TR - TERMO DE REFERÊNCIA 38/2026

O QUE SERÁ CONTRATADO?

Item	CAT ser	Código Interno	Descrição	UN	Qtde	Valor Unitário	ValorTotal
1		2000205466	Licenciamento de solução de software de segurança do tipo **Endpoint Detection and Response (EDR)**, incluindo fornecimento de licenças, console de gerenciamento em nuvem (SaaS), proteção avançada contra malware, ransomware e ameaças do tipo zero-day, com funcionalidades de detecção e resposta em tempo real, análise comportamental, proteção de arquivos, web e e-mail, controle de dispositivos, firewall integrado, relatórios gerenciais, suporte técnico, atualizações contínuas e treinamento da equipe de TI, pelo período de 36 meses.	SV	50	R$168,77	R$8.438,50
VALOR TOTAL ESTIMADO PARA ESTA CONTRATAÇÃO			**R$8.438,50 (oito mil, quatrocentos e trinto e oito reais e cinquenta centavos)**				

JUSTIFICATIVA PARA NÃO PARCELAMENTO DA CONTRATAÇÃO

Não se mostra adequada a adjudicação por item, uma vez que o objeto consiste em solução integrada de segurança da informação, envolvendo licenciamento, gestão centralizada, suporte técnico e atualização contínua.

A fragmentação da solução poderia gerar incompatibilidades técnicas, dificuldades de gestão, falhas de segurança e comprometimento da proteção dos ativos de TI.

Dessa forma, a contratação deverá ocorrer de forma integral, em observância aos princípios da eficiência, economicidade e segurança.

DESCRIÇÃO DA SOLUÇÃO	
QUAL O MOTIVO DA CONTRATAÇÃO?	A contratação visa garantir a segurança da informação do SAAE Formiga, protegendo os ativos tecnológicos contra ameaças cibernéticas, tais como malware, ransomware, spyware e ataques avançados. A ausência de solução adequada pode resultar em perda de dados, indisponibilidade de sistemas e prejuízos operacionais e institucionais.
NATUREZA E GARANTIA DO SERVICO	
NATUREZA	O objeto da presente contratação enquadra-se como **serviço comum de tecnologia da informação**, consistente no licenciamento e disponibilização de solução de software de segurança do tipo *Endpoint Detection and Response (EDR)*, incluindo suporte técnico, atualizações contínuas e serviços necessários à sua plena operacionalização. Trata-se de serviço cujos padrões de desempenho e qualidade podem ser objetivamente definidos por meio de especificações usuais de mercado, amplamente consolidadas no setor de segurança da informação, permitindo sua contratação mediante critérios objetivos de julgamento, nos termos da Lei nº 14.133/2021. A solução a ser contratada possui características padronizadas, com funcionalidades previamente estabelecidas, tais como detecção e resposta a ameaças em tempo real, análise comportamental, proteção contra ransomware, gestão centralizada em nuvem e geração de relatórios, não demandando desenvolvimento sob medida ou customizações complexas. Adicionalmente, a execução do objeto não envolve inovação tecnológica ou desenvolvimento experimental, consistindo na disponibilização de solução já existente no mercado, amplamente utilizada por organizações públicas e privadas, o que reforça seu enquadramento como serviço comum. Dessa forma, a contratação apresenta natureza continuada, uma vez que a proteção dos ativos de tecnologia da informação deve ser mantida de forma ininterrupta, sendo indispensável a atualização constante da solução e o suporte técnico durante toda a vigência contratual, a fim de garantir a eficácia da segurança cibernética da autarquia.

