuir responsável técnico habilitado, devidamente registrado em conselho profissional competente, quando aplicável, para acompanhamento de atividades técnicas que exijam responsabilidade técnica formal.
- A empresa deve ser registrada no CREA ou CAU ou outro conselho que o ampare e possuir profissionais, com as seguintes características:
- Profissional Responsável Técnico com registro no CREA ou CAU, ou outro conselho que o ampare, que será o responsável por eventuais instalações elétricas e lógicas e pela responsabilidade técnica de qualquer projeto que necessite de Anotação de Responsabilidade Técnica (ART) junto aos conselhos citados.

- Possuir em seu quadro pelo menos 01 (um) técnico com treinamento comprovado em LGPD (Lei Geral de Proteção de Dados).
- A empresa contratada deverá possuir em seu quadro pelo menos três (03) profissionais graduados na área de tecnologia, devidamente comprovados por diploma, com vínculo empregatício formal com a empresa. Essa exigência visa garantir a disponibilidade de profissionais qualificados para assegurar a cobertura contínua de suporte técnico 24 horas por dia.
- Possuir em seu quadro pelo menos (01) um funcionário pós-graduado em redes e servidores ou correlata, comprovados por diploma, com vínculo empregatício formal com a empresa.
- A empresa contratada deverá possuir em seu quadro pelo menos 1 (01) técnico com certificado valido na solução de Proxy/Firewall ofertada, com vínculo empregatício formal com a empresa.
- Possuir em seu quadro pelo menos 01(um) técnico com certificado válido em equipamentos Mikrotik (MTCNA ou equivalente), para manter em funcionamento os serviços entregues pela operadora, pois os equipamentos são de gestão da Administração municipal.
- Possuir em seu quadro pelo menos 01(um) técnico com certificado válido em equipamentos Mikrotik (MTCSE ou equivalente), para manter em funcionamento os serviços entregues pela operadora, pois os equipamentos são de gestão da Administração municipal.
- Possuir em seu quadro pelo menos 01 (um) técnico com certificado válido Ubiquiti (UWA ou equivalente), pois existem equipamentos já instalados na Administração municipal.
- A empresa licitante deverá apresentar carta de anuência específica para este certame, emitida pelo fornecedor ou distribuidor nacional da solução de firewall ofertada, atestando ciência e concordância com a participação da empresa no processo licitatório.
- A empresa contratada deverá possuir em seu quadro pelo menos três (03) técnicos com certificado valido na solução de Antivírus ofertada, com vínculo empregatício formal com a empresa. Essa exigência visa garantir a

disponibilidade de profissionais qualificados para assegurar a cobertura contínua de suporte técnico 24 horas por dia.

- A empresa licitante deverá apresentar carta de anuência específica para este certame, emitida pelo fornecedor ou distribuidor nacional da solução de antivírus ofertada, atestando ciência e concordância com a participação da empresa no processo licitatório.

2.3.1 NÍVEIS DE SERVIÇO (SLA)

- A solução deverá atender a níveis mínimos de disponibilidade e desempenho, considerando que os serviços de tecnologia da informação são essenciais para o funcionamento das atividades administrativas da Prefeitura.
- Os níveis de serviço deverão contemplar serviços de rede, segurança da informação, sistemas de backup e demais componentes contratados essenciais ao funcionamento do ambiente tecnológico.
- Os serviços considerados de missão crítica, sistemas de autenticação de rede, serviços de arquivos e soluções de segurança, deverão possuir elevados níveis de disponibilidade, com monitoramento contínuo e ações rápidas de atendimento e resolução de incidentes.
- A contratada deverá disponibilizar equipe técnica de atendimento e suporte, composta por profissionais de suporte remoto especializado, garantindo atendimento aos chamados técnicos e a manutenção da continuidade dos serviços.
- Para acompanhamento da execução contratual, a contratada deverá fornecer relatórios periódicos de desempenho e disponibilidade dos serviços, contendo indicadores de atendimento, disponibilidade dos sistemas, tempo de resolução de incidentes e histórico de ocorrências relevantes.

2.4. TECNOLOGIA DA INFORMAÇÃO NA PRESTAÇÃO DE SERVIÇO DE CONFIGURAÇÃO INICIAL E INSTALAÇÃO DE SERVIDOR E FIREWALL E MIGRAÇÃO

2.4.1. Identificação e Documentação da Infraestrutura:

a) É necessário identificar e documentar TODA a infraestrutura de redes, servidores, ativos e serviços implantados, visando o planejamento adequado

das atividades de manutenção e possíveis migrações de dados e equipamentos.

b) Pode existir a necessidade de quebra se senhas de alguns equipamentos;

c)Planejar e agendar, junto aos fornecedores afetados pela intervenção, os serviços de manutenção e migração.

d)Criar projeto e validar a documentação junto ao responsável pelo setor de TI da Prefeitura, realizando os ajustes necessários. Para depois começar a execução.

e) Criar uma cópia da estrutura atual em servidores próprios da CONTRATADA, local ou remoto, possibilitando uma rápida recuperação dos dados e sistemas em caso de incidentes durante a implantação (período máximo de 90 dias), incluso no custo do serviço de migração.

f) Verificar e validar a configuração e estrutura de rede ligada aos firewalls atuais para a migração.

g) Documentar VLANs, regras de firewall, *traffic shapping,* configurações de interfaces, configurações de endereçamentos IP de WANs e LANs. Regras de NAT e *forward.*

2.4.2. Organização dos Racks:

a) Organizar os racks que acomodarão o servidor e o Firewall, garantindo conformidade com as normas técnicas vigentes.

b) Instalar fisicamente Servidor e Firewall do LTE.

c)Verificar a adequação dos equipamentos instalados no rack, realizando as modificações necessárias mediante aprovação do Gestor do Contrato.

d)Conectar os equipamentos de rede utilizando fibra óptica (quando suportado) ou Patch Cord CAT6, atendendo às normas e legislações dos órgãos reguladores.

h) Organizar, configurar, realizar manutenção, ajustes e implementar melhorias nos servidores físicos e virtuais, bem como nos novos equipamentos adquiridos pela CONTRATANTE.

i)Validar a disposição dos equipamentos junto ao setor de TI da Prefeitura, promovendo os ajustes necessários.

j) Os materiais utilizados para conexão dos equipamentos no Data Center serão de responsabilidade exclusiva da CONTRATADA, incluindo *patchcords (UTP e óptico)*, conectores, switches topo de rack, SFP, cabos de energia, réguas de rack (PDU), *patchpanel*.

2.4.3. Projeto de Migração dos firewalls atuais para novo Firewall Locado:

a) Configuração inicial do Firewall;

b) Migrar endereçamentos de IP das interfaces;

c) Migrar e compatibilizar regras de firewall;

d) Migrar e compatibilizar regras de NAT e forwarding;

e) Criar e configurar proxy e filtros de camada

f) Migrar e criar demais regras de segurança;

g) Após a implantação do AD, configurar conexão LDAP;

h) Realizar testes diversos;

2.5. TECNOLOGIA DA INFORMAÇÃO NA PRESTAÇÃO DE SERVIÇO DE SUPORTE TÉCNICO CONTINUADO (N2/N3) E MONITORAMENTO 24/7 SOBRE OS SERVIÇOS CONTRATADOS

2.5.1. Suporte Técnico Especializado

a) A CONTRATADA deverá fornecer suporte técnico contínuo especializado de Nível 2 (N2) e Nível 3 (N3), com o objetivo de garantir a estabilidade, segurança e evolução da infraestrutura de Tecnologia da Informação da CONTRATANTE sobre os serviços contratados, com especial atenção ao gerenciamento de firewall, disponibilidade e otimização;

b) Apoiar a criação, configuração e implementação de novos serviços e soluções tecnológicas sobre os serviços contratados, conforme viabilidade técnica e necessidade da CONTRATANTE;

c) Analisar, definir e implementar políticas de segurança de acesso, incluindo:

- Avaliação e replicação, quando aplicável, das regras e políticas já utilizadas no ambiente atual para o novo ambiente e novos equipamentos;
- Configuração e revisão de regras de firewall, visando proteção contra acessos indevidos;

- Implementação e ajustes de proxy para controle de tráfego e segurança de navegação;
- Definição e manutenção de Objetos de Políticas de Grupo (GPO – Group Policy Object) para padronização e segurança do ambiente corporativo;
- Aplicação de outras políticas de segurança, visando garantir proteção e conformidade com normativas vigentes;

d) Realizar transferência de conhecimento tecnológico para a equipe de TI da CONTRATANTE, promovendo treinamentos e capacitações sobre as soluções implementadas;

e) Disponibilizar central de atendimento técnico 24 horas por dia, 7 dias por semana (24/7), composta por profissionais qualificados para:

- Atendimento de demandas de maior complexidade técnica;
- Monitoramento contínuo da infraestrutura e dos serviços críticos;

2.5.2. Implementação do Serviço de Monitoramento

a) A CONTRATADA será responsável pela implementação e operação de um Centro de Operações de Rede (NOC – Network Operations Center), com funcionamento 24 horas por dia, 7 dias por semana (24/7), garantindo a disponibilidade, segurança e desempenho dos serviços contratados pela CONTRATANTE;

b) O NOC deverá atuar como ponto central de supervisão, análise e resposta para a infraestrutura de TI da CONTRATANTE, garantindo atuação proativa em casos de falhas, incidentes ou ameaças sobre os serviços contratados;

c) O serviço deverá contemplar monitoramento contínuo e proativo, incluindo:

