Fone: 08000 112 190
CNPJ: 45.743.580/0001-45
SAAE - Saneamento Ambiental de Atibaia
Praça Roberto Gomes Pedrosa, 11
Atibaia - São Paulo

AVISO DE DISPENSA ELETRÔNICA Nº 49/2024

Processo Administrativo nº 12.297/2024

A **SAAE – Saneamento Ambiental de Atibaia** torna público que através de sua Ordenadora de Despesas, Sra. Fabiane Cabral da Costa Santiago, Superintendente desta Autarquia, ora denominada **AUTORIDADE COMPETENTE**, na forma do disposto no Decreto Municipal n.º 10.212/2022, realizará Dispensa Eletrônica com critério de julgamento menor preço, nos termos do artigo nº 75 da Lei Federal nº 14.133/2021, da Instrução Normativa SEGES/ME nº 67/2021 e demais legislação aplicável.

Data da sessão: 08/04/2024 a 11/04/2024
Link: www.portaldecompraspublicas.com.br
Horário da Fase de Lances: Início às 8h e encerramento às 14h

1. OBJETO DA CONTRATAÇÃO DIRETA

1.1 O objeto da presente dispensa é a escolha da proposta mais vantajosa para a contratação por dispensa de licitação de **ASSINATURA DE LICENÇA DO SOFTWARE ANTIVIRUS ESET PROTECT ENTRY CLOUD PELO PERÍODO DE 12 MESES** conforme condições, quantidades e exigências estabelecidas neste Aviso de Contratação Direta e seus anexos.

1.2 O critério de julgamento adotado será o **MENOR PREÇO**, observadas as exigências contidas neste Aviso de Contratação Direta e seus Anexos quanto às especificações do objeto.

Fone: 08000 112 190
CNPJ: 45.743.580/0001-45
SAAE - Saneamento Ambiental de Atibaia
Praça Roberto Gomes Pedrosa, 11
Atibaia - São Paulo

2. DA PARTICIPAÇÃO NA DISPENSA ELETRÔNICA

2.1 A participação na presente dispensa eletrônica se dará mediante Sistema de Dispensa Eletrônica integrante do Portal de Compras Públicas, disponível no endereço eletrônico www.portaldecompraspublicas.com.br.

2.2 Os fornecedores deverão se cadastrar previamente no Portal de Compras Públicas para acesso ao sistema e operacionalização.

2.3 As contratações poderão ser realizadas por meio de sistema eletrônico fornecido por pessoa jurídica de direito privado, devendo o custo de operacionalização e uso do sistema ficar a cargo do licitante.

2.4 O fornecedor é o responsável por qualquer transação efetuada diretamente ou por seu representante no Sistema de Dispensa Eletrônica, não cabendo ao provedor do Sistema ou ao órgão entidade promotor do procedimento, a responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros não autorizados.

2.5 Não poderão participar, direta ou indiretamente, da licitação ou da execução do contrato, as pessoas físicas ou jurídicas enquadradas no art. 9º, §1º e §2º e no art. 14, ambos da Lei n.º 14.133/2021.

2.6 Será realizada consulta Consolidada de Pessoa Jurídica (TCU) https://certidoes-apf.apps.tcu.gov.br/ , a qual já inclui licitantes inidôneos – TCU; CNJ (condenações cíveis por atos de improbidade administrativa); Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e Cadastro Nacional de Empresas Punidas – CNEP;

2.6.1 Consulta ao TCE/SP – Relação de Apenados.

3. DO INGRESSO NA DISPENSA ELETRÔNICA E CADASTRAMENTO DA PROPOSTA INICIAL

3.1 O ingresso do fornecedor na disputa da dispensa eletrônica se dará com o cadastramento de sua proposta inicial, na forma deste item.

3.2 O fornecedor interessado, após a divulgação do aviso de contratação direta,

encaminhará, exclusivamente por meio do Sistema de Dispensa Eletrônica, a proposta com a descrição do objeto ofertado, a marca do produto, quando for o caso, e o preço, até a data e o horário estabelecidos para abertura do procedimento.

3.2.1 A proposta também deverá conter declaração de que compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigente na data de entrega das propostas.

3.3 Todas as especificações do objeto contidas na proposta, em especial o preço, vinculam a Contratada.

3.4 Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação dos serviços.

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

3.5 Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

3.6 Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

3.7 A apresentação das propostas implica obrigatoriedade no cumprimento das disposições nelas contidas, em conformidade com o que dispõe este termo, assumindo o proponente o compromisso de executar os serviços nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

3.8 Uma vez enviada a proposta no sistema, os fornecedores NÃO poderão retirar, substituír ou modificá-la;

3.9 No cadastramento da proposta inicial, o fornecedor deverá, também, assinalar

"sim" ou "não" em campo próprio do sistema eletrônico, às seguintes declarações:

3.9.1 que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

3.9.2 que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar Federal nº 123/2026, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49;

3.9.3 que está ciente e concorda com as condições contidas no Aviso de Contratação Direta e seus anexos;

3.9.4 que assume a responsabilidade pelas transações que forem efetuadas no sistema, assumindo como firmes e verdadeiras;

3.9.5 que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, de que trata o art. 93 da Lei Federal nº 8.213/1991.

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

4. DA FASE DE LANCES

4.1 A partir das **08:00** horas da data estabelecida neste Aviso de Contratação Direta, a sessão pública será automaticamente aberta pelo sistema para o envio de lances públicos e sucessivos, exclusivamente por meio do sistema eletrônico, sendo encerrado no horário de finalização de lances também já previsto neste aviso.

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

4.2.1 O lance deverá ser ofertado pelo valor (unitário do item/total/anual).

4.3 O fornecedor somente poderá oferecer valor inferior em relação ao último lance por ele ofertado e registrado pelo sistema.

4.3.1 O fornecedor poderá oferecer lances sucessivos iguais ou superiores ao lance

que esteja vencendo o certame, desde que inferiores ao menor por ele ofertado e registrado pelo sistema, sendo tais lances definidos como “lances intermediários” para os fins deste Aviso de Contratação Direta.

4.4 Havendo lances iguais ao menor já ofertado prevalecerá aquele que for recebido e registrado primeiro no sistema.

4.5 Caso o fornecedor não apresente lances, concorrerá com o valor de sua proposta.

4.6 Durante o procedimento, os fornecedores serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do fornecedor.

4.7 Imediatamente após o término do prazo estabelecido para a fase de lances, haverá o seu encerramento, com o ordenamento e divulgação dos lances, pelo sistema, em ordem crescente de classificação.

4.7.1 O encerramento da fase de lances ocorrerá de forma automática pontualmente no horário indicado, sem qualquer possibilidade de prorrogação e não havendo tempo aleatório ou mecanismo similar.

5. DO JULGAMENTO DAS PROPOSTAS DE PREÇO

5.1 Encerrada a fase de lances, será verificada a conformidade da proposta classificada em primeiro lugar quanto à adequação do objeto e à compatibilidade do preço em relação ao estipulado para a contratação.

5.2 No caso de o preço da proposta vencedora estar acima do estimado pela Administração, poderá haver a negociação de condições mais vantajosas.

5.2.1 Neste caso, será encaminhada contraproposta ao fornecedor que tenha apresentado o melhor preço, para que seja obtida melhor proposta com preço compatível ao estimado pela Administração.

5.2.2 A negociação poderá ser feita com os demais fornecedores classificados, respeitada a ordem de classificação, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido para a contratação.

5.2.3 Em qualquer caso, concluída a negociação, o resultado será registrado na ata do procedimento da dispensa eletrônica.

