1. OBJETO:

Aquisição de licenças de uso de solução corporativa de Antivírus e Anti-Spam para Microsoft Windows XP ou superior incluindo garantia, suporte e atualização para utilização no parque tecnológico do Governo do Estado de Minas Gerais, conforme especificado na Tabela 1- Quantidade de itens e unidades de licenças:

2. CARACTERIZAÇÃO DO OBJETO:

A composição do objeto se encontra distribuídos em 1 (um) lote, conforme especificações descritas na tabela 01.

LOTE 01: LICENÇA

Tabela 1– Quantidade de itens e unidades de licenças

Item	Software/Plataforma/Ambiente	Código do Item	Quantidade de Licenças	Validade mínima das Licenças
01	FORNECIMENTO, COM GARANTIA, ATUALIZACAO E SUPORTE DE SOFTWARE ANTIVIRUS PARA WINDOWS XP OU SUPERIOR			02 Anos

2.1. DESCRIÇÃO DETALHADA DO ITEM:

Cada um dos Softwares descritos nos itens deverá possui uma mídia de instalação original (CD ou DVD) OU liberação de usuário e senha de acesso ao site do fabricante para download da imagem ou programa de instalação original, para cada aquisição.
Caberá a cada órgão ou entidade contratante junto à Contratada, efetivar análise técnica do recebimento e instalação do software.

2.2. ESPECIFICAÇÕES TÉCNICAS E REQUISITOS MÍNIMOS DO OBJETO

- Características do software Antivírus para estações de trabalho:

Prover segurança para estações de trabalho, sejam físicas ou em ambiente virtualizado.
Possuir console central única de gerenciamento. As configurações do Antivírus, AntiSpyware, Firewall, Proteção Contra Intrusos, controle de Dispositivos e Controle de Aplicações deverão ser realizadas através da mesma console.

Dar suporte total aos sistemas operacionais cliente baseado na plataforma Windows XP ou superior.
Executar atualizações automáticas das listas de definições de vírus e ameaças a partir de local predefinido da rede ou de site da Internet.
Permitir atualização incremental das definições de vírus e ameaças.
Permitir a instalação automática em máquinas novas na rede via software de gerenciamento remoto.
As novas configurações deverão ser efetivamente instaladas e ativadas no computador destino sem a necessidade de reinicialização do equipamento ou de efetuar logoff\ logon do usuário.
Atualizar a partir de um servidor web externo ou servidor web interno os repositórios locais em momentos específicos e estratégicos, objetivando a garantia de disponibilidade da rede.
Ter frequência de atualização, no mínimo, diária.
Oferecer suporte ao uso de repositórios locais e em nuvem para atualização do produto e vacinas emergenciais.
Permitir conexão através de servidor proxy para efetuar as atualizações.
Possibilitar executar varredura em tempo real: de arquivos (gravação e/ou leitura), de processos em memória.
Possibilitar executar varredura manual com interface Windows, configurável, com opção de limpeza.
Possibilitar o bloqueio das portas USB nos clientes ou a varredura automática ao usar as portas USB.
Capacidade de detectar vírus de macros do MSOffice;
Todos os tipos de varredura (tempo real, manual, etc.) devem possuir, no mínimo, as seguintes opções:

a. Escopo: todos os drives locais, drives específicos, ou pastas específicas.
b. Ação: alertar, limpar/apagar, deixar arquivos suspeitos em quarentena.
c. Frequência: diária, semanal, mensal.
d. Filtros: pastas, arquivos, tipos de arquivos e processos que devem ser varridos ou não.

Gerar registro (logs) da varredura localmente com posterior envio do seu conteúdo para o console central de gerenciamento.
A Central de gerenciamento deve ser capaz de exportar os logs de varredura e detecção em tempo real via SYSLOG.
Verificar pastas/arquivos via menu de contexto do Windows.
Permitir a instalação e atualização remota.
Possibilitar notificações de eventos críticos através de mensagem visual para usuário e via e-mail para administrador.
Detecção e remoção de programas maliciosos como spyware, adware, trojans, etc.
Monitoramento em tempo real, processos na memória, para a captura de vírus ou itens maliciosos.
Solução única para proteção contra malwares em geral, incluindo vírus, trojans, worms, adware, rootkits, spywares, aplicações potencialmente indesejadas.
Possuir algum método de desinstalação e desativação temporária do antivírus.
Possuir instalação através de Policies do Active Directory, script de logon.
Possuir área de quarentena com as seguintes funcionalidades:

a. Verificar novamente o arquivo na quarentena;
b. Exibir propriedades do arquivo na quarentena;

c. Restaurar o arquivo;
d. Adicionar arquivo suspeito à quarentena;
e. Enviar arquivo para análise manual e/ou automático.