Supervisão em tempo real de ativos de rede, links de comunicação, aplicações e serviços de segurança;

Utilização de painéis de monitoramento (dashboards) para acompanhamento de métricas como CPU, memória, armazenamento, tráfego de rede e latência de serviços;

Monitoramento de infraestrutura física, incluindo temperatura, umidade e funcionamento de nobreaks, quando aplicável;

d) O serviço deverá incluir gerenciamento de incidentes e resolução de problemas, contemplando:

Detecção e priorização de incidentes com base no impacto operacional e criticidade;

Acionamento imediato do suporte técnico N2 e N3 para análise e resolução de incidentes, conforme níveis de serviço estabelecidos;

Aplicação de correções remotas, sempre que possível, com o objetivo de reduzir o tempo de indisponibilidade dos serviços;

Elaboração de relatórios pós-incidente, visando análise de causa raiz e implementação de melhorias preventivas;

e) O serviço deverá prever a realização de ações corretivas e preventivas, incluindo:

Aplicação de patches e atualizações de firmware e software, com o objetivo de reduzir vulnerabilidades;

Revisão e ajustes em regras de firewall e proxy, conforme necessidade de segurança e conformidade da CONTRATANTE;

Identificação e tratamento de ameaças de segurança cibernética, como tentativas de intrusão, acessos não autorizados e ataques de negação de serviço (DDoS);

f) O serviço deverá contemplar gestão de logs e auditoria de segurança, incluindo:

Coleta, análise e armazenamento de logs de eventos e acessos, permitindo rastreabilidade das atividades realizadas;

Correlação de eventos para detecção precoce de anomalias ou possíveis incidentes de segurança;

Emissão de relatórios periódicos para a CONTRATANTE contendo estatísticas de acessos, tentativas de invasão e avaliação de conformidade com políticas de segurança;

g) A CONTRATADA deverá garantir comunicação eficiente e acionamento das equipes técnicas, incluindo:

Disponibilização de canais de comunicação 24/7 entre o NOC, a CONTRATANTE e fornecedores externos, tais como telefone, sistema de help desk, aplicativo de mensagens e e-mail;

Notificação imediata de eventos críticos ao Gestor do Contrato, garantindo transparência e rápida tomada de decisão.

2.5.3. Ambiente Legado

a) A infraestrutura de rede da Administração Municipal é composta por dispositivos sem fio e equipamentos de rede cabeada, incluindo equipamentos das marcas Ubiquiti/Unifi, Intelbras, Mikrotik, D-Link, TP-Link e 3Com, os quais deverão ser

configurados, monitorados e mantidos, garantindo a estabilidade, segurança e desempenho da comunicação de dados;

b) A CONTRATADA será responsável por:

Realizar a configuração e otimização dos equipamentos de rede sem fio e cabeada, garantindo o melhor desempenho da rede;

Executar monitoramento contínuo da infraestrutura, com o objetivo de identificar falhas, degradação de desempenho ou tentativas de acesso não autorizado;

Gerenciar políticas de segurança, incluindo controle de acesso, segmentação de rede (VLANs), qualidade de serviço (QoS) e recursos de firewall quando disponíveis;

Realizar atualizações, ajustes e melhorias de configuração nos equipamentos sempre que necessário;

c) A adequada gestão desses equipamentos é essencial para garantir eficiência na conectividade interna e externa da Administração Municipal, assegurando níveis adequados de segurança, desempenho e disponibilidade dos serviços de rede;

d) A estrutura legada atualmente é composta, entre outros, pelos seguintes equipamentos:

- Switches TP-Link;
- Switches D-Link;
- Switches 3Com;
- Switches Intelbras;
- Servidor NAS Sinology
- Servidor HP DL380
- Mini PC (utilizado como firewall Pfsense)
- Servidor Dell (saúde)
- Roteador TP LINK

e) Os materiais e equipamentos necessários para operação dessa infraestrutura são disponibilizados pela CONTRATANTE, cabendo à CONTRATADA sua configuração, gerenciamento e manutenção conforme as necessidades do ambiente.

2.6. TECNOLOGIA DA INFORMAÇÃO PARA FORNECIMENTO, NA MODALIDADE LOCAÇÃO, DE FIREWALL CORPORATIVO

a) Deverá ser fornecido equipamento de segurança de rede do tipo Next Generation Firewall (NGFW) com funcionalidades integradas de proteção de rede, aplicações e sistemas web, capaz de identificar, prevenir e responder a ameaças avançadas em tempo real, incluindo malware, ransomware, ataques APT e ameaças de dia zero.
b) O equipamento deverá operar como solução unificada de segurança perimetral, incorporando funcionalidades avançadas de inspeção de tráfego, inteligência artificial aplicada à detecção de ameaças e mecanismos de análise comportamental.

c) O equipamento deverá possuir arquitetura integrada contendo, no mínimo, os seguintes recursos:

- Firewall de próxima geração (NGFW);
- Sistema de prevenção de intrusão (IPS);
- Controle de aplicações (Application Control);
- Filtro de URLs;
- Antivírus e antimalware;
- Proteção contra ameaças avançadas (APT);
- Sandbox em nuvem para análise de arquivos suspeitos;
- Web Application Firewall (WAF);
- Detecção e bloqueio de botnets;
- Análise comportamental baseada em inteligência artificial;
- Plataforma de inteligência de ameaças integrada.

d) A solução deverá utilizar mecanismos de inteligência artificial e machine learning para detecção de ameaças desconhecidas e ataques de dia zero.

- Correlação de eventos de segurança;
- Detecção de malware desconhecido;
- Identificação de domínios maliciosos;
- Monitoramento de comportamento suspeito de rede;
- Análise automatizada de ameaças.

e) A solução deverá possuir mecanismo de análise de malware baseado em IA capaz de detectar variantes desconhecidas sem necessidade de assinatura prévia.
f) A solução deverá prover no mínimo os seguintes recursos de proteção:

- Proteção contra ransomware

- Proteção contra ataques de rede
- Proteção contra ataques web (SQL Injection, XSS, Web Shell, entre outros)
- Detecção de tráfego malicioso
- Inspeção profunda de pacotes (Deep Packet Inspection)
- Controle de acesso por aplicação
- Gerenciamento de largura de banda
- Identificação automática de ativos de rede
- Avaliação de vulnerabilidades

g) A solução deverá possibilitar descoberta automática de ativos não gerenciados na rede, identificando riscos como vulnerabilidades, aplicações não autorizadas e dispositivos IoT.

h) O equipamento deverá possuir sistema de monitoramento e gerenciamento que permita:

- Visualização centralizada de eventos de segurança
- Dashboard de ameaças em tempo real
- Identificação automática de incidentes relevantes
- Recomendações de mitigação
- Otimização automática de políticas de segurança

i) O sistema deverá fornecer visibilidade completa de usuários, aplicações, tráfego e ativos da rede.

j) O equipamento deverá possuir desempenho mínimo, com as seguintes capacidades:

- Throughput de Firewall: 20 Gbps
- Throughput com controle de aplicações: 12 Gbps
- Throughput NGFW: 3 Gbps
- Throughput com prevenção de ameaças: 1,5 Gbps
- Throughput de proteção de aplicações web (WAF): 2,3 Gbps
- Throughput IPsec VPN: 1,5 Gbps
- Túneis IPsec simultâneos: 1.000
- Conexões simultâneas: 2.000.000
- Novas conexões por segundo: 90.000

k) Especificações Técnicas mínimas:

- 8 portas Ethernet 10/100/1000 Base-T
- 2 interfaces SFP
- 1 porta de gerenciamento RJ45
- 1 porta serial
- 2 portas USB

l) O equipamento deverá possuir no mínimo as seguintes certificações:

- CE
- FCC
- RoHS

2.6.1. Recursos de Segurança e Controle de Acesso

m) A solução deverá suportar VLANs padrão IEEE 802.1Q;

n) O firewall deverá permitir criação de regras baseadas em:

- IP de origem e destino
- Portas TCP/UDP
- Protocolos
- Limite de conexões simultâneas
- Balanceamento de links ou failover por regra.

o) A solução deverá permitir criação de objetos de rede, incluindo:

- Endereços IP
- Portas
- URLs
- Sub-redes.

p) O firewall deverá possuir controle de aplicações na camada 7 (Application Firewall), permitindo:

- Identificação de aplicações independentemente de porta ou protocolo;
- Bloqueio ou liberação por aplicação;
- Regras baseadas em usuários ou grupos.

q) A solução deverá permitir integração com Microsoft Active Directory ou base local de usuários;

r) O firewall deverá reconhecer aplicações em diversas categorias, incluindo no mínimo:

- Redes sociais

- Portais web
- Aplicações corporativas
- Conteúdo adulto
- Aplicações potencialmente perigosas.

s) O sistema deverá apresentar painel de monitoramento de aplicações, incluindo informações de:

- Aplicação utilizada
- Usuário responsável
- Data e hora do acesso
- Status (permitido ou bloqueado).

t) A solução deverá gerar relatórios de uso de aplicações e consumo de banda.