5.3 Estando o preço compatível, será solicitado o envio da proposta adequada ao último lance e, se necessário, de documentos complementares.

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

5.5 Será desclassificada a proposta vencedora que:

5.5.1 contiver vícios insanáveis;

5.5.2 não obedecer às especificações técnicas pormenorizadas neste aviso ou em seus anexos;

5.5.3 apresentar preços manifestamente inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

5.5.4 não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

5.5.5 apresentar desconformidade com quaisquer outras exigências deste aviso ou seus anexos, desde que insanável.

5.6 Quando o fornecedor não conseguir comprovar que possui ou possuirá recursos suficientes para executar a contento o objeto, será considerada inexequível a proposta de preços ou menor lance que:

5.6.1 for insuficiente para a cobertura dos custos da contratação, apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da dispensa não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio fornecedor, para os quais ele renuncie a parcela ou à totalidade da remuneração.

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

5.8 Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço.

5.8.1 O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas.

5.8.2 Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

5.9 Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.

5.10 Se a proposta ou lance vencedor for desclassificado, será examinada a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

5.11 Havendo necessidade, a sessão será suspensa, informando-se no “chat” a nova data e horário para a sua continuidade.

5.12 Encerrada a análise quanto à aceitação da proposta, se iniciará a fase de habilitação, observado o disposto neste Aviso de Contratação Direta.

6. DA HABILITAÇÃO

6.1 Os documentos a serem exigidos para fins de habilitação constam do **ANEXO II – DOCUMENTAÇÃO EXIGIDA PARA HABILITAÇÃO** deste aviso e serão solicitados do fornecedor mais bem classificado da fase de lances.

6.1.1 Os documentos de habilitação e a proposta readequada deverão ser encaminhados dentro do prazo máximo de 2 (duas) horas a partir da solicitação pelo agente de contratação/pregoeiro, sob pena de desclassificação.

6.2 Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Aviso de Contratação Direta e já apresentados, o fornecedor será convocado a encaminhá-los, em formato digital, após solicitação da Administração, sob pena de inabilitação.

6.3 Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital.

Fone: 08000 112 190
CNPJ: 45.743.580/0001-45
SAAE - Saneamento Ambiental de Atibaia
Praça Roberto Gomes Pedrosa, 11
Atibaia - São Paulo

6.4 O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar Federal nº 123/2006, estará dispensado (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal.

6.5 Havendo necessidade, a sessão será suspensa, para análise minuciosa dos documentos exigidos sendo informada a nova data e horário para a sua continuidade.

6.6 Será inabilitado o fornecedor que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Aviso de Contratação Direta.

6.6.1 Na hipótese de o fornecedor não atender às exigências para a habilitação, o órgão ou entidade examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda às especificações do objeto e as condições de habilitação.

6.7 Constatado o atendimento às exigências de habilitação, o fornecedor será habilitado e o processo será encaminhado à autoridade superior para homologação e adjudicação.

7. DA CONTRATAÇÃO

7.1 Após a homologação e adjudicação, caso se conclua pela contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.

7.2 O adjudicatário terá o prazo de 03 (três) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato ou aceitar instrumento equivalente, conforme o caso (Nota de Empenho/Pedido), sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Aviso de Contratação Direta.

7.2.1 O prazo previsto para assinatura do contrato ou aceitação da nota de empenho ou instrumento equivalente poderá ser prorrogado 1 (uma) vez, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

7.3 O Aceite da Nota de Empenho ou do instrumento equivalente, emitida à empresa adjudicada, implica no reconhecimento de que:

7.3.1 referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei Federal nº 14.133/2021;

7.3.2 a contratada se vincula à sua proposta e às previsões contidas no Aviso de Contratação Direta e seus anexos;

7.3.3 a contratada reconhece que as hipóteses de rescisão são aquelas previstas no artigo 137 da Lei Federal nº 14.133/2021 e reconhece os direitos da Administração previstos nos artigos 138 a 139 da mesma Lei.

8. DAS SANÇÕES

8.1 Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa, incorrer nas condutas elencadas no **Anexo III – Das Sanções**.

8.2 Com fulcro na Lei Federal nº 14.133/2021, a SAAE poderá garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

8.2.1 advertência;

8.2.2 multa;

8.2.3 impedimento de licitar e contratar e

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

8.3 Na aplicação das sanções serão considerados os elementos previstos no art. 156, § 1º, da Lei Federal 14.133/2021.

8.4 As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade, bem como a sanção de multa respeitarão o devido processo legal e obedecerão os prazos de defesa previstos na Lei Federal 14.133/2021.

8.5 Se o adjudicatário não celebrar o contrato ou a ata de registro de preço ou não entregar a documentação exigida para a contratação, no prazo estabelecido pela SAAE, restará caracterizado o descumprimento total da obrigação assumida e o

sujeitará às penalidades cabíveis e à imediata perda da garantia de proposta em favor da SAAE.

9. DAS DISPOSIÇÕES GERAIS

9.1 O procedimento será divulgado no Portal de Compras Públicas e no Portal Nacional de Contratações Públicas - PNCP, e encaminhado automaticamente aos fornecedores registrados no aviso de licitações do Portal de Compras Públicas, por mensagem eletrônica, na correspondente linha de fornecimento que pretende atender.

9.2 No caso de todos os fornecedores restarem desclassificados ou inabilitados (procedimento fracassado), a Administração poderá:

9.2.1 republicar o presente aviso com uma nova data;

9.2.2 valer-se, para a contratação, de proposta obtida na pesquisa de preços que serviu de base ao procedimento, se houver, privilegiando-se os menores preços, sempre que possível, e desde que atendidas às condições de habilitação exigidas.

9.2.2.1 No caso do subitem anterior, a contratação será operacionalizada fora deste procedimento.

9.2.3 fixar prazo para que possa haver adequação das propostas ou da documentação de habilitação, conforme o caso.

9.3 As providências dos subitens 9.2.1 e 9.2.2 acima poderão ser utilizadas se não houver o comparecimento de quaisquer fornecedores interessados (procedimento deserto).

9.4 Havendo a necessidade de realização de ato de qualquer natureza pelos fornecedores, cujo prazo não conste deste Aviso de Contratação Direta, deverá ser atendido o prazo indicado pelo agente competente da Administração na respectiva notificação.

9.5 Caberá ao fornecedor acompanhar as operações, ficando responsável pelo ônus decorrente da perda do negócio diante da inobservância de quaisquer mensagens emitidas pela Administração ou de sua desconexão.

9.6 Não havendo expediente ou ocorrendo qualquer fato superveniente que

impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário.

9.7 Os horários estabelecidos na divulgação deste procedimento e durante o envio de lances observarão o horário de Brasília-DF, inclusive para contagem de tempo e registro no Sistema e na documentação relativa ao procedimento.

9.8 No julgamento das propostas e da habilitação, a Administração poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

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

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

9.11 Em caso de divergência entre disposições deste Aviso de Contratação Direta e de seus anexos ou demais peças que compõem o processo prevalecerá as deste Aviso.

9.12 Os casos omissos neste Edital, serão resolvidos pelo(s) subscritor(es) do Edital, nos termos da legislação pertinente.

9.13 O foro designado para julgamento de quaisquer questões judiciais resultantes deste Edital será o da Comarca de Atibaia / SP.