HAVERÁ GARANTIA DO SERVIÇO?	☒ Sim. A contratada deverá garantir: • funcionamento da solução durante toda a vigência contratual; • atualizações contínuas das bases de dados; • suporte técnico; • correção de falhas sem ônus adicional. ☐ Não.
CRITÉRIOS DE SELEÇÃO	
FORMA DE CONTRATAÇÀO	☐ Inexigibilidade de licitação, com fundamento no art. 74, , da Lei Federal Nº 14.133/21. ☐ Dispensa de licitação em razão do valor*, com fundamento no art. 75, II, da Lei Federal n° 14.133/21. ☐ Dispensa de licitação, com fundamento no art. 75, , da Lei Federal n° 14.133/21. ☒ **Pregão eletrônico.**
CRITÉRIO DE JULGAMENTO	☒ **Menor Preço** ☐ Maior desconto.
O ORÇAMENTO ESTIMADO É SIGILOSO?	☐ Sim. ☒ Não.
REQUISITOS DA CONTRATADA	
SERÁ EXIGIDA HABILITAÇÃO TÉCNICA?	☒ **Sim.** • Atestado (s) de capacidade técnica, emitido (s) por pessoa (s) jurídica (s) de direito público ou privado, que comprove (m) ter fornecido ou estar fornecendo softwares compatíveis em características e prazos de cada item do objeto da licitação; • Declaração informando se a licitante é a fabricante, revendedora ou distribuidora autorizada do fabricante. Caso a licitante não possua uma das qualificações anteriormente, deverá ser apresentada declaração do próprio licitante de que a aquisição dos softwares, objeto desse edital, será realizada através de um canal oficial do fabricante. ☐ Não.

HÁ CRITÉRIO DE SUSTENTABILIDADE?	☒ Sim. • utilização de solução em nuvem; • redução de consumo de recursos físicos; • aumento da vida útil dos equipamentos. ☐ Não.
HÁ RISCOS A SEREM ASSUMIDOS PELA CONTRATADA?	☒ Sim. A contratada assumirá riscos relacionados a: • falhas na solução; • indisponibilidade do sistema; • ausência de atualizações; • falhas no suporte técnico. ☐ Não
HÁ PREVISÃO DE VISTORIA?	☐ Sim. ☒ Não.
COMO O SERVIÇO SERÁ PRESTADO?	☒ O serviço será prestado conforme emissão de ordem de serviço. **REQUISITOS TÉCNICOS DA SOLUÇÃO** A solução deverá obrigatoriamente possuir: **Proteção e Detecção** • Detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos e códigos nocivos, garantindo a integridade do ambiente sem a necessidade de intervenção manual. • A solução deve ser capaz de detectar, analisar e remediar ameaças (via eliminação ou quarentena), incluindo, mas não se limitando a: malware, spyware, worms, adware, exploits, cross-site scripting, trojans, keyloggers, rootkits e phishing. • Proteção contra ransomware com capacidade de detectar e bloquear tentativas de criptografia de arquivos em tempo real, protegendo dados contra sequestro digital. A solução

	deve identificar comportamentos típicos de ransomware, como modificação rápida de múltiplos arquivos, exclusão de shadow copies e alterações em boot records, interrompendo automaticamente o ataque e preservando cópias de arquivos afetados. • Análise em tempo real da memória RAM para identificação de processos ativos, detecção de injeções de código e mitigação de ameaças residentes em memória (fileless malware); • Conter antiexploit avançado para prevenção de exploração e proteção a memória e aplicativos vulneráveis, como navegadores, leitores de documentos, arquivos multimídia. Os mecanismos avançados devem observar a rotina de acesso na memória para detectar e bloquear técnicas de exploração, como verificação de chamadas de API, pivotamento de pilha(stack pivot), ROP(return oriented programming), etc • Monitoramento abrangente do sistema de arquivos, capaz de interceptar e avaliar eventos de execução, criação, cópia, renomeação, movimentação, alteração de atributos e comandos executados de forma não-gráfica via linha de comando (Prompt de Comando/DOS, PowerShell ou Shell Linux); • Escaneamento de Arquivos Compactados: Verificação automática do interior de pacotes e pastas zipadas (nos formatos ZIP e RAR), garantindo que nenhum vírus "escondido" dentro de um arquivo compactado. • O sistema deve prover um módulo de segurança flexível, permitindo que o usuário efetue verificações de forma manual, ou integre essa rotina ao gerenciador do antivírus para execução em segundo plano. • Análise heurística e comportamental capaz de identificar malware desconhecido (zero-day) com base em características e comportamentos típicos de ameaças, independentemente de assinatura prévia. O sistema deve empregar técnicas de machine learning treinadas com milhões de amostras para classificação automática de arquivos e comportamentos suspeitos. • Possibilitar a configuração de ações automáticas ou manuais a serem executadas mediante a detecção de ameaças, contemplando, no mínimo: desinfecção (reparo), exclusão