2.6.2. Proteção Contra Ameaças

u) O firewall deverá possuir proteção contra ameaças em camada de aplicação (Layer 7), incluindo:

- Worms
- Trojans
- Malware
- Protocolos de anonimização e VPN não autorizadas.

v) A solução deverá incluir mecanismos integrados de:

- **Malware**
- **Phishing**
- **Spyware**
- **Ransomware**
- **Intrusões (IDS/IPS)**

w) O sistema deverá apresentar dashboard com informações geográficas das tentativas de ataque;

2.6.3. Recursos de Rede e Conectividade

x) A solução deverá suportar:

- NAT

- Port forwarding
- NAT avançado
- NAT reflection.
- DHCP Server
- DHCP Relay
- DNS dinâmico
- SNMP
- NTP.

y) A solução deverá permitir balanceamento de links e failover automático;

z) O firewall deverá permitir criação de VPNs do tipo Site-to-Site e Client-to-Site, incluindo suporte a:

- IPSec
- SSL VPN.

2.6.4. Gerenciamento e Logs

aa) A solução deverá permitir registro e armazenamento de logs, incluindo:

- Firewall
- DHCP
- Autenticação
- VPN
- Balanceamento de links.

ab) Os logs deverão poder ser enviados para servidores externos (Syslog);

ac) A solução deverá possuir suíte de relatórios integrada, acessível também por dispositivos móveis;

ad) O sistema deverá permitir gerenciamento de certificados digitais e controle de acesso administrativo.

2.6.5. Alta Disponibilidade

ae) O equipamento deverá suportar modo cluster (failover), permitindo operação com dois equipamentos em redundância;

af) Em caso de falha do equipamento primário, o secundário deverá assumir automaticamente sem interrupção dos serviços.

2.6.6. Características do Equipamento (Appliance)

ag) A solução deverá ser fornecida em appliance dedicado, integrando hardware e software do fabricante;
ah) Não serão aceitos equipamentos SOHO ou destinados a uso doméstico;
ai) Caso o fabricante disponibilize modelo superior durante a vigência do contrato, a CONTRATADA deverá efetuar a substituição sem custos adicionais.

2.7. TECNOLOGIA DA INFORMAÇÃO NA PRESTAÇÃO DE SERVIÇO BACKUP LOCAL E EM NUVEM

a) A CONTRATADA deverá disponibilizar infraestrutura de armazenamento em nuvem com capacidade mínima de 5 TB, destinada ao armazenamento de backups da infraestrutura de TI da CONTRATANTE;
b) O ambiente de armazenamento deverá estar disponível 24 horas por dia, 7 dias por semana (24x7), garantindo restauração sempre que necessário;
c) O armazenamento deverá estar hospedado em data center localizado em território nacional, com certificação mínima TIER III ou equivalente;
d) A CONTRATADA será responsável pelo fornecimento, gerenciamento e manutenção do ambiente de armazenamento em nuvem, incluindo a capacidade necessária para suportar:

- Servidores físicos;
- Máquinas virtuais;
- Sistemas e aplicações da CONTRATANTE.

2.7.1. Software de Backup

e) O software responsável pelo gerenciamento do backup deverá possuir **console de gerenciamento totalmente em nuvem**, acessível via **HTTPS**;
f) A solução deverá suportar **múltiplos repositórios de backup**, incluindo no mínimo:

- S3 ou compatível
- NFS
- NAS

- Armazenamento em nuvem.

g) O sistema deverá disponibilizar **agentes de backup nativos**, gerenciados por console centralizado.

h) Os agentes de backup deverão ser compatíveis, no mínimo, com:

- Sistemas **Microsoft Windows** (desktop e servidor)
- **macOS**
- **Distribuições Linux** amplamente utilizadas
- **Hipervisores VMware e Hyper-V**.

i) A solução deverá suportar backup de aplicações corporativas, incluindo no mínimo:

- Microsoft Exchange
- Microsoft SQL Server.

2.7.2. Funcionalidades do Sistema de Backup

j) A solução deverá disponibilizar, no mínimo, os seguintes recursos:

- Compressão e criptografia de dados;
- Deduplicação de dados;
- Política de retenção **GFS (Grandfather-Father-Son)**;
- Verificação automática de consistência dos backups;
- Testes automatizados de restauração;
- Imutabilidade de backups (proteção contra ransomware).

k) O sistema deverá permitir:

- Backup de máquinas virtuais;
- Restauração granular de arquivos;
- Restauração em hardware diferente;
- Restauração para ambientes locais ou nuvem pública.

l) A solução deverá permitir **controle de acesso e auditoria**, incluindo:

- Autenticação em dois fatores (2FA);
- Controle de permissões por usuário;
- Registro de logs de todas as operações realizadas.

2.7.3. Políticas e Planos de Backup

m) A solução deverá permitir a criação de planos e políticas de backup, contemplando no mínimo:

- Backup completo (Full);
- Backup incremental;
- Backup diferencial.

n) O sistema deverá permitir:

- Agendamento automático das rotinas de backup;
- Definição de políticas de retenção;
- Seleção de arquivos, pastas ou servidores para backup.

o) A solução deverá disponibilizar relatórios e alertas, incluindo:

- Status de backups;
- Alertas de falhas;
- Relatórios de atividades;
- Sumário de execução semanal.

2.7.4. Backup Local

a) A solução deverá contemplar armazenamento local para backup com capacidade mínima de 5 TB;

b) O mesmo software utilizado para backup em nuvem deverá ser utilizado para o gerenciamento do backup local;

c) A CONTRATADA será responsável por:

- Criação e configuração das rotinas de backup;
- Monitoramento das execuções;
- Correção de falhas identificadas;
- Proposição de melhorias nas políticas de backup.

2.8. TECNOLOGIA DA INFORMAÇÃO NO FORNECIMENTO DE SOLUÇÃO DE ANTIVÍRUS – 100 LICENÇAS

2.8.1 Licenciamento

a) A solução deverá contemplar:

- 95 (noventa) licenças para estações de trabalho;
- 5 (cinco) licenças para servidores Windows ou Linux.

b) O quantitativo foi estimado considerando:

- Computadores cadastrados na rede de fibra urbana;
- Equipamentos das unidades da área rural;
- Computadores dos laboratórios;
- Equipamentos do Paço Municipal.

c) Atualmente estima-se:

- 40 computadores no Paço Municipal;
- Aproximadamente 40 computadores nas demais unidades administrativas.

d) Considerando a aquisição contínua de novos equipamentos e notebooks institucionais, foi adotada margem de segurança de 100 licenças, garantindo cobertura do parque computacional.

2.8.2 Características Gerais da Solução

- A solução de antivírus deve estar devidamente licenciada e atender a todos os requisitos descritos abaixo, garantindo uma proteção abrangente e eficiente contra ameaças cibernéticas;
- Deverá possuir a capacidade de varrer, detectar, analisar e remover malwares, riskwares, spywares e demais formas de ameaças e códigos maliciosos conhecidos, que estão associadas a tipos específicos de malware para detectar e prevenir ataques semelhantes.
- Deverá possuir a capacidade de proteção uma combinação de inteligência artificial, detecção comportamental, algoritmos de aprendizado de máquina e mitigação de exploração, que utiliza de consulta em nuvem do fabricante para antecipar e prevenir ameaças conhecidas e desconhecidas (zero-day), usando uma abordagem não dependente de assinatura para fornecer uma segurança de endpoint complementar e mais eficaz;
- Além dos mecanismos de proteção contra malware, tanto via assinatura quanto com base em consulta em nuvem, o produto deverá possuir capacidade de quarentena de arquivos centralizada, bem como Firewall, IDS/IPS/HIPS, controle de aplicativos, controle de conexões, atualizador de softwares, proteção para a navegação, reversão de arquivos comprometidos, controle de conteúdo web por categorias, criptografia de disco, controle de dispositivos e quarentena de rede. Estas devem ser totalmente integradas, instaladas através

de um único agente sem a necessidade de instalação de módulos adicionais ou agente de comunicação prévio;

- O conjunto de softwares que compõe a solução de antivírus deverão ser totalmente gerenciáveis através de uma única console de gerenciamento centralizado, em nuvem (Cloud) e de forma que todos os produtos sejam monitorados através desta.
- Ter a funcionalidade de repositório remoto centralizado e integrado de atualizações do produto, bem como a lista de vacinas de vírus (assinatura de malwares), do mecanismo da solução (engines) e principalmente do cache/repositório de atualizações de software da Microsoft e de terceiros (atualizador de softwares), podendo o administrador instalar sem ônus, com suporte para as plataformas Windows e Linux, podendo o administrador escolher a plataforma desejada de acordo com seu ambiente;
- Ter a função de prevenção de epidemia ou isolamento do host na rede, de forma manual ou automática;
- O fabricante deve possuir site próprio para envio de amostras de arquivos e URL, infectados, suspeitos ou falsos positivos, e que registre por e-mail através de um código identificado (por exemplo, número do chamado, protocolo ou solicitação).
- Possuir suporte à integração com soluções no padrão Syslog/SIEM (Security Information and Event Management);
- O fabricante deverá ser membro do programa “Microsoft Active Protection Program” para obtenção de acesso antecipado a informações de vulnerabilidade para que eles possam fornecer proteções atualizadas aos clientes mais rapidamente;
- O fabricante deve seguir e respeitar o Framework de Cibersegurança do NIST (National Institute of Standards and Technology) e a NBR ISO/IEC 27001 com suas soluções de segurança;
- A solução deve ser certificada pela organização independente e reconhecida, AV-TEST;
- A solução deve usar o MITRE ATT&CK para fornecer informações correlacionadas;