9.14 Da sessão pública será divulgada em Ata no sistema eletrônico.

9.15 Integram este Aviso de Contratação Direta, para todos os fins e efeitos, os seguintes anexos:

ANEXO I – Termo de Referência;

ANEXO II – Documentação exigida para Habilitação

ANEXO III – Sanções.

saae
saneamento ambiental
ATIBAIA

Fone: (11) 4414-3500
CNPJ: 45.743.580/0001-45
SAAE - Saneamento Ambiental de Atibaia
Praça Roberto Gomes Pedrosa, 11
Atibaia - São Paulo

TERMO DE REFERÊNCIA

SAAE – AUTARQUIA MUNICIPAL DE SANEAMENTO AMBIENTAL DE ATIBAIA

Memorando n° 12.297/2024
Área Solicitante: **Setor de Tecnologia da Informação.**
Referente à Aquisição de **Software anti-virus (renovação)**

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Aquisição de 120 licenças do software ESET corporativo, incluindo atualizações, garantia e suporte técnico pelo periodo de 12 (doze) meses, para continuar cobrindo com a presente solução a demanda de segurança da informação desta autarquia, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

ITEM	ESPECIFICAÇÃO	UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Assinatura de licença do ESET Protect Entry Cloud pelo período de 12 meses	Un	120	49,90	R$5988,00

1.2. Os bens objeto desta contratação são caracterizados como comuns, ou seja, possui padrões de desempenho e qualidade que podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado, conforme art. 29 da Lei 14.133/2023.

1.3. O prazo de vigência da contratação será de 1 (um) ano e poderá ser prorrogado, por igual período, nos termos do art. 84 da Lei n° 14.133, de 2021.

Modelo Aprovado pela Diretoria de Administração da SAAE Atibaia
Referência: setembro/23.
(Com base no modelo da Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União Atualização: maio/2023 – Termo de Referência Aquisições – Licitação - Modelo para Pregão Eletrônico)

1.4. Demais detalhamentos das regras que serão aplicadas em relação à vigência da contratação poderão ser estabelecidos em contrato aprovado pela administração.

1.5. Demais detalhamentos podem ser estabelecidos pela área solicitante, caso não haja maiores detalhes retirar esta cláusula.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

A Contratação se faz necessária pela necessidade de garantir a continuidade de proteção e segurança do ambiente de informática da SAAE, principalmente considerando a existência e o aumento contínuo de softwares maliciosos de softwares maliciosos como vírus, trojan entre outros malwares. Uma solução corporativa de antivírus torna-se imprescindível para o bom funcionamento dos computadores e servidores da SAAE. Este tipo de software é capaz de prevenir infecções e também detectar, capturar e eliminar malwares. Torna-se assim indispensável para a segurança de dados e continuidade das atividades desempenhadas pelos setores da SAAE Atibaia.A licença da atual solução adotada pela SAAE, a ESET Protect expira no mês de abril/2024, sendo necessária a presente aquisição para manter o parque da SAAE com a devida proteção atualizada.

2.1. O objeto da contratação não está previsto no Plano de Contratações previsto no art. 12, § 1º da Lei 14.133/2021 e não foi disponibilizado no PNCP – Portal Nacional de Contratações Públicas, consoante estabelecido no art. 174, § 2º, I da mesma lei, pois, com a prorrogação da vigência da lei em epígrafe, a Administração ainda está em fase de elaboração do mesmo.

.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

Fone: (11) 4414-3500
CNPJ: 45.743.580/0001-45
SAAE - Saneamento Ambiental de Atibaia
Praça Roberto Gomes Pedrosa, 11
Atibaia - São Paulo

3.1. A Solução atual compreende a aquisição das licenças nas respectivas quantidades já listadas e também como parte integrante do produto o fornecimento de uma console de gerenciamento da solução em nuvem própria da fabricante. As licenças também compreendem o uso tanto para as estações (Endpoint) bem como para os servidores (Server).

A console de gerenciamento centralizada da solução deve possuir as seguintes funcionalidades:

1. O software deve dispor de gerenciamento com administração centralizada, com facilidades para instalação, administração, monitoramento, atualização e configuração, com todos os módulos de um único fornecedor.
2. O acesso ao Console de Gerenciamento deve ser possível via tecnologia Web segura (HTTPS) compatível, no mínimo, com os navegadores Google Chrome, Mozilla Firefox, Microsoft Edge, Opera e Safari.
3. O acesso ao Console deve suportar várias sessões simultâneas.
4. Mecanismo de comunicação (via push) em tempo real entre servidor e clientes, para entrega de configurações e assinaturas.
5. Permitir o agrupamento dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio.
6. O servidor de gerenciamento deve possuir compatibilidade para instalação nos seguintes sistemas operacionais em todas as versões/distribuições/releases e Hypervisors: Microsoft Windows (10,11,Server 2012,2016,2019,2022), Linux (Ubuntu,18,20 Desktop/Server,CentOs 7, Debian 10, Vmware Exsi 6.5 e posterior, MS Hyper-V Server 2012,2016,2019,2022)
7. O servidor de gerenciamento deve possuir compatibilidade para instalação em sistemas operacional de 64-bits tanto em ambiente virtual quanto físico, disponibilizado pela CONTRATANTE.

8. A console de gerenciamento deve oferecer também, opção para gerenciamento em nuvem, disponibilizado pela CONTRATADA.
9. Possuir integração com LDAP e Active Directory, para importação da estrutura organizacional e autenticação dos Administradores.
10. Possibilidade de criar grupos separando as regras aplicadas a cada dispositivo.
11. Possibilidade de instalação dos clientes em estações de trabalho e servidores podendo estes ser físicos ou virtualizados, via console de gerenciamento, de forma remota, sem intervenção do usuário (modo silencioso)
12. Descobrir automaticamente as estações da rede que não possuem o cliente instalado através de funcionalidade integrada ao console de gerenciamento.
13. Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado com opção de instalação remota.
14. A console de gerenciamento deve apresentar funcionalidade que impeça o usuário de alterar as configurações do cliente gerenciado de modo que não se possa alterar, importar e exportar configurações, abrir a console do cliente, desinstalar ou parar o serviço do cliente.
15. Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação (minimamente os níveis de operador e administrador).
16. A solução deve possuir sistema RBAC (Role Based Access Control) para definir acessos customizados de usuários adicionais no console, oferecendo granularidade para configuração dos acessos, para segregar os acessos, limitando os acessos a não exclusivamente políticas, tarefas, e demais objetos do console.
17. O log deve ser centralizado e conter, no mínimo, os seguintes itens: a) Nome da ameaça; b) Nome do arquivo infectado; c) Caminho da detecção; d) HASH do arquivo; e) Data e hora da infecção; f) Ação tomada; g) Endereço de IP da máquina; h) Usuário autenticado na máquina; PARCEIROS i) Origem da ameaça (IP ou hostname da máquina) caso a ameaça tenha se propagado;

18. Fornecer, em tempo real, o status atualizado das estações de trabalho, com pelo menos as seguintes informações: a) Nome da máquina; b) Endereço IP da máquina; c) Malwares não removidos; d) Status da conexão; e) Data da vacina; f) Versão do antivírus instalado.

19. O console de gerenciamento deve prover alertas de segurança via E-mail, com informações de infecção de máquinas e ataques. Suportando no mínimo alertas dos seguintes módulos: a) Detecções de Malware; b) Detecções de Firewall; c) Detecções via EDR;

20. Utilizar o protocolo HTTPS ou outro protocolo seguro para comunicação entre console de gerenciamento e o cliente gerenciado.

21. Capacidade de voltar (rollback) para versão de atualização (da solução ou vacina) através de procedimento específico no console de gerenciamento.

22. Interface da Console de Gerenciamento totalmente em português.

23. Deve permitir criar o backup da Base de dados da Console de gerenciamento.

24. O acesso a console de gerenciamento deverá ser autenticado.

25. A console deverá funcionar também através de um Appliance Virtual fornecido pelo fabricante.

26. O acesso ao console de administração do antivírus deve permitir a possibilidade de ser feito com duplo fator de autenticação integrado dentro da mesma console onde é possível ativá-lo sem a necessidade de nenhum add-on adicional.