	definitiva, isolamento em área de quarentena ou adição à lista de exceções. • Garantir a integridade dos arquivos críticos do sistema operacional e das chaves de registro do Windows contra modificações não autorizadas • Serviço de Monitoração e gestão de riscos que permita a identificação de ameaças digitais conhecidas e ameaças do dia zero, vulnerabilidade, URL's maliciosas e spams dirigidos no protocolo SMTP e serviços de mitigação complementares para a segurança do ambiente; • A solução deve prover uma interface de gerenciamento unificada, permitindo a orquestração e configuração de todas as políticas de segurança englobando os módulos de Antivírus, AntiSpyware, Firewall, Detecção de Intrusão (IDS/IPS), Gerenciamento de Dispositivos a partir de um único ponto de administração • Possuir capacidade de aferir a reputação das URLs acessadas pelas estações de trabalho, bloqueando automaticamente o acesso caso o site seja classificado como perigoso ou malicioso • O sistema deve possibilitar a configuração de listas de exceção que viabilizem o acesso a determinadas URLs definidas pelo administrador, independentemente de sua classificação de reputação como perigosa. • Proteção robusta de arquivos, web e email, bloqueando ameaças transmitidas através de anexos de email, downloads, websites e arquivos infectados. A solução deve incluir filtragem de conteúdo e análise de anexos em tempo real; • Funcionalidades de Endpoint Protection Platform-EPP, tais como antimalware, web reputation, controle de aplicação, host IPS, host Firewall. • Para mitigar riscos associados a vetores físicos de ataque, a solução deverá atuar proativamente na proteção de dispositivos de armazenamento extraível, englobando unidades ópticas (CD/DVD), discos rígidos externos e Pendrive USB. • A solução deverá oferecer proteção na fase de pré-execução, utilizando modelos locais de aprendizado de máquina e heurística avançada para detectar ferramentas de ataque, exploits e técnicas de evasão de malware,

bloqueando ameaças sofisticadas antes de sua execução. Adicionalmente, deverá identificar técnicas de propagação e sites que hospedam kits de exploração (exploit kits), além de bloquear tráfego web suspeito.

Resposta a Incidentes

- Capacidade de isolamento automático de endpoints comprometidos da rede, bloqueando comunicações de entrada e saída. O isolamento deve poder ser revertido manualmente;
- Parar os ataques com base em macros e scripts. Analisar scripts, como Powershell, WMI, intérpretes de Javascript, etc e bloqueia a execução de scripts no caso de executar comandos maliciosos.
- Reparo e resposta automatizada a ameaças, quando uma ameaça é detectada, a ferramenta deve neutralizá-la imediatamente por meio de ações que incluem a conclusão do processo, a quarentena, a exclusão e a reversão de alterações mal-intencionadas.

Gerenciamento

- A solução deverá disponibilizar um console de gerenciamento web baseado em nuvem (modelo SaaS). A infraestrutura de hospedagem será de responsabilidade exclusiva da Contratada ou do fabricante, sem incidência de quaisquer custos adicionais durante a vigência do contrato.
- O console de gerenciamento deve fornecer uma interface unificada para todas as operações de segurança de endpoints, com dashboards contendo ferramentas de administração e recursos de configuração de políticas. A experiência do usuário deve ser otimizada, permitindo triagem rápida de alertas e gestão eficiente de incidentes.
- Dashboard principal com visão consolidada do estado de segurança, incluindo número de endpoints protegidos, alertas ativos, incidentes em andamento, indicadores de risco e métricas de eficácia da proteção. O dashboard deve suportar múltiplas visualizações e filtros temporais;
- Gestão de acessos granular e segura: Possibilidade de criar diferentes usuários no painel de gerenciamento, definindo exatamente quais recursos cada um pode visualizar ou alterar. Essa segregação de funções evita ações indevidas,

protege informações críticas e garante rastreabilidade total sobre quem fez o quê no sistema.