Ao selecionar a opção "e. enviar arquivo para análise manual e/ou automático", o programa deverá enviar o arquivo para análise da equipe responsável por criar vacinas do fabricante. O arquivo suspeito deverá ser mantido inoperante em quarentena até que seja desinfectado por eventual vacina enviada pelo fabricante.

Ao detectar um malware, a solução deverá executar ações automáticas, ambas ao menos com as seguintes opções disponíveis:

a. Reparar o arquivo;
b. Enviar para a quarentena;
c. Excluir o arquivo.

Funcionalidade de Controle de Dispositivos:

a. Gerenciar o uso de dispositivos USB e CD/DVD, através de controles de leitura/escrita/execução do conteúdo desses dispositivos e também sobre o tipo de dispositivo permitido (ex: permitir mouse USB e bloquear disco USB);
b. Permitir criar políticas de bloqueio de dispositivos baseadas na localização atual da estação de trabalho;
c. Gerenciamento integrado à console de gerência da solução;

Funcionalidade de Controle de Aplicações:

a. Oferecer proteção para o sistema operacional, permitindo a definição de controles de acesso (escrita/leitura) para arquivos, diretórios, chaves de registro e controle de processos;
b. Permitir o bloqueio do uso de aplicações baseado em nome, diretório e hash da aplicação;
c. Possibilidade de envio de eventos críticos da máquina como alerta de vírus para a console de gerenciamento, no intuito de informar os administradores da solução sobre as novas ameaças encontradas no ambiente de antivírus;
d. Capacidade de detectar comportamentos anormais de aplicações para encontrar ameaças e vulnerabilidades baseando-se em tecnologias de heurística.
e. Controlar a atualização periódica de aplicações comumente instaladas em estações de trabalho, tais como Java, Plugins da Adobe, Navegadores Web, alertando o usuário sobre o uso de versões desatualizadas e vulneráveis dessas aplicações e possibilitando a atualização automática das mesmas.

- Características do módulo para gerenciamento

Suporte à instalação do servidor em todas as plataformas Windows 2008 Server ou superior, Red Hat Enterprise Linux versão 6 ou superior, tanto em máquinas físicas quanto virtuais.

Suportar o gerenciamento de, no mínimo, 5.000 máquinas a partir de um único servidor. Deve permitir a composição de servidores sendo administrados por um servidor primário, quando for o caso.

Permitir o gerenciamento do servidor utilizando a pilha de protocolos TCP/IP.

Permitir o gerenciamento centralizado da instalação nos clientes a partir de um único servidor, com possibilidade de Sincronização com o Active Directory.
Integração e importação, manual ou automática, da estrutura de domínios do Active Directory, LDAP;
Permitir a alteração das configurações dos antivírus/antimalware nos clientes de maneira remota e através de regras aplicáveis a uma máquina ou um grupo de máquinas.
Permitir a atualização incremental e através do uso de políticas da lista de definições de vírus nos clientes a partir de um único ponto da rede.
Permitir a criação de tarefas de atualização, verificação de vírus e upgrades de produto em intervalos de tempo pré-determinados.
Permitir o armazenamento das informações coletadas nos clientes em um banco de dados centralizado. Caso a ferramenta utilize banco de dados (SGBD) que requeira licenciamento específico, este deverá ser fornecido sem custo adicional para a Contratante.
Permitir diferentes níveis na administração do console de gerenciamento utilizando usuários do domínio.
Forçar a configuração determinada no servidor para os clientes.
Exportação dos relatórios e dados para, no mínimo, 2 (dois) dos seguintes formatos: PDF, XML, HTML, CSV, XLS, DOC e RTF.
A solução deverá possuir Dashboard que deverá conter informações como:

a. Máquinas com a lista de definições de vírus desatualizada.
b. Qual a versão do software instalado em cada máquina.
c. Os vírus que foram detectados.
d. Máquinas com eventos suspeitos

Possuir a capacidade de geração de relatórios gráficos
Possibilidade de aplicar regras diferenciadas baseando na localidade lógica da rede.
Permitir que a localidade lógica da rede seja definida pelo conjunto dos seguintes itens:

a. IP ou faixa de IP.
b. Servidores de DNS.
c. Conexão com o servidor de gerência.