27. Gerar pacotes de instalação dos clientes, para cada tipo de sistema operacional existente na estrutura da CONTRATANTE, possibilitando a gravação em mídia e a instalação do software em ambientes onde não seja possível a instalação via rede corporativa.

28. Permitir forçar a instalação do software cliente do antivírus nos computadores, reinstalando-o em caso de desinstalação ou corrupção do mesmo.

29. Atualização de vacinas sem a necessidade de reinicialização.

30. Suportar o gerenciamento de todos os clientes instalados nas máquinas (estações de trabalho, servidores, tablets e smartphones) a partir do servidor de Console de Gerenciamento, oferecendo a possibilidade de configuração centralizada e remota de todas as funcionalidades.

31. Gerenciar de forma remota as configurações do firewall local de cada máquina com o cliente instalado.

32. A solução deve oferecer recurso para isolar as máquinas da rede, mantendo apenas comunicação segura com o servidor de gerenciamento.

33. Criação de grupos e subgrupos de máquinas baseada na hierarquia do Active Directory e LDAP ou em identificador único de clientes, tal como endereço IP;

34. Forçar a configuração determinada no servidor para os clientes, protegendo o software cliente de alterações pelos usuários, com senha pré-determinada na console de gerenciamento.

35. Atualização/sincronização de configurações nos clientes sem a necessidade de reinicialização ou logoff.

36. Permitir a criação de tarefas de rastreamento em períodos de tempo pré-determinados e na inicialização do sistema operacional.

37. Permitir a criação de tarefas de atualização de vacinas e novas versões de software em períodos de tempo pré-determinados.

38. Permitir o uso de ferramentas para centralizar a distribuição de atualizações de software e atualizações dos módulos, não será aceito o uso de ferramentas de terceiros;

39. Permitir criação das tarefas para uma máquina, um grupo de máquinas e/ou para todas as máquinas.

40. Possuir no mínimo 40 modelos de relatórios pré-configurados com filtros e conjuntos de filtros na console de gerenciamento.

Fone: (11) 4414-3500
CNPJ: 45.743.580/0001-45
SAAE - Saneamento Ambiental de Atibaia
Praça Roberto Gomes Pedrosa, 11
Atibaia - São Paulo

41. No console de gerenciamento em nuvem, a solução deve permitir a criação de relatórios customizados. Não serão aceitos apenas os relatórios pré-configurados da solução.

42. Geração de relatórios, permitindo a customização dos mesmos e a exportação para os seguintes formatos (no mínimo um deles): a) CSV; b) PDF;

43. Geração de relatórios que contenham as seguintes informações: a) Máquinas com a lista de definições de vírus desatualizada, ou todas as máquinas e suas respectivas versões da lista de definições de vírus; b) Versão do software instalado em cada máquina; c) Vírus que mais foram detectados; d) Máquinas que mais sofreram infecções em um determinado período de tempo;

44. Permitir o armazenamento em um banco de dados centralizado das informações coletadas nos clientes: PARCEIROS a) Registro de eventos (log); b) Relatórios de eventos de vírus e status dos clientes; c) Relatórios de Softwares instalados; d) Relatórios de Hardware encontrados;

45. Deve ter a capacidade de enviar eventos para um servidor SIEM, suportando no mínimo os seguintes formatos: a) JSON; b) LEEF; c) CEF;

46. Fornecer, em tempo real, o status atualizado das estações de trabalho;

47. Possibilitar a exportação, em formato PDF e CSV, de relatórios que atuem com inventário de hardware e software de todas as estações e servidores ativos na estrutura da console de gerenciamento.

48. Permitir a instalação remota do agente e produto de segurança através de GPO ou SCCM.

49. Possuir módulo de gerenciamento de dispositivos móveis Android e iOS.

50. Por meio do console de gerenciamento deve ser possível gerenciar dispositivos móveis iOS e Android e ter um banco de dados separado do restante dos servidores e estações de trabalho.

51. O módulo de gerenciamento de dispositivos móveis deverá possuir arquitetura padrão de soluções MDM (Mobile Device Management) do mercado.

52. A solução deverá disponibilizar o gerenciamento de dispositivos móveis também através do console em nuvem.

53. O gerenciamento em dispositivos IOS deverá requerer certificado do serviço de notificação por push da Apple, a fim de possibilitar uma comunicação segura entre o servidor e o device.

54. Possibilitar a instalação da solução de segurança aos dispositivos móveis de maneira manual através de QRcode, link gerado pela solução de gerenciamento e e-mail

55. Através da console de gerenciamento a solução deve possibilitar a ativação da opção de bloqueio de exploit por meio do módulo de firewall nas estações e servidores.

56. Atualização incremental e on-line das vacinas.

57. Atualização em clientes móveis (notebook, laptop, netbook, ultrabook e similares) a partir do site do fabricante do antimalware ou de outra fonte definida pelo administrador.

58. Capacidade de configurar políticas móveis para quando um computador estiver fora da estrutura de proteção, possa atualizar-se via internet.

59. Possibilidade de criação de planos de distribuição das atualizações via comunicação segura entre clientes e servidor de gerenciamento e Site do Fabricante.

60. Possibilidade de eleição de qualquer cliente gerenciado como um servidor de distribuição das atualizações, podendo eleger mais de um cliente para esta função.

61. Nas atualizações das configurações e das definições de malwares não se poderá fazer uso de logon scripts, agendamentos ou tarefas manuais ou módulos adicionais que não sejam parte integrante da solução.

62. Qualquer atualização de vacinas deve ser possível sem a necessidade de reinicialização do computador ou serviço para aplicá-la.

63. Atualização automática das assinaturas dos servidores de gerenciamento e clientes via Internet, com periodicidade mínima diária.

64. O sistema deve fornecer um único e mesmo arquivo de vacina de malwares para todas as versões do Windows e do antimalware, sendo aceitável arquivos diferentes, para plataformas 32-bits e 64-bits.

Solução de Antivírus para estações e servidores deve possuir as seguintes funcionalidades

1. A solução ofertada deve suportar sistemas operacionais com arquitetura 32-bits e 64-bits.
2. Gerenciado através de Console de Gerenciamento.
3. Interface do software cliente em português.
4. Manuais em português.
5. O cliente para instalação em estações de trabalho e servidores deverá possuir compatibilidade para instalação com os seguintes sistemas operacionais, minimamente, nas seguintes versões: a) Microsoft Windows 10; b) Microsoft Windows 11; c) Microsoft Windows Server 2012; d) Microsoft Windows Server 2012 R2; e) Microsoft Windows Server 2016 (Server Core e Desktop Experience); f) Microsoft Windows Server 2019 (Server Core e Desktop Experience); g) Microsoft Windows Server 2022 (Server Core e Desktop Experience); h) Ubuntu Desktop 18.04 LTS 64 bits; i) Ubuntu Desktop 20.04 LTS; j) Ubuntu Desktop 22.04 LTS; k) Red Hat Enterprise Linux 7; l) Red Hat Enterprise Linux 8; m) Red Hat Enterprise Linux 9; n) Linux Mint 20; o) Linux Mint 21; p) CentOS 7; PARCEIROS q) Ubuntu Server 18.04 LTS; r) Ubuntu Server 20.04 LTS; s) Ubuntu Server 22.04 LTS; t) Debian 10; u) Debian 11; v) Debian 12; w) Alma Linux 8; x) Alma Linux 9; y) Rocky Linux 8; z) Rocky Linux 9; aa) SUSE Linux Enterprise Server (SLES) 15; bb)Oracle Linux 8; cc) Amazon Linux 2; dd)MacOS 10.15 Catalina; ee) MacOS 10.15 Catalina Server; ff) MacOS 11 Big Sur; gg) MacOS 12 Monterey; hh)MacOS 13 Ventura; ii) MacOS