- Suportar o gerenciamento de todos os endpoints a partir da nuvem do próprio fabricante, sendo vedada a possibilidade de hospedar em terceiros;
- A console de administração deve centralizar a administração dos sistemas operacionais Windows, macOS, Linux e dispositivos móveis;
- Permitir a criação de tipo de usuários para acesso à console de gerenciamento, com no mínimo as opções de usuário administrador e usuário para leitura (read only);
- Não possuir restrições para múltiplos logins simultâneos de usuários ao sistema de gerenciamento da solução;
- Deve ser possível implementar MFA (Multi-Fator de Autenticação) para todos os usuários da console de Administração
- Manter um registro de ações realizadas pelos administradores no sistema de gerenciamento da solução de segurança;
- Atualização de listas, vacinas, mecanismos de varredura e desinfecção através da Internet via protocolo HTTP/80 ou HTTPS/443 (visando evitar conflitos com protocolos e portas ou não permitidos em nossa rede/data center/DMZ/VPN) e disponibilizando estas atualizações para todas as demais ferramentas que compõem a solução de anti-malware automaticamente sem a intervenção do administrador;
- Comunicação segura entre a console de gerenciamento e clientes gerenciados utilizando protocolo seguro HTTPS através da porta TCP/443, visando ter mais segurança da comunicação e proteção das configurações de políticas do produto, além de evitar conflitos com protocolos e portas não permitidos em nossa rede/data center/DMZ/VPN.
- Ser capaz de atrelar uma política de configuração automaticamente para novas máquinas ingressadas no domínio;
- Ser capaz de atrelar uma política de configuração do produto a uma Unidade Organizacional do MS Active Directory, ou seja, ser possível atrelar uma política de configuração Financeiro às máquinas da OU de nome Financeiro no MS AD;
- A console de gerenciamento dos endpoints em Nuvem deve ser capaz de propor recomendações de segurança baseado nas detecções do ambiente;

- A solução deve conter um único agente de instalação para gerenciar todas as funções nas estações de trabalho e fazer comunicação direta com a plataforma de gerenciamento, sem a necessidade de interfaces ou equipamentos intermediários;
- A solução deve ter um único agente conectado a console de administração para todos os recursos descritos nesse documento;

Deverá ser possível e estar licenciado para coletar as seguintes informações dos dispositivos gerenciados:

Versão do agente instalado;

- Nome e versão do sistema operacional;
- Quantidade de memória RAM;
- Tamanho total e espaço livre do Disco;
- Fabricante e modelo da CPU;
- Versão da BIOS;
- Endereços IP atribuídos;
- Endereço IP externo da origem da conexão;
- Chave de recuperação de sistemas operacionais criptografados;
- Endereço físico (MAC);
- Nome do Host;
- Nome do usuário conectado no dispositivo;

Permitir a alteração das configurações do produto/agentes endpoint nos clientes de maneira remota;

Deve ser capaz de bloquear as configurações nos endpoints, evitando que os usuários ou administradores locais alterem as configurações do produto;

Deve ser capaz de bloquear o encerramento dos processos do produto e a sua desinstalação nos endpoints, mesmo os usuários com privilégios de administradores locais ou do domínio;

Deve ser capaz de configurar uma senha através da console de gerenciamento, que será solicitada ao usuário, caso seja executado uma das seguintes ações no endpoint: desinstalar o produto, desativar todos os recursos de segurança ou desativar temporariamente os recursos de segurança;

A solução deve permitir fácil acesso às estações de trabalho através de conexão RDP (Remote Desktop Protocol), proporcionando meios como atalhos (rdp://hostname) ou botões de acesso direto;

Geração de relatórios que contenham informações sobre as infecções e atualizações da solução;

Deve ter a capacidade de exportar relatórios gerados pela solução;

- Enviar alertas em caso de epidemias através de e-mail;
- Permitir a visualização de relatórios contendo as seguintes informações:
- Visão geral do status de proteção;
- Relatório de uso de assinatura;
- Relatório de eventos de segurança;
- Relatório de registro de auditoria;
- Possuir no dashboard informações do estado geral da solução de segurança e hosts gerenciados;
- Possuir no dashboard status geral de atualizações de software do ambiente;
- Os logs de eventos gerados e armazenados na plataforma devem possuir no mínimo as seguintes informações:
- Data e hora do evento;
- Gravidade;
- Módulo de proteção que gerou o evento;
- Máquina em que ocorreu o evento de segurança;
- Descrição do evento;
- Nome do usuário;
- Identificar eventos similares;
- Deve ser possível exportar os logs de eventos;

Deve ser possível facilitar e customizar a identificação do dispositivo na console, através de: grupos de máquinas, TAGs e/ou grupos;

Deve ser possível através da console de gerenciamento, realizar manualmente as seguintes tarefas nos dispositivos, de forma individual ou agrupado:

- Aplicar atualizações de Software;
- Verificar atualizações pendentes;
- Realizar a verificação de existência de malware (Scan);

- Remover e/ou desinstalar o dispositivo da console de gerenciamento;
- Entrar ou sair do modo de isolamento de rede;
- Reiniciar o sistema operacional;
- Reiniciar o serviço do agente de Endpoint Protection;
- Enviar mensagens customizadas para o dispositivo;
- Desativar e/ou reativar recursos individuais de segurança;

A solução deverá possuir suporte, no mínimo, aos seguintes sistemas operacionais:

- Microsoft Windows 11 (todas as edições 64-bits, incluindo ARM64);
- Microsoft Windows 10 (edições 32-bit e 64-bits);
- macOS 12 "Monterey", 13 "Ventura" e 14 "Sonoma";
- AlmaLinux 8, 9;
- Amazon Linux 2;
- CentOS 7 e 8;
- Debian 10, 11, 12;
- Oracle Linux 7, 8, 9;
- RHEL 7, 8, 9;
- Ubuntu 18.04, 20.04, 22.04, 24.04;

A interface dos clientes de proteção do endpoint deve ter a opção de ser instalada em português do Brasil;

A solução de proteção do endpoint deve permitir ser instalada, no mínimo, através das seguintes opções:

Via pacote MSI compatível com MS GPO (Active Directory), Através de scripts de instalação;

Instalação manual com envio de informações automáticas por e-mail;

Ter a possibilidade de configuração de políticas diferenciadas para cada estação ou grupo de estações;

Deve ser possível ocultar a interface do agente de segurança do endpoint da barra de tarefas do sistema para evitar a intrusão do usuário e higienização da barra de tarefas dos aplicativos;

A solução deve incluir um mecanismo de atualização automática dos agentes de endpoints instalados, eliminando a necessidade de intervenção manual por parte do administrador, garantindo que todos os endpoints permaneçam atualizados com as últimas definições de segurança do agente;

Os endpoints devem ter a capacidade de consultar um proxy HTTP, definido através da console de gerenciamento, para realizar as atualizações automáticas;
Deve ser possível definir pastas, arquivos e hashes de arquivo do tipo SHA-1, possibilitando estes serem excluídos de todas as verificações e medidas de segurança;
Deve ser possível exibir ou ocultar as notificações relacionadas à expiração da licença;
Deve ser possível definir a quantidade de dias anteriores à expiração da licença para começar a mostrar notificações;
Deve ser possível definir uma mensagem que será exibida para os usuários antes que a licença expire;
Proteção em tempo real;
Deve possuir verificação em tempo real de todos os objetos / artefatos que os usuários f inais acessam ou executam;
Possuir gerenciamento e configuração remota para a funcionalidade de antivírus, anti spyware, anti-malwares, detecção de rootkit e proteção de browser;

Possuir gerenciamento e configuração remota para a funcionalidade de Zero Hour e/ou Zero Day, análise comportamental de ameaças, deverá também ter ação contra arquivos raros ou suspeitos;
Deve possuir integração da Interface de Verificação de Anti-malware (AMSI), que permite que os sistemas operacionais usem mecanismos fabricante de Anti-malware para fornecer segurança adicional. Por exemplo, o Windows usa o AMSI para verificar scripts do PowerShell e macros do Office VBA com as soluções anti-malware instaladas;
Deve ser possível verificar automaticamente todos os arquivos que serão executados;
Deve ser possível definir extensões de arquivos que serão excluídos da varredura em tempo real; Deve ser possível definir processos que serão excluídos da varredura em tempo real;
Deve ser possível decidir a ação automaticamente em caso de detecção de uma infecção.
As ações no objeto infectado devem ser pelo menos:

- Renomear;

- Excluir;
- Desinfetar;
- Quarentenar;