- Gestão de políticas de segurança com capacidade de criar, editar e aplicar políticas diferenciadas para grupos de endpoints baseadas em critérios como sistema operacional, localização, departamento ou nível de criticidade.
- Gestão de whitelist e blacklist de arquivos, sites, certificados digitais, processos e comportamentos, permitindo a customização de regras de detecção para o ambiente específico da autarquia;
- Controle de acesso baseado em funções (RBAC) com perfis prédefinidos (administrador, visualizador) e capacidade de criação de perfis customizados com permissões granulares.
- O sistema de instalação deve parametrizável, no qual o administrador de TI possa definir políticas de customização por grupo ou por máquina. Essa funcionalidade deve permitir a ativação ou desativação seletiva de recursos do antivírus (como proteção em tempo real, firewall, análise heurística ou verificação de pendrives), adequando a solução às limitações de hardware e ao papel de cada dispositivo na rede.
- Todos os módulos de segurança da solução devem operar de forma nativamente integrada, consolidando a geração de relatórios e o armazenamento de logs de incidentes em uma única base de dados centralizada

Integrações e Segurança

- Disponibilizar um módulo de firewall. A sua instalação nas estações de trabalho fica a cargo do gestor de TI, proporcionando a flexibilidade necessária para evitar possíveis conflitos com firewalls de borda já existentes ou para preservar o desempenho de máquinas com hardware mais limitado.
- A solução deve oferecer flexibilidade na criação de políticas de verificação por meio de listas de exclusões personalizáveis. O administrador deverá ter a capacidade de configurar o software de segurança para ignorar arquivos específicos, caminhos de diretórios completos ou aplicações de terceiros reconhecidamente seguras.

Relatórios e Notificações

	• Relatórios de Gestão disponibilizar relatórios com periodicidades diária, semanal e mensal, contendo:
	  ○ Levantamento de endpoints comprometidos por malware;
	  ○ Histórico de ameaças detectadas e bloqueadas;
	  ○ Inventário de agentes com bases de dados desatualizados.
	• Geração de relatórios em formato PDF ou CSV. Oferecer possibilidade de criar relatórios de maneira dinâmica no painel administrativo da solução.
	• Escopo de Alertas: Geração automática de notificações para: anomalias de licenciamento, detecção de surtos de vírus em massa na rede, falhas críticas de atualização dos agentes e eventos relevantes do módulo antimalware.
	• Classificação e Triagem: Todas as notificações deverão ser obrigatoriamente segmentadas por severidade (categorias: Críticas para ações imediatas e Avisos para monitoramento) e por status de interação (categorias: Não lidas e Lidas), facilitando o fluxo de trabalho da equipe de segurança.
	
	Entrega das Licenças
	
	• O fornecimento das chaves de licenciamento deverá ocorrer exclusivamente por meio digital, enviadas para um endereço de e-mail a ser definido pela Autarquia, ou por outro meio eletrônico que seja conveniente para ambas as partes.
	
	Canal de Comunicação e Suporte:
	
	• A contratada deverá disponibilizar um canal oficial de comunicação (e-mail, WhatsApp, portal de chamados ou similar) para que a equipe técnica da Autarquia possa acioná-la em caso de dúvidas técnicas ou operacionais sobre a solução. O atendimento neste canal deverá funcionar em horário comercial (segunda a sexta-feira).
	