Possibilidade de aplicar regras diferenciadas por grupos de usuários e maquinas.
Configuração das localidades lógicas da rede por Faixa de IP, subnet, servidor de DNS, nome do domínio e cliente conectado (ou não) ao servidor de gerenciamento.
Possuir recursos para a criação e agendamento periódicos de backups da base de dados.
Permitir a opção de instalação de Servidores de Gerenciamento adicionais fornecendo assim a possibilidade de trabalhar em modo de Load Balance e Failover.
Permitir a replicação do Banco de Dados entre os Servidores de Gerenciamento.
O antivírus deverá promover mecanismos de customização dos pacotes de instalação em clientes e servidores, com possibilidade de uso de pacotes de instalação auto-executáveis (.exe), instalação silenciosa, pastas de instalação no destino, configurações avançadas das tecnologias a serem instaladas.

O pacote deverá detectar automaticamente a versão do sistema operacional Windows do computador destino e instalar o produto correspondente sem a necessidade de intervenção do administrador ou do usuário.
A customização do pacote de instalação deverá permitir que a distribuição seja feita para os computadores em conformidade com a política de configuração determinada pelo administrador, juntamente com as últimas vacinas, em um único processo transparente e silencioso.
Caso o sistema necessite de mais de um servidor para atender o ambiente, a instalação em modo móvel (roaming) deverá possibilitar ao administrador a configuração de uma lista hierárquica de servidores de administração, para uso dos antivírus instalados em notebooks.
Possuir ferramenta que permita analisar toda a rede e faixas da rede e identificar os computadores que porventura não estejam com o antivírus instalado ou atualizado, de acordo com as políticas determinadas na console da administração.
A análise da rede deverá identificar computadores que tenham antivírus de outros fabricantes, ou que tenham antivírus instalados, porém desativados. Esta análise deverá ser feita pela rede a partir da console.
A console única de gerenciamento deve travar as configurações em clientes através de senhas para que somente o administrador possa alterar a configuração, desinstalação ou parar o antivírus dos clientes;
A console única de gerenciamento deve exibir logs e alertas de todos os clientes e servidores, em tempo real, sem a necessidade de exportar ou transferir arquivos manualmente ou através de patches entre clientes, servidores e central de gerenciamento.
Deverá possuir capacidade de envio de alertas, no mínimo, através de um destes meios: envio de mensagem de e-mail, mensagem de alerta na tela do computador, execução de scripts/programas ou SNMP.
Os alertas, sob a forma de mensagem na tela do computador, deverão possibilitar a personalização do texto a ser apresentado ao usuário e somente para computadores ou zonas de rede especificados pelo administrador.
A solução de gerenciamento centralizado deve permitir a integração com a solução de segurança para proteção de estações de trabalho (desktops e notebooks), com todos os seus módulos, e dispositivos móveis.

- Gerenciamento de dispositivos móveis (MDM):

Deve possuir compatibilidade com Dispositivos conectados através do Microsoft Exchange ActiveSync (Apple iOS; Symbian OS; Windows Mobile e Windows Phone;Android e Palm WebOS)
Deve possuir compatibilidade com Dispositivos com suporte ao Apple Push Notification (APNs) servisse (Apple iOS 3.0 ou superior)
Deve possuir as Caracteristicas de:

- Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange
- Capacidade de ajustar as configurações de:
- Sincronização de e-mail
- Uso de aplicativos
- Senha do usuário
- Criptografia de dados

- Conexão de mídia removível
- Capacidade de instalar certificados digitais em dispositivos móveis

Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão;

2.3. SERVIÇO DE SUPORTE TÉCNICO DAS LICENÇAS DE SOFTWARE ADQUIRIDAS:

A Contratada deverá prestar suporte técnico às licenças adquiridas durante todo o período de vigência contratual de 24 meses.
Detalhamento do serviço

- Serviços de suporte.