Deve ser possível atribuir ações diferentes para Riskware e Spywares detectados;
Deve possibilitar proteger o arquivo “Hosts”. Com esse recurso ativado todas as alterações serão revertidas para um arquivo limpo;
Deve possibilitar verificar arquivos armazenados em unidades de rede;
A solução deve integrar-se com um sistema de análise de ameaças cibernéticas baseado em nuvem, que utilize inteligência artificial e aprendizado de máquina para analisar e refinar dados de ameaças. Este sistema deve fornecer uma rede de proteção em tempo real, aproveitando dados de milhões de dispositivos conectados, garantindo detecção rápida e precisa de novas ameaças;
Verificação Manual e Agendada
Deve permitir que o escaneamento seja configurado pelo administrador, com frequência diária, em horário definido, para todas as estações, para um grupo ou estações específicas;
Possuir capacidade de diminuir a prioridade do processo evitando a sobrecarga do processamento da estação de trabalho, e dessa forma causando menos impacto para o usuário final;
Deve ser possível controlar o que acontece quando um dispositivo de armazenamento USB é conectado ao computador, possuindo pelo menos as seguintes ações:

- Não fazer nada;
- Pedir para o usuário para verificar o USB;
- Verificar o USB silenciosamente;
- Fazer a verificação do USB e mostrar o resultado para o usuário;

Deve ser possível definir uma frequência de escaneamento de malware, possibilitando escolher pelo escaneamento diário, semanal ou mensal;
Deve ser possível especificar os dias da semana e o horário do escaneamento de procura por malwares no disco;
Deve ser possível especificar por extensões (por exemplo: COM EXE SYS BIN SCR DLL SHS HTM HTML HTT VBS JS), os arquivos que serão escaneados pelo produto;

Deve ser possível habilitar ou desabilitar a verificação de arquivos dentro de arquivos compactados (por exemplo, arquivos ZIP);
Deve ser possível habilitar ou desabilitar a verificação de arquivos que estão dentro dos arquivos da caixa de correio (por exemplo, arquivos pst);
Deve ser possível definir uma das seguintes ações, após detecção de um arquivo malicioso encontrado:

- Limpar;
- Excluir;
- Renomear;
- Quarentenar;
- Perguntar ao usuário;

Deve ser possível definir a quantidade de recursos do sistema que a verificação pode usar, podendo definir um modo de menor consumo de recursos no host analisado;

Deve ser possível a definição de arquivos ou pastas que serão excluídos da verificação;
Controle de conteúdo web;
Deve possuir gerenciamento e configuração remota para a funcionalidade de controle do Conteúdo da Web por categorização do conteúdo, independente do firewall da rede, pois, em caso dos equipamentos estiverem fora do parque computacional (por exemplo home office ou em trânsito) as políticas da corporação podem continuar sendo adotadas, além de controle específico para proteger equipamentos que necessitam de conexões bancárias;
Possuir controle de conteúdo da navegação web, com no mínimo 15 categorias, que sejam atualizadas e fornecidas pelo fabricante, sem necessidade de criar/acrescentar ou customizar novas categorias manualmente. As categorias desejadas são:

- Serviços de Pagamento;
- Bancos/Transações Bancárias;
- Hacking/Invasão;
- Navegação anonima/proxy/vpn;
- Chat/Bate Papo/Namoro;

- Golpe/Phishing/Spam;
- Downloads considerados Ilegais;
- Downloads de Softwares (em geral);
- Streaming;
- Entretenimento;
- Jogos;
- Redes Sociais;
- Compras Online;
- Webmails;
- Conteúdo Adulto;

O controle de conteúdo por categorização deve permitir a configuração por grupos, podendo o administrador determinar, por grupo, quais categorias serão permitidas ou não e se o controle estará ativado para aquele grupo ou não;

Deve possibilitar adicionar manualmente através da console de gerenciamento, websites que serão permitidos ou bloqueados nos grupos de estações de trabalho;

Deve possibilitar através de uma opção de configuração, o bloqueio imediato de acesso a todos os sites e deve ser possível especificar uma lista de websites de exceção que serão permitidos caso esta opção seja configurada; 82. Deve possibilitar que os usuários com direitos administrativos na estação de trabalho prossigam ou não para as páginas bloqueadas;

A solução de proteção de navegação deve usar mecanismos para identificar a reputação de websites, classificando-os como:

- Perigosos;
- Suspeitos;
- Proibidos;

Deve ser possível mostrar a reputação dos websites nos resultados de pesquisa da Web (Google e Bing);

Deve possibilitar a imposição de busca segura (conceito SafeSearch) nos endpoints, que faz com que os mecanismos de pesquisa usem o nível estrito para ocultar conteúdo adulto;

Deve possibilitar o controle de execução no navegador de tipos de conteúdo/mídias da Web, tais como: pdf, msword, x-excel, silverlight, flash e java;

Deve possibilitar adicionar regras customizadas para o controle de execução de tipos de conteúdo/mídias da Web;
Deve possibilitar armazenar na console de gerenciamento em Cloud todos os eventos de URL do website bloqueado;
Controle de Conexões Bancárias
Deve possuir a funcionalidade de bloqueio automático de novas conexões quando for detectado que foi aberta uma conexão bancária e/ou conexão que utilize protocolo seguro;
Além da detecção automática, deve ser possível também adicionar um conjunto de websites que processam informações confidenciais para serem protegidas pelo controle conexão;
Quando conectado a um portal de pagamento, a solução deverá restringir acesso remoto ao equipamento para evitar a exposição de dados sensíveis através de conexões remotas (Remote Desktop, Logmein, VNC, Anydesk, Teamviewer e etc);

A área de transferência do Windows deverá ser limpa após o encerramento das conexões bancárias, visando evitar equívocos dos usuários e a maior proteção dos dados que possam estar presentes na área de transferência durante o trabalho realizado em uma conexão com o banco (senhas, dados sensíveis, informações pessoais, etc.);
Quando conectado a um portal de pagamento, deverá ser possível bloquear automaticamente as conexões de rede de ferramentas de linha de comando e scripts;
Gerenciamento Firewall

- Deve possibilitar o gerenciamento e configuração remota para a funcionalidade de firewall através da console de gerenciamento em Cloud;
- Deve ser possível a criação de pelo menos 03 (três) perfis diferentes de firewall;
- Deve permitir controlar as conexões de entrada e saída dos endpoints;
- Deve possibilitar a definição de regras de entrada e saída baseadas em controle de portas TCP e UDP;
- Deve ser integrado ao Firewall do Windows, possibilitando escolher pela definição de novas regras de entrada e saída, bem como a definição apenas

de regras adicionais as já existentes no Firewall do Windows; Deve ser possível habilitar a notificação para o usuário final quando um novo evento de bloqueio de conexão for realizado pelo Firewall;

Deve possibilitar o isolamento da estação de trabalho, restringindo a comunicação da máquina com outros hosts da rede e da internet;

Deve possibilitar definir um conjunto de domínios ou FQDN, ao qual a estação de trabalho poderá se comunicar durante o tempo que estiver em modo de isolamento;

Deve possibilitar a retirada da máquina do isolamento através da console de gerenciamento em nuvem;

Deve ser possível definir uma mensagem personalizada, que será exibida para o usuário quando a estação de trabalho entrar em modo de isolamento;

Atualizador de softwares:

- Possuir gerenciamento e configuração remota para a funcionalidade de atualização de softwares de terceiros;
- Se baixar todas as atualizações diretamente da internet, os dispositivos de uma rede consomem uma enorme quantidade de tráfego externo. Para reduzir isso, deve ser possível usar um servidor local de cache, que baixará os arquivos solicitados apenas uma vez e, em seguida, os distribuirá para os dispositivos dentro da rede;
- O repositório de atualizações local deverá possibilitar ser instalado em Sistemas Operacionais Windows e Linux;

A solução de atualização de softwares de terceiros deve ter a capacidade e estar licenciado devidamente para implementar um repositório de atualizações local, que funcione como um armazenador de atualizações de software e vacinas para toda a rede corporativa;

O repositório centralizado e local das atualizações de software, deve haver compatibilidade com Microsoft e softwares de terceiros, tais como softwares da Google (Chrome), Oracle (Java), Mozilla (Thunderbird), dentre outros;

Deve ter a capacidade de verificar a disponibilidade de atualizações, gerenciar, obter os pacotes de instalação de forma centralizada, armazenar (cache local) e aplicar/instalar automaticamente as atualizações de softwares, melhorias e patches de correções disponibilizados pela Microsoft, para seus sistemas operacionais, aplicativos de escritório da família Microsoft Office e demais aplicativos como o .NET, Internet Explorer e Edge, entre outros softwares deste mesmo fabricante,

através de configurações na console de gerenciamento central da solução de proteção para endpoints;

Capacidade de verificar a disponibilidade de atualizações, gerenciar, obter os pacotes de instalação de forma centralizada, armazenar (cache local) e aplicar/instalar automaticamente as atualizações de softwares, melhorias e patches de correções para softwares de terceiros (Adobe, Oracle Java, Google Chrome, Zoom, 7-Zip, aplicativos Open Source como a família Open Office, Notepad++, Mozilla Firefox e Thunderbird, etc), através de configurações na console de gerenciamento central da solução de proteção para endpoints;

Deve ter a capacidade de aplicar as atualizações e correções de produtos Microsoft e de terceiros:

Em horário agendado;

- Sem a necessidade de intervenção ou ação do usuário final;
- Mesmo quando o usuário logado não possui privilégios administrativos;
- Mesmo quando o computador estiver bloqueado ou quando não houver usuário conectado;
- Quando necessário reiniciar o equipamento após um update, ser capaz de adiar o reboot para evitar atrapalhar o usuário em horário de trabalho;