	Pré-configuração da Solução (Out-of-the-box):
	
	• A solução deverá ser entregue com as configurações de segurança e os perfis de usuários já pré-configurados pelo fabricante. Isso garante que, mesmo sem ajustes manuais imediatos, o administrador conte com um nível mínimo essencial de proteção aplicado à rede desde o primeiro dia de uso, otimizando o tempo de implantação e evitando erros de configuração inicial.

	Responsabilidade pela Instalação: • A instalação da solução nos endpoints serão de responsabilidade da equipe técnica interna da contratante. **Modelo de Capacitação:** • A capacitação da equipe técnica ocorrerá da seguinte maneira a contratada fornecerá vídeos e manuais detalhados sobre as funcionalidades e configurações da solução. Essa abordagem flexível permite que os profissionais responsáveis pela implantação assimilem o conteúdo no seu próprio ritmo, consultando o material sempre que houver disponibilidade ou dúvida durante o processo. **Outros requisitos** • A solução deve ser compatível, com os sistemas operacionais para estações de trabalho com o ecossistema Windows (versões 7, 8, 10 e 11) e Windows Server 2012 e 2012 R2 e respectivas versões subsequentes, contemplando ambas as arquiteturas de processamento (32 e 64 bits).
LOCAL E HORA DA PRESTAÇÃO DO SERVIÇO	O serviço será prestado de forma remota (online). A contratada deverá disponibilizar as licenças de software por email, no prazo máximo de **10 (dez) dias corridos**, contados a partir do recebimento da Autorização de Fornecimento encaminhada por email. A instalação, configuração da solução e realização de treinamento da equipe serão executadas em momento posterior, mediante alinhamento prévio entre a contratada e o Setor de Tecnologia da Informação do SAAE Formiga, observando-se a conveniência administrativa e a disponibilidade das partes.
PRAZO, FORMA DE PAGAMENTO E GARANTIA DO CONTRATO	
PRAZO DO CONTRATO	36 (trinta e seis) meses.
HAVERÁ POSSIBILIDADE DE PRORROGAÇÃO?	☒ Sim, nas hipóteses dos artigos 84 e 111 da Lei Federal n° 14.133/21, desde que o preço seja vantajoso. ☐ Não.
FORMA DE PAGAMENTO	**Meio:** Ordem bancária

	Onde? Em conta corrente, informada por e-mail, ao Setor de Tesouraria do SAAE Formiga, através do endereço: **saaetesouraria@hotmail.com** **Qual o prazo? Em até 10 (dez) dias corridos, após a comprovação da execução dos serviços e entrega da nota fiscal eletrônica*.** *A nota fiscal deverá ser emitida observando as regras de retenção dispostas na Instrução Normativa RFB nº 1234 de 11 de janeiro de 2012 e Decreto Municipal nº 9961 de 05 de maio de 2023, sob pena de não aceitação por parte desta Autarquia.
QUAL A GARANTIA DO CONTRATO?	☐ X% do valor inicial do contrato. ☒ Não há. Optou-se por não exigir garantia contratual na presente contratação.
GESTÃO E FISCALIZAÇÃO CONTRATUAL	
Todas as atividades relacionadas à gestão e fiscalização do contrato/da ARP deste processo licitatório deverão seguir a IN 02/2025 do SAAE Formiga. Pela decisão da Diretoria Geral do SAAE Formiga, tais atividades ficarão sob a responsabilidade dos servidores a seguir identificados.	
Gestão	Guilherme Stalone Arantes Gonçalves
Fiscalização Técnica	Fabiano Gonçalves Rocha
Fiscalização Administrativa	Wellington Jorge Lasmar
PREVISÃO ORÇAMENTÁRIA	
DADOS ORCAMENTÁRIOS DA CONTRATAÇÃO	30.001.04.122.0001.6003.3.3.90.40.00 – F/25 – Manutenção do setor administrativo – Locação de Softwares

Formiga (MG), 03 de agosto de 2026.

Elaborado por Guilherme Stalone Arantes Gonçalves
Assessor em Tecnologia da Informação
Matrícula 1544