Durante a vigência do contrato e da garantia, deverá ser fornecido suporte técnico pela CONTRATADA.
A Contratada deverá fornecer serviços de suporte técnico em horário comercial para correção de erros da solução, resolução de dúvidas técnicas pelo telefone;
O horário comercial compreende o horário de 08h00min as 18h00min, de 2ª a 6ª feira, em dias úteis.
Os pedidos poderão ser registrados através de linha telefônica (local DDD 31 ou gratuita 0800), correio eletrônico ou serviço equivalente via internet, desde que seja formalizado número de protocolo ou registro de abertura de chamado;
O fabricante deverá possuir Centro de Suporte Técnico de 1º nível com atendentes que falem português.
A CONTRATADA deve fornecer correção de qualquer defeito ou falha que ocorra nos programas que impeçam o seu perfeito funcionamento de acordo com suas características e desempenho especificados em documentação técnica que acompanha cada software.
A CONTRATADA deve revisar Manuais Técnicos e Guias do Usuário, inclusive documentação, a qualquer tempo, e desde que acompanhada da respectiva atualização/revisão dos softwares.
A CONTRATADA, após a assinatura do contrato, deve disponibilizar material ou meio de consulta para a Contratante sobre como instalar, configurar e utilizar o objeto adquirido, capacitando o(s) administrador(es) e operador(es) a executar essas atividades com o console central de gerenciamento da solução adquirida. Quaisquer dúvidas técnicas na execução dessas atividades, bem como na instalação, configuração e utilização do Console de Gerenciamento Central deverão ser sanadas por meio do suporte técnico acima descrito.
Os serviços de manutenção de software deverão prover suporte aos componentes (licenças de uso); orientações sobre uso, configuração e instalação; orientações para identificação de causas de falhas de software; fornecimento de informações conhecidas sobre defeitos conhecidos e envio de informações sobre falhas não conhecidas para tratamento do fabricante do produto.

2.4. ATUALIZACAO DAS LICENÇAS:

A Contratada deverá prover toda e qualquer atualização ao produto durante a vigência do contrato.
Entende-se como atualização o fornecimento de qualquer evolução do produto, incluindo patchs, fixes, correções, updates, service packs e novas versões lançadas.
O fornecimento de novas versões e releases não acarretará quaisquer ônus adicionais à Contratante durante a vigência do contrato.
A Contratada deverá informar à Contratante toda e qualquer atualização lançada pelo Fabricante, com detalhamento técnico.

3. JUSTIFICATIVA DA AQUISIÇÃO:

A aquisição de licenças de antivírus possui, como intuito, prevenir a contaminação por vírus, malwares, suas variantes e demais ameaças cibernéticas, nos computadores da Contratante que podem pôr em risco o sigilo, a integridade e a disponibilidade das informações.
Devido à grande utilização de e-mails e acesso a páginas de internet, a aquisição de software de antivírus passa a ser necessária para fornecer segurança à infraestrutura de rede dos órgãos do Governo Estadual, sendo este licenciamento imprescindível para os ambientes informatizados.
Estas aquisições buscam proporcionar maior proteção aos computadores dos órgãos, resguardando problemas que possam prejudicar os serviços prestados aos cidadãos. Portanto, é uma questão de segurança, que possibilita garantir o desempenho das estações de trabalho e, por conseguinte, disponibilizar aos funcionários condições para a realização de suas atividades. A aquisição destas licenças é essencial para que estas tarefas sejam executadas com êxito.
Dessa forma, justifica-se a necessidade de aquisição dessas ferramentas para promover e realizar as atividades demandadas para o governo nos próximos anos.