14 Sonoma; jj) Android 6 e versões posteriores; kk) iOS 9 e versões posteriores; ll) iPadOS 13 e versões posteriores.

6. O cliente deve ter a capacidade de continuar operando, mesmo quando o servidor de gerenciamento não puder ser alcançado pela rede.
7. O cliente deve ter a capacidade de atualizar a versão do agente através do servidor de gerenciamento.
8. Quando o servidor de gerenciamento estiver inoperante ou o agente estiver incapaz de comunicar-se com o servidor por razões distintas, o agente deve ser capaz de atualizar vacinas e componentes através de comunicação com uma nuvem de dados fornecida pelo fabricante.
9. Possibilidade de criação de planos de distribuição das atualizações via comunicação segura entre clientes e servidor de gerenciamento.
10. Permitir o rastreamento de malware, agendado ou manual, com a possibilidade de selecionar como alvo uma máquina ou grupo de máquinas, com periodicidade mínima diária.
11. O cliente gerenciado deve implementar funcionalidade em que as configurações, alteração, desinstalação, desativação do serviço, importação e exportação de configurações possam ser bloqueadas por senha, através do console de modo a evitar que o usuário da estação de trabalho interfira no funcionamento da solução.
12. Atualização de configurações, sem interação (em background), nos clientes sem a necessidade de reinicialização ou logoff.
13. Capacidade de tratar ameaças que exploram a ausência de correções do Sistema Operacional (patches) fazendo com que as ameaças que se utilizam de vulnerabilidades sejam bloqueadas enquanto a correção oficial não esteja instalada/disponível corretamente, ou possuir análise heurística ou inteligência artificial (machine learning)

capaz de identificar e bloquear qualquer ameaça externa que se utilize de vulnerabilidades dos sistemas operacionais.

14. Caso a solução encontre algum arquivo mal-intencionado (tais como ameaça “diazero”, ameaça persistente), deve possuir capacidade de análise e posterior bloqueio automático.

15. A função de Escaneamento de vírus deverá ter a possibilidade de configuração de exceções: a) Excluir da verificação tipos de arquivos tais como .TXT (arquivo de texto simples). b) Pastas e arquivos pré-determinados através do caminho ou Hash.

16. Deve permitir a instalação e desinstalação remota pela console de gerenciamento centralizada.

17. Possibilidade de instalação presencial através de mídia de instalação fornecida ou gerada através do servidor de antivírus.

18. Programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, com frequência (no mínimo diária) e horários definidos no console de gerenciamento centralizado: a) Permitir atualização incremental da lista de definições de vírus; b) Permitir atualização por endereço do próprio fabricante, como opção além do servidor local; c) Permitir configuração remota de ordem de preferência de endereços de atualização; d) Permitir configurar conexão através de serviço Proxy local; e) Permitir a atualização da lista de arquivos a serem verificados contra vírus através da lista de definições de vírus;

19. No sistema operacional Linux além de proteger e rastrear seus sistemas de arquivos, também aos arquivos armazenados em compartilhamentos SAMBA/CIFS ou que de alguma forma estejam disponibilizados para o acesso de clientes Windows em um servidor Linux.

20. Deve ser capaz de detectar e remover todos os tipos de malwares, incluindo vírus, ransomware, worm, trojan, spyware, rootkit, vírus de macro e códigos maliciosos.

21. Possuir mecanismo de detecção baseado em ferramentas de análise e detecção como: a) Machine Learning b) Instrusion Prevention System c) Inteligência Artificial

22. Rastreamento em tempo real para vírus de macro e arquivos criados, copiados, renomeados, movidos ou modificados, inclusive em sessões DOS abertas pelo Windows.
23. Possuir módulo de proteção em tempo real do sistema de arquivos, o qual deve controlar todos os arquivos no sistema a fim de detectar código malicioso quando os arquivos são abertos, criados ou executados.
24. Possuir módulo de detecção proativa que forneça proteção contra uma nova ameaça durante a propagação inicial.
25. A solução para estações de trabalho Windows deve possuir módulo com funcionalidade de navegador seguro, para proteção de acesso a websites que contenham dados confidenciais. Não serão aceitos módulos convencionais de “Web Protection”, deverá oferecer camada adicional dedicada para tal proteção.
26. Empregar proteção baseada em nuvem conectada diretamente aos laboratórios de pesquisa e desenvolvimento do fabricante.
27. Possuir módulo nativo de detecção e proteção contra variantes de ransomware existentes no mundo, a fim de atuar como um escudo contra este tipo de ameaça.
28. A solução deve ser capaz de fazer a varredura em um estado ocioso para fornecer proteção proativa enquanto o equipamento não está em uso
29. Permitir diferentes configurações de varredura em tempo real, tornando o desempenho do produto mais estável, principalmente em máquinas com baixo desempenho de hardware.
30.Rastreamento em tempo real dos processos em memória, para a captura de vírus que são executados em memória sem a necessidade de escrita de arquivo.
31.Detecção em tempo real e limpeza de programas maliciosos como spywares, ransomware, adwares, jokes, discadores, ferramentas de administração remota e programas quebradores de senha, realizando a remoção desses programas e a restauração de áreas do sistema danificados pelos mesmos, com possibilidade de criar

uma lista de exclusão dos programas não desejados, onde a administração seja centralizada pela mesma console de gerenciamento do antivírus.

32. Rastreamento manual com interface gráfica, customizável, com opção de limpeza.

33. Rastreamento por linha de comando, parametrizável, com opção de limpeza.

34. Programação de rastreamentos automáticos do sistema com as seguintes opções: a) Escopo: todos os drives locais, específicos ou pastas específicas; b) Ação: somente alertas, limpar automaticamente, apagar automaticamente ou mover automaticamente para área de segurança; c) Frequência: diária, semanal e mensal; d) Exclusões: pastas ou arquivos que não devem ser rastreados;

35. Possuir área de segurança (quarentena) no computador no qual o cliente estiver executando.

36. Detecção de anomalias através dos métodos de assinatura, heurística e por comportamento.

37. Proteção contra ameaças via internet. A solução deve conter pelo menos: a) Ajuste no nível de sensibilidade da detecção; b) Lista de exceção.

38. Detecção em tempo real e possibilidade de bloqueio e remoção de malwares provenientes de downloads realizados no ambiente web.

39. Permitir que a funcionalidade de rastreamento em tempo real na navegação possa ser desabilitada;

40. Detecção em tempo real e possibilidade de bloqueio e remoção de malwares no conteúdo e anexos de mensagens de correio eletrônico, pelo antivírus cliente, analisando tráfego e suportando principais clientes (no mínimo outlook).

41. Permitir que a funcionalidade de rastreamento em tempo real de e-mail possa ser desabilitada.

42 Detecção em tempo real e possibilidade de bloqueio e remoção de malwares nas áreas de armazenamento de dispositivos removíveis, tais como: a) PenDrive; b) HD externo; c) Celulares; d) Tablets; e) CD/DVD; f) Impressora USB; g) Armazenamento de

FireWire; h) Dispositivo Bluetooth; i) Leitor de cartão inteligente; j) Dispositivo de criação de imagem; k) Modem; l) Porta LPT/COM; m) Dispositivo portátil;

43 O módulo de controle de dispositivos deve estar disponível para estações de trabalho Windows, macOS e Linux.

44 Detecção, análise e reparação de vírus em arquivos compactados, automaticamente, incluindo pelo menos 05 níveis de compactação, nos formatos mais utilizados no mercado.