Ter a capacidade de excluir atualizações especificas da varredura ou da instalação automatizada, seja ela pelo seu ID ou simplesmente pelo nome do produto, por exemplo “java”;

Deve ser capaz de gerar alertas sobre atualizações críticas de segurança pendentes de instalação;

Deve ser capaz de apontar através da console de gerenciamentos os CVEs (Common Vulnerabilities and Exposures) de cada atualização pendente no ambiente;

Possibilidade de criar lista de programas para exclusão da verificação da necessidade de atualização de software;

Controle de Dispositivos:

- Deve possuir gerenciamento e configuração remota para liberação ou restrição de funcionalidade de controle de dispositivos (Ex.: pen drives, hd externo, impressoras, Wi-Fi, bluetooth). Deverá possuir a capacidade de alertar caso um equipamento seja conectado, restringir acesso e a gravação

em dispositivos de armazenamento removíveis (pen drive e HD externo, por exemplo);

- Deve permitir bloquear dispositivos no mínimo pelo Hardware ID, ID do dispositivo, ID compatível e Classe GUID;
- Deve ter a capacidade de bloquear a escrita em dispositivos de armazenamento em massa, permitindo somente a leitura; 118. Deve ter a capacidade de bloquear a execução de binários (executáveis) a partir de dispositivos de armazenamento em massa;
- O bloqueio de dispositivos deve permitir bloquear um único dispositivo e liberar os demais, bem como liberar um único dispositivo e bloquear os demais. Ex.: Bloquear qualquer Pendrive exceto um em um único computador;
- Deve emitir alertas de tentativa de uso do dispositivo bloqueado por ordem do administrador do sistema, contendo no alerta o ID do dispositivo bloqueado e a identificação da máquina que tentou utilizá-lo;

Tarefas Automatizadas:

- Deve possuir a capacidade que criar backups do sistema operacional ou pontos de restauração do sistema de forma agendada e centralizada através da console de gerenciamento;
- Deverá ter a capacidade de buscar e upgrade do “instalador do agente de segurança” (tecnologia do cliente do endpoint, não referente a update de vacinas ou mecanismos internos do produto) e implementá-la automaticamente se disponível, para que ele possa estar sempre na versão mais moderna, com novas funcionalidade e atualizada, consequentemente deixando o ambiente mais protegido;
- Deverá ter a capacidade de automaticamente ou de forma agendada, bloquear, hibernar, reiniciar ou desligar o sistema operacional do endpoint;

Reversão de comprometimento:

- Deverá possuir a capacidade de efetuar backup em tempo real e reverter/restaurar arquivos ao estado original e o registro do sistema Windows em caso de uma infecção/ataque bem-sucedida por ransomware, tanto na estação de trabalho, quanto nos servidores;

- Deve possibilitar apenas o monitoramento do sistema operacional e apenas relatar alterações não autorizadas;
- Deverá ser possível especificar um caminho nos hosts protegidos que serão armazenados os arquivos de backup;
- Deve possibilitar especificar o tamanho máximo para os arquivos de backup. Desta forma se o tamanho de um arquivo exceder o valor fornecido, não será realizado o backup do arquivo, possibilitando assim evitar cópias de arquivos muito grandes;
- Configurações locais de rede
- A solução de proteção de endpoint deve oferecer a funcionalidade de configuração de diferentes locais de rede. Essa funcionalidade deve permitir que os administradores controlem e ajustem as configurações de segurança com base no local onde o dispositivo está conectado, proporcionando uma proteção adaptativa e específica para cada ambiente de rede;
- Um administrador pode configurar um perfil de rede “Em casa” onde o firewall e o Atualizador de Software estão ativados para garantir proteção máxima em uma rede possivelmente menos segura. Simultaneamente, o administrador pode configurar um perfil de rede “No escritório”, onde o firewall pode ser desativado (supondo que a rede do escritório já esteja protegida por um firewall centralizado) e o Atualizador de Software pode ser desativado para evitar interferências durante o horário de trabalho.
- A solução deve automaticamente aplicar as regras correspondentes assim que o dispositivo muda de uma rede para outra, garantindo uma segurança adaptada e eficaz em todos os cenários de uso;
- A solução deve permitir a criação e gerenciamento de múltiplos perfis de rede, cada um representando um ambiente de rede específico, tais como “Em casa”, “No escritório” e “Rede pública”;
- Cada perfil de rede deve incluir um conjunto de regras e políticas de segurança que se aplicam automaticamente quando um dispositivo é detectado em um determinado local de rede;

A solução deve ser capaz de identificar o local de rede com base em pelo menos:

- Máscara de rede;
- Endereço IP do servidor DHCP;

- Endereço IP do gateway padrão;
- Deve ser possível configurar múltiplos gatilhos para um mesmo local, assegurando uma identificação precisa;
- A solução deve permitir a criação de regras específicas para cada perfil de rede configurado. Essas regras podem incluir, mas não se limitam a:
- Ativação ou desativação do firewall;
- Ativação ou desativação do Atualizador de Software;
- Regras específicas de acesso à internet e restrições de aplicativos;
- As regras devem ser aplicadas automaticamente quando o dispositivo é detectado no local de rede correspondente;

A solução deve fornecer uma interface de gestão centralizada que permita aos administradores configurar, visualizar e gerenciar os perfis de rede, locais e regras de segurança;

A interface deve oferecer facilidade de uso, com opções intuitivas para adicionar, modificar e remover locais e regras, bem como monitorar o status e a eficácia das políticas aplicadas;

Coleta de chaves da Criptografia de disco:

- A solução deve incluir ferramentas para o gerenciamento eficaz da criptografia nos dispositivos, permitindo sua ativação, configuração e monitoramento centralizado.
- A solução de proteção de endpoint deve oferecer funcionalidades de criptografia de disco, garantindo a confidencialidade dos dados armazenados nos dispositivos. A criptografia deve ser gerenciável a partir de uma visão geral do estado da criptografia em todos os dispositivos protegidos;
- A solução deve permitir a visualização do status da criptografia de disco ao selecionar um endpoint na console de administração, também deve ser possível observar através de relatórios de dispositivo, proporcionando uma gestão completa e centralizada;
- A solução deve incluir ferramentas para a coleta e gerenciamento de chaves de recuperação. A funcionalidade deve garantir que as chaves de recuperação estejam acessíveis e visíveis em um portal centralizado;
- A solução deve suportar a criptografia de discos utilizando o Bitlocker com o “protetor de senha de recuperação”. Deve ser possível configurar e verificar a

coleta bem-sucedida das chaves de recuperação em um portal de segurança centralizado, garantindo a disponibilidade dessas chaves para procedimentos de recuperação de dados;

Proteção contra Ransomware:

- A solução deve monitorar pastas em busca de alterações potencialmente prejudiciais feitas por ransomware ou outro software prejudicial semelhante;
- A solução deve possibilitar que aplicativos confiáveis possam ter acesso à pasta;
- A solução deve possibilitar que aplicativos desconhecidos pelo fabricante possam ser adicionados a lista de aplicativos confiáveis;
- A solução deve ser capaz de identificar pastas que contém documentos, imagens ou outro conteúdo de usuário final e fazer o monitoramento da mesma;
- A solução deve possibilitar adicionar pastas para serem excluídas do monitoramento, ou seja, não serão verificadas;

Controle de aplicativos:

A solução de deve ser capaz de realizar no mínimo as seguintes ações quando executado uma aplicação:

- Permitir;
- Bloquear;
- Permitir e monitorar;

A solução dever ser capaz de identificar o evento executado pela aplicação, possibilitando assim a capacidade de criar regras de bloqueio ou de acesso, correspondendo com no mínimo os eventos abaixo:

- Execução do aplicativo;
- Carga de modulo;
- Início do instalador;
- Inicialização do aplicativo e carregamento do modulo;
- Acesso a arquivo;
- A solução dever possuir no mínimo os tipos de condições(gatilhos) abaixo para possibilitar a criação de regras de bloqueio ou de acesso:
- Caminho do arquivo;

- SHA1 de identificação;
- SHA256 de identificação;
- Reputação do software;
- Versão do software;
- Nome do software;
- Empresa que fabricou o software;

A solução dever possuir no mínimo os tipos de condicional abaixo para possibilitar a criação de regras de bloqueio ou de acesso:

- Contém;
- Começa com;
- Termina com;
- É igual a;
- Não é igual a;
- É menor que;
- É maior que;
- É menor que ou igual a;
- É maior ou igual a;

Detecção de eventos do sistema

A solução deve ser capaz de centralizar os logs de eventos dos sistemas Windows na console de gerenciamento. É essencial que permita uma análise detalhada dos eventos relacionados a possíveis ataques em máquinas Windows, incluindo, por exemplo: contas bloqueadas, tentativas de alteração de senha, falhas de logon, registros de auditoria apagados, tentativas de instalação de serviço, erros fatais do Windows (BSoD), entre outros eventos relevantes.

III. LEVANTAMENTO DE MERCADO

Com o objetivo de identificar soluções capazes de atender às necessidades da Administração Municipal quanto à infraestrutura de Tecnologia da Informação, foi realizado levantamento de mercado considerando alternativas disponíveis para atendimento da demanda.