4. OBRIGAÇÕES DAS PARTES *(ESPECÍFICAS AO OBJETO)*:

Compete ao ÓRGÃO GERENCIADOR:
Gerenciar a presente Ata, devendo para tal, nomear um gestor para acompanhamento dos fornecimentos realizados, avaliar o mercado constantemente de forma a comprovar que os preços registrados permanecem compatíveis com os praticados no mercado, promover as negociações necessárias ao ajustamento do preço e publicar trimestralmente os preços registrados.
Cuidar para que, durante a vigência da presente Ata, sejam mantidas todas as condições de habilitação e qualificação exigidas na licitação, bem assim, a sua compatibilidade com as obrigações assumidas.
Notificar o FORNECEDOR de qualquer irregularidade ocorrida no fornecimento.

Compete aos ÓRGÃOS PARTICIPANTES:
Emitir Nota de Empenho a crédito do FORNECEDOR no valor correspondente ao fornecimento das licenças;

Efetuar o pagamento referente ao objeto a ser contratado nos termos da presente Ata.
Informar ao ÓRGÃO GERENCIADOR as irregularidades ocorridas durante o fornecimento dos softwares.

Compete ao FORNECEDOR:
Fornecer durante 12 (doze) meses os softwares objeto desta Ata, a contar da publicação do extrato da mesma no Diário Oficial, na forma e condições aqui fixadas, mediante requisição do ÓRGÃO PARTICIPANTE, devidamente assinada pela autoridade responsável, em conformidade com o Edital e demais informações constantes do Pregão Eletrônico;
Entregar os itens de acordo com as especificações exigidas no Edital e em consonância com a proposta respectiva, responsabilizando se por eventuais prejuízos decorrentes do descumprimento de qualquer cláusula estabelecida na Ata. Entregar os softwares com as respectivas mídias e licenças de uso nos prazos estipulados, a contar do recebimento da Nota de Empenho ou Autorização de Fornecimento.
Entregar os softwares nos locais indicados pelos ÓRGÃOS PARTICIPANTES;
Comunicar antecipadamente a data e horário da entrega, não sendo aceitos os produtos que estiverem em desacordo com as especificações constantes deste instrumento;
Substituir, no prazo de 05 (cinco) dias úteis e sem ônus para o ÓRGÃO PARTICIPANTE, os produtos devolvidos em razão de divergências entre o material entregue e as especificações contidas nesta Ata, sujeitando-se, ainda, às sanções cabíveis.
Manter durante a execução do Contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação, bem como apresentar a cada fatura, comprovação de regularidade perante a Seguridade Social (FGTS e INSS);
Apresentar, durante todo o prazo de vigência desta Ata, a medida que forem vencendo os prazos de validade da documentação apresentada, novos documentos que comprovem as condições de habilitação e qualificação exigidas para a contratação, bem como os que comprovem a sua compatibilidade com as obrigações assumidas;
Reparar, corrigir, remover, refazer ou substituir às suas expensas, no total ou em parte, os fornecimentos em que se verificarem vícios, defeitos ou incorreções resultantes da sua execução;
Providenciar a imediata correção das deficiências, falhas ou irregularidades constatadas pelos ÓRGÃOS PARTICIPANTES, referentes à forma de fornecimento dos softwares e ao cumprimento das demais obrigações assumidas nesta Ata;
Prestar os esclarecimentos que forem solicitados pelo ÓRGÃO GERENCIADOR, cujas reclamações se obriga a atender prontamente, bem como dar ciência ao mesmo, imediatamente e por escrito, de qualquer anormalidade que verificar quando da execução do fornecimento e da garantia.
Prover todos os meios necessários à garantia da plena operacionalidade do fornecimento, inclusive considerados os casos de greve ou paralisação de qualquer natureza.

Comunicar imediatamente ao ÓRGÃO GERENCIADOR qualquer alteração ocorrida no endereço, conta bancária e outras necessárias para recebimento de correspondência.
Ressarcir os eventuais prejuízos causados ao Estado de Minas Gerais ou a terceiros, provocados por ineficiência ou irregularidades cometidas na execução das obrigações assumidas na presente Ata.
Guardar em relação aos dados, informações ou documentos de qualquer natureza, exibidos, manuseados, ou que por qualquer motivo venham a tomar conhecimento em razão dos seus serviços, o mais completo e absoluto sigilo, sob pena de responsabilidade civil e criminal por sua indevida divulgação, descuidada ou incorreta utilização.