45. Ferramenta de firewall bidirecional local no cliente, com possibilidade de configuração, ativação e desativação através da console de gerenciamento centralizada, contendo filtros especificados por aplicação, protocolo, IP, range de IPs, rede, porta e range de portas.

46. A ferramenta de firewall local deverá tratar tráfego de entrada e de saída de forma independente.

47. Deve permitir o bloqueio do “Autorun” nas portas USB ou bloquear automaticamente a execução de qualquer ameaça em dispositivos móveis.

48. Permitir bloquear a conexão de dispositivos removíveis.

49. Gerar registro (log) dos eventos de vírus em arquivo.

50. Gerar relatórios, ao menos, de: a) Eventos de vírus; b) Status dos clientes; c) Status dos Updates;

51. Gerar notificações de eventos de vírus através de alerta por e-mail, ao menos.

52. Gerar relatórios incluindo tipos de vírus, nome do vírus e se precisa de atualização do Sistema Operacional.

53. Possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total.

54. Permitir a criação de exceções nos escaneamentos de arquivos.

55.Permitir o bloqueio de dispositivos com base nos seguintes critérios: a) Fabricante; b) Modelo; c) Número de série;

56. Permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URLs acessadas.
57. A solução deve permitir a configuração de quais portas HTTPs serão escaneadas para verificação de conexões criptografadas.
58. O Firewall deve possuir funcionalidade deve suportar os protocolos TCP e UDP.
59. O Firewall deve reconhecer o tráfego DNS, DHCP e WINS com opção de bloqueio.
60. Possuir proteção contra ataques de Denial of Service (DoS), Port-Scan e Spoofing e botnet.
61. Possibilidades de criação de assinaturas personalizadas para detecção.
62. Possibilidade de agendar a ativação de novas regras do firewall.
63. Possibilidade de criar regras diferenciadas por aplicações.
64. Bloqueio de ataques baseado na exploração da vulnerabilidade.
65. Permitir integração com navegadores WEB para prevenção de ataques.
66. Realizar proteção usando mecanismo de reputação on-line, reportando informações referentes ameaças durante a navegação web.
67. Possuir taxa de performance de rede inferior a 70MB (mega bytes) comprovada junto a instituições reconhecidas mundialmente em análises profundas de funcionalidades de fabricantes de soluções de segurança.
68. A solução deve prover proteção em tempo real contra vírus, trojans, worms, spyware, adwares e outros tipos de códigos maliciosos.
69. As configurações do antimalware deverão ser realizadas através da mesma console de todos os itens da solução.
70. Permitir a criação de listas de exceções de arquivos e diretórios (arquivos ou diretórios que não serão varridos em tempo real).
71. Permitir verificação das ameaças de maneira manual, agendada e em tempo real detectando ameaças no nível do Kernel do sistema operacional fornecendo a possibilidade de detecção de Rootkits.

72. Possibilitar que, nas varreduras agendadas, o disparo do processo ocorra por grupos com intervalos de tempo determinados, de forma a reduzir impacto em ambientes.

73. Permitir configurar ações a serem tomadas na ocorrência de ameaças, incluindo Reparar, Deletar e Ignorar.

74. Verificação de malwares nas mensagens de correio eletrônico, pelo antimalware da estação de trabalho, suportando clientes Outlook, ou que utilizem os protocolos POP3/SMTP.

75. Possuir funcionalidades que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos mesmo que sejam compactados.

76. Deve suportar varredura de, no mínimo, os seguintes padrões de compactação: a) CAB; b) ZIP; c) RAR; d) LHA; e) ARJ; f) TAR;

77. Capacidade de terminar o processo e serviço da ameaça no momento de detecção.

78. Capacidade de identificação da origem da infecção, para malwares que utilizam compartilhamento de arquivos como forma de propagação, informando nome ou endereço IP da origem com opção de bloqueio da comunicação via rede.

79. Possibilidade de bloquear verificação de malware em recursos mapeados da rede.

80. Capacidade de realizar monitoramento em tempo real por heurística correlacionando com a reputação de arquivos.

81. Não serão aceitas soluções de Antimalware que possuam engine de terceiros.

82. Permitir o bloqueio da execução de aplicações baseado em nome e pasta

83.A solução deve permitir a detecção de ameaças desconhecidas que estão em memória por comportamento dos processos e arquivos das aplicações.

84. Capacidade de detecção de keyloggers por comportamento dos processos em memória.

85. Reconhecimento de comportamento malicioso de modificação da configuração de DNS e arquivo Hosts.

86. Capacidade de detecção de Trojans e Worms por comportamento dos processos em memória, com opção de níveis distintos de sensibilidade de detecção.
87. Realizar inspeção de ameaças em ambiente isolado, com o emprego de ferramentas como: a) Aprendizado de máquina; b) Deep Learning; c) Análise estatística e dinâmica; d) Detecção baseada em comportamento; e) Introspecção na memória;
88. Detecção do malware por DNA do vírus.
89. Deverá ter a capacidade de atualizar os patches do sistema operacional.
90. A solução deve ser capaz de detectar o uso do Hyper-V e ter uma verificação de malware específica disponível para este hypervisor.
91. Em servidores que usam “OneDrive for Business” deve ser possível explorar os arquivos armazenados nesta nuvem, procurando por arquivos comprometidos ou possível malware.
92. A solução de proteção de servidor deve incluir a detecção e bloqueio de intrusões, adicionando à lista negra os endereços que foram identificados com este comportamento malicioso.
93. A solução deve adicionar exclusões automaticamente para aplicativos de servidor críticos.
94. A solução deve possuir otimização de desempenho para infraestruturas mistas (física e virtual), podendo eliminar a duplicação de verificações de arquivos, excluindo arquivos já verificados e limpos.
95. Controlar acesso a sites, possibilitando o bloqueio dos mesmos.
96. Permitir criar políticas de bloqueio com base em categorias e lista de URL.
97. Permitir gerar relatórios de sites acessados e bloqueados.
98. Permitir a personalização das mensagens exibidas quando um ou mais sites forem bloqueados.
99. Deverá possuir um plug-in que se integre com o cliente de correio eletrônico como Outlook, Outlook Express e Windows Mail.

100. Para o módulo de proteção de e-mail, deve suportar minimamente os seguintes protocolos: a) POP3; b) POP3S; c) IMAP; d) IMAPS; PARCEIROS

101. Deve permitir a configuração de ações personalizadas para detecções realizadas pelo módulo de proteção de e-mail, suportando minimamente as seguintes ações: a) Mover o e-mail para uma pasta; b) Excluir o e-mail; c) Manter o e-mail;

102. Em equipamentos macOS, a solução deve possuir módulo para proteção de emails de entrada e saída.

103. Para a navegação na internet o produto deve contar o antiphising para proteger os usuários finais de sites web falsos que tentam obter informações confidenciais.

104. A solução de proteção anti-spam deve realizar as verificações utilizando o protocolo SSL.

105. O módulo de proteção anti-spam deverá ser nativo e integrado ao Endpoint.

106. Possuir protocolo de replicação que utilize o protocolo HTTPS e o serviço de notificação via push.

Outros requerimentos gerais.

1. A solução ofertada não deve possuir restrições sobre a quantidade de equipamentos para ativação das licenças. A totalidade das licenças contratadas pode ser ativada completamente em servidores, estações de trabalho, ou dispositivos móveis, respeitando o limite total contratado.