A partir da análise realizada, foram identificadas as seguintes possibilidades:

- **Solução 1 – Contratação de empresa especializada para prestação de serviços de TI.**
- **Solução 2 – Aquisição de equipamentos e contratação de equipe própria para suporte técnico.**

Após a identificação das alternativas possíveis para atendimento da demanda da Administração Municipal, procedeu-se à análise comparativa das soluções apresentadas, considerando aspectos técnicos, operacionais e econômicos.

A **Solução 1**, que consiste na contratação de empresa especializada para prestação de serviços de Tecnologia da Informação com locação de equipamentos, apresenta como principais vantagens a disponibilização de infraestrutura tecnológica atualizada, suporte técnico especializado, monitoramento contínuo dos ativos de rede e maior agilidade na solução de incidentes e falhas operacionais. Além disso, esse modelo permite maior previsibilidade de custos, atualização tecnológica periódica e redução da necessidade de investimentos iniciais elevados por parte da Administração.

Outro fator relevante é que a contratação de empresa especializada possibilita o acesso a profissionais com conhecimento técnico específico e experiência na gestão de infraestrutura de TI, incluindo segurança da informação, monitoramento de rede, gerenciamento de servidores e implementação de rotinas de backup e recuperação de dados.

Por outro lado, a **Solução 2**, que consiste na aquisição direta de equipamentos e na manutenção da infraestrutura tecnológica por equipe própria da Administração, exigiria investimentos iniciais mais elevados para aquisição de servidores, equipamentos de rede, softwares e licenças, além da necessidade de constante atualização tecnológica para evitar a obsolescência dos equipamentos.

Essa alternativa também demandaria a disponibilização de equipe técnica especializada para administração, monitoramento e manutenção dos sistemas e equipamentos, o que poderia gerar custos adicionais com capacitação, contratação de profissionais especializados e aquisição de ferramentas de gestão e segurança da informação.

Dessa forma, considerando os aspectos analisados, verifica-se que a **Solução 1 apresenta maior viabilidade técnica e operacional**, permitindo maior eficiência na gestão da infraestrutura tecnológica, atualização contínua dos

equipamentos e suporte técnico especializado, além de proporcionar maior previsibilidade de custos e redução de riscos relacionados à indisponibilidade dos serviços.

Assim, conclui-se que a contratação de empresa especializada para prestação de serviços de Tecnologia da Informação, incluindo locação de equipamentos e suporte técnico especializado, mostra-se como a solução mais adequada para atender às necessidades da Administração Municipal.

IV. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

A presente contratação será realizada por meio de **Pregão Eletrônico**, em conformidade com a Lei nº 14.133/2021, por se tratar de serviço comum de Tecnologia da Informação, cujas especificações podem ser objetivamente definidas no Termo de Referência.

Após a realização do levantamento de mercado e análise das alternativas disponíveis, verificou-se que a solução mais vantajosa para a Administração consiste na contratação de empresa especializada para prestação de serviços de Tecnologia da Informação, contemplando a locação de equipamentos, suporte técnico especializado e gestão da infraestrutura tecnológica do Município.

A solução compreende a locação de equipamentos de firewall, bem como a realização da migração da estrutura tecnológica atualmente existente, além da prestação de suporte técnico especializado, remoto, incluindo monitoramento e serviços de manutenção preventiva e corretiva, sobre os serviços contratados.

Também integra a solução a implementação e gestão de rotinas de backup redundante, com armazenamento local e em nuvem, visando garantir maior segurança, integridade e disponibilidade das informações institucionais, bem como possibilitar a recuperação de dados em situações de falhas ou incidentes de segurança.

Adicionalmente, a contratação contempla a disponibilização do fornecimento de licenças de antivírus para proteção dos computadores e servidores que compõem a rede da Administração Municipal, contribuindo para o fortalecimento da segurança da informação.

Os serviços deverão ser executados com monitoramento contínuo da infraestrutura tecnológica, em regime 24 horas por dia e 7 dias por semana (24x7),

garantindo maior estabilidade, segurança e disponibilidade dos sistemas utilizados pelas unidades administrativas.

A presente solução visa garantir a continuidade das atividades administrativas, o adequado funcionamento dos sistemas utilizados pelas secretarias municipais, a segurança das informações institucionais e a melhoria da eficiência operacional da infraestrutura de Tecnologia da Informação da Administração Municipal.

V. ESTIMATIVA DAS QUANTIDADES DA CONTRATAÇÃO

Dentro do presente estudo, foram analisados os históricos dos quantitativos de prestação de serviços anteriormente contratados por este Órgão. Verificou-se, contudo, que os quantitativos atualmente praticados já não atendem de forma adequada às demandas da Administração, em razão do crescimento da infraestrutura tecnológica, do aumento do número de equipamentos e usuários atendidos, bem como da ampliação dos serviços públicos prestados de forma digital.

Dessa forma, além da análise do histórico contratual, foi considerada a necessidade de adequação dos quantitativos à realidade atual da Administração, bem como a previsão de uma margem prudente para atendimento da expansão dos serviços públicos, o que justifica os quantitativos estimados no presente estudo.

Item	Descrição	Unidade	Quantidade
1	Contratação de empresa especializada na prestação de serviços de tecnologia da informação, incluindo a locação de equipamentos de firewall e serviços de migração da estrutura local e remota. A solução contempla a implementação e gestão de backup redundante, tanto local quanto em nuvem, bem como a contratação de licenças de antivírus para computadores e servidores da rede, incluindo serviços de manutenção, configuração preventiva e corretiva, e monitoramento 24/7 dos serviços contratados.	Mês	12
ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO (MENSAL)			
LOTE UNICO – Locação de Firewall, Serviço de Migração, Serviço de Backup, Licenças de antivírus, Suporte e Monitoramento 24/7 sobre			

os serviços contratados:

ITEM 01 – Contratação De Empresa Especializada Em Tecnologia Da Informação Para Fornecimento, Na Modalidade Locação, De Firewall Corporativo;

ITEM 02 – Contratação De Empresa Especializada Em Tecnologia Da Informação Na Prestação De Serviço De Configuração Inicial E Instalação De Firewall E Migração;

ITEM 03 – Contratação De Empresa Especializada Em Tecnologia Da Informação Na Prestação De Serviço De Suporte Técnico Continuado (N2/N3) E Monitoramento 24/7 sobre os serviços contratados;

ITEM 04 – Contratação De Empresa Especializada Em Tecnologia Da Informação Na Prestação De Serviço Backup Local E Em Nuvem;

ITEM 05 – Contratação De Empresa Especializada Em Tecnologia Da Informação No Fornecimento De Solução De Antivírus – 100 Licenças;

VI. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

O valor estimado para essa contratação não está planejado para o ano de 2026, estimamos o valor da presente aquisição em **R$ 100.000,00 (cem mil reais).** Destacando que se trata somente de valor estimado, sendo que para valor de edital será considerado valores conforme a pesquisa de preço e atendendo a todos os mecanismos legais, fica autorizado a contratação de quantitativo temporário até que a solução mais ampla, efetiva, qualitativa e mais econômica fique estabelecida na forma da Lei.

A presente contratação ainda não está incluída no Plano de Contratações Anual em razão de sua superveniência, contudo, será encaminhada para inclusão, após a autorização da autoridade competente. Vale ressaltar que a contratação se compatibiliza com os demais instrumentos de planejamento.

VII. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

Para a solução em questão, não será adotado o parcelamento do objeto, tendo em vista que os serviços pretendidos são tecnicamente integrados e interdependentes, envolvendo atividades de suporte técnico, gestão da infraestrutura

de Tecnologia da Informação, manutenção de firewall, rede, estações de trabalho, backup, antivírus e monitoramento contínuo do ambiente tecnológico.

A eventual divisão do objeto em múltiplos contratos poderia gerar fragmentação da responsabilidade técnica, dificultando a identificação de falhas, a resolução de incidentes e a adequada gestão da infraestrutura de TI da Administração Municipal. Além disso, a atuação de diferentes fornecedores em um mesmo ambiente tecnológico pode ocasionar conflitos operacionais, incompatibilidades técnicas e dificuldades de coordenação, comprometendo a continuidade e a eficiência dos serviços.

Outro aspecto relevante se refere ao ganho de eficiência operacional e economia de escala, uma vez que a contratação de uma única empresa possibilita a gestão integrada do ambiente tecnológico, melhor planejamento das atividades, padronização de procedimentos e maior agilidade no atendimento das demandas da Administração.

Adicionalmente, a centralização da contratação em um único fornecedor reduz os custos administrativos de gestão contratual, fiscalização e acompanhamento da execução dos serviços, contribuindo para maior controle e eficiência na execução do contrato.

Dessa forma, embora exista, em tese, a possibilidade de divisão do objeto, entende-se que o parcelamento não se mostra técnica e economicamente vantajoso para a Administração, motivo pelo qual a licitação será realizada em lote único, abrangendo todos os serviços previstos neste estudo.

VIII. CONTRATAÇÕES CORRELATAS OU INTERDEPENDENTES

Não foram identificadas contratações correlatas ou interdependentes neste estudo.