5. CONDIÇÕES DE RECEBIMENTO:

5.1. CRITÉRIOS DE ACEITABILIDADE DO OBJETO E QUALIFICAÇÃO TÉCNICA:

Comprovação de aptidão para desempenho de atividade pertinente e compatível com as características, quantidades e prazos do objeto da licitação, através da apresentação de, no mínimo, 01 (um) atestado de desempenho anterior, fornecido por pessoa jurídica de direito público ou privado, comprobatório da capacidade técnica para atendimento ao objeto da presente licitação, com indicação da quantidade fornecida, da qualidade do material, do atendimento, do cumprimento de prazos e demais condições do fornecimento.
Entende-se por compatibilidade das características, o fornecimento de cessão de direito de uso de solução corporativa de Antivírus e AntiSpam para Microsoft Windows XP ou Superior; da quantidade, o fornecimento de, no mínimo, 10% (dez por cento) da quantidade de licenças ofertada na proposta; e dos prazos, o fornecimento do quantitativo dentro dos prazos contratados.
Para comprovação do quantitativo fornecido poderão ser apresentados tantos atestados quantos necessários para comprovar que todo o quantitativo indicado na cláusula já tenha sido fornecido pela licitante.
Na comprovação descrita anteriormente serão considerados apenas os atestados em conformidade com o descrito acima.
Após a licitação será realizada recepção técnica das licenças com finalidade de verificação das especificações técnicas descritas no Edital.
Os Softwares devem ser fornecidos preferencialmente no idioma Português do Brasil.
Deverá ser disponibilizada sempre a última versão atualizada pelo fabricante.

5.2. PRAZO DE EXECUÇÃO:

Os Kits de instalação e Licenças devem ser entregues no prazo máximo de 10 (dez) dias úteis aos órgãos participantes a partir da data da publicação do contrato.
Todas as licenças fornecidas pela Contratada durante a execução do contrato deverão ser entregues com o respectivo documento fiscal.

5.3. LOCAL DE ENTREGA:

As entregas deverão ser feitas a partir da demanda da Contratante.
Todos os produtos especificados no objeto deste Termo de Referência deverão ser entregues dentro dos limites territoriais do Estado de Minas Gerais em horário comercial, nos locais indicados pelos órgãos Contratantes, observando o disposto no art. 74 da Lei Federal n° 8.666/93.
Os locais corretos serão descritos pelos órgãos e entidades contraentes, conforme Autorização de Fornecimento ou Ordem de Serviço emitidos.
Provisoriamente, para efeito de posterior verificação da conformidade do objeto com as especificações, e caso seja encontrada alguma irregularidade, será fixado prazo para correção pela Contratada.
Definitivamente, após recebimento provisório, para verificação da integridade e realização de testes de funcionamento, se for o caso, e sendo aprovados, nos exatos termos do edital e da proposta vencedora, será efetivado o recebimento definitivo mediante expedição de termo circunstanciado e recibo aposto na Nota Fiscal (1ª e 2ª vias), que ocorrerá em até 10 dias úteis.

6. GARANTIA:

A garantia dos materiais deverá ser de, no mínimo, 24 (vinte e quatro) meses, contados a partir da data de ateste do seu recebimento.
Constatada a necessidade de reparo ou troca do produto, ela deverá ocorrer em até 30 (trinta) dias após a notificação do defeito à CONTRATADA feita pelo CONTRATANTE.
A CONTRATADA deverá manter canal de comunicação – telefone ou e-mail – durante o prazo de garantia com o CONTRATANTE.

7. PAGAMENTO:

O pagamento será efetuado através do Sistema Integrado de Administração Financeira - SIAFI/MG e/ou por meio de ordem bancária emitida por processamento eletrônico, a crédito do beneficiário em um dos bancos credenciados pelo Estado, no prazo de 30 (trinta) dias corridos da data do recebimento definitivo, com base nos documentos fiscais devidamente conferidos e aprovados pelo CONTRATANTE.

8. VIGÊNCIA:

Os contratos têm vigência de 24 (vinte e quatro) meses, contados a partir de sua publicação.

9. ASSINATURA DO RESPONSÁVEL PELA EMISSÃO DO TERMO DE REFERENCIA E ASSINATURA DA AUTORIDADE COMPETENTE (com indicação de nome e MASP)