2. Todos os módulos ofertados pelo fabricante, devem ser ativados utilizando uma única licença, sem a necessidade de aquisição de módulos separados (add-ons).

3. O fabricante deverá ter suporte local em idioma português.

4.O fabricante deve possuir escritório próprio no Brasil.

5. Possuir manuais de apoio sobre a solução em português ou inglês.

6. fabricante deverá ter documentação publicada na internet no idioma português.

REQUISITOS DA CONTRATAÇÃO

Fundamentação: De acordo com os requisitos básicos da administração.

Comentários: De acordo com o art. 62 e 170 Lei 14.133 e que atendam as especificações do anexo I, sendo exigido apresentação de amostra para verificação.

Da sustentabilidade:

3.2. A Contratada deverá observar as diretrizes, critérios e procedimentos para a gestão de resíduos estabelecidos pela Lei n° 12.305, de 2010 – Política Nacional de Resíduos Sólidos e Resolução CONAMA n° 307, de 2002 e suas alterações;

3.3. Além dos critérios de sustentabilidade eventualmente inseridos na produção do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

3.3.1. sem utilização de trabalho escravo ou infantil na sua produção;

Da subcontratação:

3.4. É vedada a subcontratação para o fornecimento do objeto.

Da garantia da contratação

3.5. Por tratar-se de material de consumo, na modalidade registro de preços, não se exigirá garantia.

4. MODELO DE EXECUÇÃO DO OBJETO

Das Condições de Entrega

4.1. O prazo de entrega dos bens é de 5 dias, contados do recebimento do pedido.

4.2. Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 2 dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

4.3. A não entrega dentro do prazo estabelecido poderá acarretar nas sanções previstas em contrato aprovado pela administração.

4.4. Os bens deverão ser entregues e instalados e configurados na sede da SAAE, praça Roberto Gomes Pedrosa, 11 – Centro – Atibaia/SP, na sala do setor de T.I. de segunda a sexta-feira das 07:30h as 16:00h.

4.5. A console de gerenciamento deverá ser configurada com o auxílio do suporte da contratada para a configuração geral do ambiente.

Da garantia, manutenção e assistência técnica

4.6. Por tratar-se de material de consumo, por ata de registro de preço, o prazo e as condições de garantia são aqueles estabelecidos na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).

5. MODELO DE GESTÃO DO CONTRATO

5.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021 e, ainda, segundo as diretrizes e os dispositivos do Decreto Municipal 9.376/2020, que define as atribuições do gestor e fiscal do contrato e cada parte responderá pelas consequências de sua inexecução total ou parcial.

5.2. Ficam nomeados para a gestão deste contrato:

Gestor	Ramon da Silva Rocha
Suplente Gestor	Djelaine Aparecida da Silva

Fiscal	Roberto Kenji de Campos Nishimura
Suplente Fiscal	Henrique Romero Rocha

6. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

Recebimento

6.1. Os materiais serão recebidos no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável, sendo verificada a sua conformidade com as especificações constantes no Termo de Referência e na proposta.

6.2. Os materiais poderão ser rejeitados, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 5 dias, a contar da recusa de recebimento, às custas da contratada, sem prejuízo da aplicação das penalidades.

6.3. Demais condições de recebimento poderão ser estabelecidas em contrato aprovado pela administração.

6.4. Demais detalhamentos podem ser estabelecidos pela área solicitante, caso não haja maiores detalhes retirar esta cláusula.

Liquidação

6.5. Recebida a Nota Fiscal ou documento de cobrança equivalente, será processada a liquidação, de acordo com os procedimentos internos.

6.6. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

6.6.1. o prazo de validade ou vencimento;

6.6.2. a data da emissão;

6.6.3. os dados do contrato e do órgão contratante;

6.6.4. o valor a pagar; e

6.6.5. eventual destaque do valor de retenções tributárias cabíveis.

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

6.8. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

6.9. Demais condições de liquidação poderão ser estabelecidas em contrato aprovado pela administração.

Da forma e prazo de pagamento

6.10. Os pagamentos serão feitos através de transferência bancária ou boleto, em até 30 (trinta) dias corridos após a entrega e aprovação da Nota Fiscal Eletrônica em substituição à Nota Fiscal, modelo 1 ou 1-A, conforme estabelecido no Protocolo ICMS 42, de 03/07/2009 e na Portaria nº 162 CAT, DE 29/12/2008, salvo outra hipótese contemplada na legislação vigente.

6.10.1. A SAAE terá o prazo de 05 (cinco) dias úteis, a contar da apresentação da Nota Fiscal/Fatura, para aceitá-la ou rejeitá-la.

6.11. Demais condições sobre a forma pagamento poderão ser estabelecidas em contrato aprovado pela administração.

7. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E FORMA DE FORNECIMENTO

Da Forma de seleção e critério de julgamento da proposta

7.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo **menor preço por item**

Forma de fornecimento

7.2. O fornecimento do objeto será por pedido, mediante demandada da contratante.

Exigências de habilitação

Habilitação jurídica

Em conformidade com o Edital aprovado pela administração.

Habilitação fiscal, social e trabalhista

Em conformidade com o Edital aprovado pela administração.

Qualificação Econômico-Financeira

Em conformidade com o Edital aprovado pela administração.

Qualificação Técnica

7.3. Comprovação de aptidão para desempenho da atividade objeto desta licitação, em nome do licitante, através de, no mínimo, 1 (um) atestado de fornecimento, emitido por pessoas jurídicas de direito público ou privado, compatível com o objeto ora licitado em características e admitindo-se o quantitativo mínimo de 50% (cinquenta por cento).

Fone: (11) 4414-3500
CNPJ: 45.743.580/0001-45
SAAE - Saneamento Ambiental de Atibaia
Praça Roberto Gomes Pedrosa, 11
Atibaia - São Paulo

8. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

8.1. O valor estimado total da ata é de **R$5.988,00 (cinco mil, novecentos e oitenta e oito reais)**, conforme custos unitários descritos na cláusula 1.1 deste Termo de Referencia.

A estimativa de custo levou em consideração orçamentos objetos desta aquisição, nas quantidades mencionadas.

9. ADEQUAÇÃO ORÇAMENTÁRIA

9.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento da Autarquia Municipal – SAAE Saneamento Ambiental de Atibaia.

9.2. A contratação será atendida pela seguinte dotação: (solicitar preenchimento ao departamento de contabilidade antes da elaboração do TR no memorando respectivo)

Gestão/Unidade	100- Superintendência
Centro de Custo	603021 – Central de Tecnologia da Informação
Fonte de Recursos	04 – Recursos Próprios da Administração Indireta
Programa de Trabalho	0091 – Manutenção e Estruturação da Superintendência do SAAE
Código Orçamentário	33.90.40.00 – Serviços de Tecnologia da Informação e Comunicação – Pessoa Jurídica

Atibaia, 03 de abril de 2024

Modelo Aprovado pela Diretoria de Administração da SAAE Atibaia
Referência: setembro/23.
(Com base no modelo da Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União Atualização: maio/2023 – Termo de Referência Aquisições – Licitação - Modelo para Pregão Eletrônico)

Fone: (11) 4414-3500
CNPJ: 45.743.580/0001-45
SAAE - Saneamento Ambiental de Atibaia
Praça Roberto Gomes Pedrosa, 11
Atibaia - São Paulo

Roberto Kenji de Campos Nishimura

Identificação e assinatura do solicitante

_____

Identificação e assinatura do Diretor responsável

saae
saneamento ambiental
ATIBAIA

Fone: 08000 112 190
CNPJ: 45.743.580/0001-45
SAAE - Saneamento Ambiental de Atibaia
Praça Roberto Gomes Pedrosa, 11
Atibaia - São Paulo

ANEXO II

DOCUMENTOS NECESSÁRIOS PARA HABILITAÇÃO

1. HABILITAÇÃO JURÍDICA

1.1. Registro empresarial na Junta Comercial, no caso de empresário individual (ou cédula de identidade em se tratando de pessoa física não empresária);
1.2. Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial, tratando-se de sociedade empresária;
1.3. Documentos de eleição ou designação dos atuais administradores, tratando-se de sociedade empresária;
1.4. Ato constitutivo devidamente registrado no Registro Civil de Pessoas Jurídicas tratando-se de sociedade não empresária, acompanhado de prova da diretoria em exercício;
1.5. Decreto de autorização, tratando-se de sociedade estrangeira no país e ato de registro ou autorização para funcionamento expedida pelo órgão competente, quando a atividade assim o exigir.