IX. DEMONSTRATIVO DA PREVISÃO DA CONTRATAÇÃO NO PLANO ANUAL

A presente contratação ainda não está incluída no Plano de Contratações Anual de 2026 em razão de sua superveniência, contudo, será encaminhada para

inclusão, após a autorização da autoridade competente. Vale ressaltar que a contratação se compatibiliza com os demais instrumentos de planejamento.

X. MAPA DE RISCOS

O mapeamento de riscos tem como objetivo identificar, avaliar e propor medidas de mitigação para eventos que possam comprometer o sucesso da contratação e a adequada execução dos serviços de Tecnologia da Informação, assegurando maior previsibilidade, eficiência e segurança na gestão contratual.

Risco	Descrição	Probabilidade	Impacto	Medidas Mitigadoras
Planejamento inadequado	Definição incompleta ou imprecisa das necessidades da Administração	Média	Alto	Elaboração detalhada do ETP e Termo de Referência, com validação técnica
Falha na migração de dados	Perda ou corrupção de dados durante o processo de migração	Média	Alto	Realização de backup prévio, testes de migração e plano de contingência
Indisponibilidade dos serviços	Interrupção dos sistemas durante implantação ou execução	Média	Alto	Implantação em fases, execução fora do horário crítico e monitoramento contínuo
Baixa qualidade dos serviços prestados	Execução inadequada pela contratada	Baixa	Alto	Exigência de qualificação técnica e acompanhamento por fiscal de contrato
Descumprimento de SLA	Não atendimento aos níveis de serviço estabelecidos	Média	Médio	Definição de SLA em contrato e aplicação de penalidades
Ataques cibernéticos	Ocorrência de novos incidentes de segurança	Média	Alto	Implementação de firewall, antivírus, monitoramento e políticas de segurança
Falta de suporte técnico	Demora ou ausência de atendimento a chamados	Média	Médio	Exigência de suporte 24x7 e canais de atendimento definidos

Risco	Descrição	Probabilidade	Impacto	Medidas Mitigadoras
Dependência excessiva da contratada	Dificuldade de continuidade em caso de rescisão contratual	Baixa	Médio	Documentação dos serviços e transferência de conhecimento
Problemas na integração com ambiente existente	Incompatibilidade com sistemas e equipamentos atuais	Média	Médio	Levantamento prévio da infraestrutura e testes de compatibilidade

Dessa forma, verifica-se que os riscos identificados são administráveis e podem ser mitigados mediante planejamento adequado, definição clara das obrigações contratuais e acompanhamento efetivo da execução, não representando impedimento à realização da contratação pretendida.

XI. DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS

A contratação pretendida tem como objetivo garantir a continuidade, estabilidade e segurança da infraestrutura de Tecnologia da Informação da Administração Municipal, assegurando o adequado funcionamento dos sistemas utilizados na execução das atividades administrativas e na prestação de serviços públicos à população.

Com a implementação da solução proposta, pretende-se alcançar os seguintes resultados:

- Garantir alta disponibilidade dos sistemas e serviços de TI, reduzindo riscos de interrupções nas atividades administrativas;
- Assegurar maior segurança da informação, por meio da utilização de firewall, antivírus, controle de acesso, monitoramento da rede e políticas de proteção de dados;
- Promover a modernização da infraestrutura tecnológica, substituindo equipamentos e soluções defasadas por tecnologias mais atuais e eficientes;
- Implementar rotinas de backup confiáveis, com armazenamento local e em nuvem, garantindo maior proteção contra perda de dados;
- Disponibilizar suporte técnico especializado, local e remoto, para atendimento ágil das demandas das secretarias e unidades administrativas;

- Melhorar o desempenho da rede e dos servidores, contribuindo para maior eficiência no uso dos sistemas institucionais;
- Garantir a padronização e organização do ambiente de TI, facilitando a gestão da infraestrutura tecnológica;
- Ampliar a capacidade de atendimento às demandas atuais e futuras da Administração, considerando a expansão dos serviços públicos digitais.

Dessa forma, espera-se que a contratação contribua para maior eficiência administrativa, segurança da informação, continuidade dos serviços públicos e melhor desempenho da infraestrutura tecnológica, proporcionando condições adequadas para o funcionamento dos sistemas e ferramentas utilizados pela Administração Municipal.

XII. PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO

Para viabilizar a adequada execução do objeto e garantir a efetividade da contratação, a Administração deverá adotar previamente e durante a execução contratual as seguintes providências:

- Inicialmente, deverá ser designado servidor responsável pela gestão e fiscalização do contrato, nos termos da Lei nº 14.133/2021, com a atribuição de acompanhar, monitorar e atestar a execução dos serviços contratados.
- Deverá ser disponibilizado acesso às dependências, sistemas, equipamentos e informações necessárias para a correta execução dos serviços, observadas as normas de segurança da informação e proteção de dados.
- A Administração deverá promover o levantamento e a organização das informações relativas à infraestrutura atual de tecnologia da informação, incluindo inventário de equipamentos, rede, servidores e sistemas utilizados, a fim de subsidiar o processo de migração e implantação da nova solução.
- Também será necessário o alinhamento prévio com a empresa contratada quanto ao cronograma de implantação, especialmente no que se refere à migração de dados e configuração dos sistemas, visando minimizar impactos nas atividades administrativas.

- Durante a execução contratual, a Administração deverá acompanhar os níveis de serviço prestados, analisando relatórios periódicos de desempenho, disponibilidade e incidentes, garantindo o cumprimento das obrigações contratuais.
- Por fim, deverá ser promovida a capacitação básica dos servidores responsáveis pela área de tecnologia da informação, visando assegurar a correta utilização das ferramentas implementadas e a adequada interação com a empresa contratada.

XIII. DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS

A presente contratação, por se tratar de serviços de Tecnologia da Informação com fornecimento de equipamentos em regime de locação, não apresenta impactos ambientais significativos diretos. No entanto, podem ser observados impactos indiretos relacionados ao consumo de energia elétrica, geração de resíduos eletrônicos e uso de recursos tecnológicos.

A utilização de equipamentos como firewall, servidores e dispositivos de armazenamento implica aumento no consumo energético, ainda que em escala moderada, devendo a contratada priorizar o fornecimento de equipamentos com maior eficiência energética e menor impacto ambiental.

Quanto aos resíduos, destaca-se a possibilidade de geração de lixo eletrônico ao final da vida útil dos equipamentos utilizados. Nesse sentido, a responsabilidade pela destinação final ambientalmente adequada dos equipamentos deverá ser da contratada, observando a legislação vigente, especialmente no que se refere à logística reversa e ao descarte correto de resíduos tecnológicos.

A adoção de soluções em nuvem e backup remoto contribui para a redução da necessidade de infraestrutura física local, podendo resultar em menor consumo de recursos e otimização do uso de energia.

Adicionalmente, recomenda-se que a contratada observe boas práticas de sustentabilidade, tais como o uso de equipamentos certificados, redução de consumo energético, e destinação adequada de materiais, contribuindo para a minimização de impactos ambientais.

Dessa forma, conclui-se que os impactos ambientais decorrentes da contratação são de baixa relevância, podendo ser mitigados mediante a adoção de práticas sustentáveis e o cumprimento da legislação ambiental aplicável.

XIV. POSICIONAMENTO CONCLUSIVO

Com base nos estudos realizados no presente Estudo Técnico Preliminar, conclui-se que a contratação de empresa especializada para a prestação de serviços de Tecnologia da Informação, contemplando a locação de equipamentos, suporte técnico, monitoramento contínuo, solução de backup e fornecimento de antivírus, mostra-se técnica e economicamente viável, além de necessária para atender às demandas da Administração Municipal.

A solução proposta apresenta-se como a mais adequada sob os aspectos de eficiência, segurança, continuidade dos serviços e racionalização de recursos públicos, considerando as fragilidades identificadas na infraestrutura atual, bem como os riscos associados à indisponibilidade dos sistemas e à segurança da informação.

Destaca-se que a contratação permitirá a modernização do ambiente tecnológico, a mitigação de riscos operacionais e cibernéticos, a melhoria no desempenho dos sistemas e a garantia da integridade, confidencialidade e disponibilidade das informações institucionais.

Dessa forma, manifesta-se favoravelmente à continuidade do processo, recomendando-se a realização de procedimento licitatório na modalidade Pregão Eletrônico, visando à contratação da solução ora definida, em conformidade com a Lei nº 14.133/2021.

Diante do exposto, declara-se viável a contratação pretendida com base neste Estudo Técnico Preliminar.

Rebouças, 07 de abril de 2026.

_____

Nara Cassiane Paluch
Secretária de Administração

_____	_____
Alesson José Fassini	**Edina Cristina Faganeli**
Setor de Compras	Departamento de Licitação

Assinado por: Alesson Fassini - 09451621970 10/04/2026 15:41:46 DOCUMENTO ASSINADO ELETRONICAMENTE - DECRETO MUNICIPAL 110/2023

Assinado por: Édina Faganeli - 06751947925 10/04/2026 16:08:13 DOCUMENTO ASSINADO ELETRONICAMENTE - DECRETO MUNICIPAL 110/2023

Assinado por: NARA CASSIANE CELEZINSKY PALUCH - 04747252940 10/04/2026 16:29:25 DOCUMENTO ASSINADO ELETRONICAMENTE - DECRETO MUNICIPAL 110/2023