2. REGULARIDADE FISCAL E TRABALHISTA

2.1. Prova de **inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ)** do Ministério da Fazenda;

2.2. Prova de **Regularidade Fiscal para com a Fazenda Pública Federal – CND** (Certidão Negativa de Débito ou Positiva com efeitos de Negativa) relativa a Tributos Federais (inclusive as contribuições sociais) e a Dívida Ativa da União.

2.3. Prova de **Regularidade Relativa ao Fundo de Garantia por Tempo de Serviço – FGTS** através do Certificado de Regularidade do FGTS – CRF, emitido pela Caixa Econômica Federal.

2.4. Prova de **Inexistência de Débitos Inadimplidos perante a Justiça do Trabalho**, mediante apresentação de Certidão Negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei Nº 5.452, de 1º de maio de 1943.

OBSERVAÇÃO: Poderão ser apresentadas **CERTIDÕES POSITIVAS COM EFEITOS DE NEGATIVA**, conforme Artigo 206 do Código Tributário Nacional (Lei Nº 5.172, de 25 de Outubro de 1.966).

3. DISPOSIÇÕES GERAIS

7.1. Os documentos de habilitação deverão ser apresentados em original, por qualquer processo de cópia autenticada por cartório competente ou por servidor da Administração ou publicação em órgão de imprensa oficial. Os documentos deverão estar em plena vigência, ficando, porém, a critério do Agente de Contratação/Pregoeiro solicitar as vias originais de quaisquer dos documentos, caso haja constatação de fatos supervenientes.

7.2. O Agente de Contratação/Pregoeiro reserva-se o direito de solicitar das licitantes, em qualquer tempo, no curso da licitação, quaisquer esclarecimentos sobre documentos já entregues, fixando-lhes prazo para atendimento.

7.3. A falta de quaisquer dos documentos mencionados, ou a apresentação dos mesmos em desacordo com o presente edital, implicará na inabilitação da licitante.

7.4. A licitante deverá apresentar os documentos correspondentes ao estabelecimento (matriz ou filial) através do qual pretende firmar o contrato.

7.5. É vedada a mesclagem de documentos de estabelecimentos diversos, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos em nome da matriz e, válidos para todas as suas filiais.

7.6. Todas as certidões e documentos deverão ser apresentadas na forma da Lei dentro do prazo de validade fixado nos documentos oficiais apresentados, ou de 90 (noventa) dias a contar da expedição dos mesmos, caso não estipulem qualquer prazo de validade.

7.7. Em atendimento ao disposto no Capítulo V da Lei Complementar Nº 123 de

Fone: 08000 112 190
CNPJ: 45.743.580/0001-45
SAAE - Saneamento Ambiental de Atibaia
Praça Roberto Gomes Pedrosa, 11
Atibaia - São Paulo

14/12/06 e alterações na Lei Nº 147 de 07/08/14, serão observados os seguintes procedimentos:

a) As Microempresas, Empresas de Pequeno Porte e Microempresário Individual (MEI), por ocasião da habilitação, deverão apresentar toda documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição;

b) Havendo alguma restrição quanto a regularidade fiscal e trabalhista, será assegurado o prazo de 05 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que for homologado o certame, para regularização da documentação.

7.8. Não será aceita a substituição de documentos de habilitação por protocolo de requerimento de certidão.

ANEXO III

DAS SANÇÕES

<table>
<tr><th>SANÇÃO</th><th>INFRAÇÃO</th></tr>
<tr><td>1. Advertência</td><td>Dar causa à inexecução do objeto, quando não se justificar a imposição de penalidade mais grave.
* Pode ser aplicada cumulativamente com a multa.</td></tr>
<tr><td>2. Multa</td><td>
<table>
<tr><th>HIPÓTESE</th><th>MULTA</th></tr>
<tr><td>2.1 dar causa à inexecução parcial do objeto / contrato</td><td>10% sobre o valor total do Pedido / Contrato</td></tr>
<tr><td>2.2 dar causa à inexecução parcial objeto / contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo</td><td>30% sobre o valor total do Pedido / Contrato</td></tr>
<tr><td>2.3 dar causa à inexecução total do objeto / contrato</td><td>30% sobre o valor total do pedido / contrato</td></tr>
<tr><td>2.4 ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;</td><td>0,5% por dia de atraso, calculado sobre o valor da ata, até o limite de 10 (dez) dias, caracterizado o motivo para cancelamento.</td></tr>
<tr><td>2.5 irregularidade do produto por ocasião de sua utilização</td><td>10% sobre o valor total do Pedido</td></tr>
<tr><td>2.6 descumprimento de qualquer obrigação não</td><td>10% sobre o valor total do Pedido / Contrato</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>mencionadas</td><td></td></tr>
<tr><td>2.7 descumprimento do prazo de entrega</td><td>0,5% por dia de atraso, calculado sobre o valor do pedido, até o limite de 10 (dez) dias, caracterizado o motivo para cancelamento do Pedido / contrato</td></tr>
</table>
* a base de cálculo das multas será o valor do Pedido ou valor total do Contrato, quando for o caso.
</td></tr>
<tr><td>3. Impedimento de licitar e contratar</td><td>Será aplicada ao responsável por:
3.1 dar causa à inexecução parcial do objeto / contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;
3.2 dar causa à inexecução total do objeto / contrato;
3.3 deixar de entregar a documentação exigida para o processo;
3.4 não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
3.5 não celebrar o pedido / contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
3.6 ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;
* Será aplicada quando não se justificar a imposição de penalidade mais grave.
** Impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de Atibaia, pelo prazo máximo de 3 (três) anos.
*** Pode ser aplicada cumulativamente com a multa.</td></tr>
<tr><td>4. Declaração de inidoneidade para licitar ou contratar</td><td>Será aplicada ao responsável por:
4.1 apresentar declaração ou documentação falsa exigida para o processo ou prestar declaração falsa durante a execução do contrato, quando for o caso;
4.2 fraudar o processo ou praticar ato fraudulento na execução do contrato, quando for o caso;</td></tr>
</table>

	4.3 comportar-se de modo inidôneo ou cometer fraude de qualquer natureza; 4.4 praticar atos ilícitos com vistas a frustrar os objetivos da licitação; 4.5 praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013. 4.6 praticar algum dos atos descritos no item 3 acima, que justifiquem a imposição de penalidade mais grave que o impedimento de licitar e contratar. * impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos. ** Pode ser aplicada cumulativamente com a multa.

Obs.:

1. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração ao contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

2. A aplicação das sanções previstas no **caput** deste artigo não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

3. Na aplicação das sanções será observada a Lei nº 14.1333/2021, em especial arts. 155/163.