GOVERNO DO ESTADO DE MINAS GERAIS

SEPLAG SECRETARIA DE ESTADO DE PLANEJAMENTO E GESTÃO

Central de Compras

ANEXOS

ANEXO I

TERMO DE REFERÊNCIA

PREGÃO ELETRÔNICO PARA REGISTRO DE PREÇO

PLANEJAMENTO Nº 349

1. DO OBJETO

Registro de Preços para aquisição de subscrições de licenças de uso de solução corporativa de Segurança de Endpoint's e Servidores para múltiplas plataformas incluindo garantia, suporte e atualização para utilização no parque tecnológico do Governo do Estado de Minas Gerais, conforme especificado nas Tabelas abaixo - Quantidade de itens e unidades de licenças e demais especificações descritas neste Termo de Referência.

2. CARACTERIZAÇÃO DO OBJETO

A composição do objeto se encontra distribuída em 2 (dois) lotes, conforme especificações descritas nas tabelas abaixo.

LOTE 1 – LICENÇAS PARA ENDPOINTS E SERVIDORES (ABERTO À TODOS)

Tabela 1 - Quantidade de itens e unidades de licenças

Item	Software/Plataforma/Ambiente	Código do Item	Quantidade de Licenças	Validade mínima das Licenças
01	SUBSCRIÇÃO DE LICENÇA, ATUALIZAÇÃO E SUPORTE DE	78018	30.323	12

	SOFTWARE DE SOLUÇÃO PARA SEGURANÇA DE ENDPOINTS E SERVIDORES, COM GARANTIA, PARA MÚLTIPLAS PLATAFORMAS			meses

LOTE 2 – LICENÇAS PARA ENDPOINTS E SERVIDORES (EXCLUSIVOS PARA ME/EPP)

Tabela 2 - Quantidade de itens e unidades de licenças

Item	Software/Plataforma/Ambiente	Código do Item	Quantidade de Licenças	Validade mínima das Licenças
01	SUBSCRIÇÃO DE LICENÇA, ATUALIZAÇÃO E SUPORTE DE SOFTWARE DE SOLUÇÃO PARA SEGURANÇA DE ENDPOINTS E SERVIDORES, COM GARANTIA, PARA MÚLTIPLAS PLATAFORMAS	78018	4.202	12 meses

2.1. DESCRIÇÃO DO ITEM:

Cada uma das Subscrições de Softwares descritos nos itens anteriores deverá possuir 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 endpoint e servidor demandado.

Os softwares, objetos deste Termo de Referência, são classificados como Subscrição de Softwares.

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 e solução de segurança para estações de trabalho:

As licenças devem contemplar módulos e agentes das chamadas soluções de proteção de endpoint's e Servidores de nova geração.

Prover segurança para estações de trabalho sejam físicas ou em ambiente virtualizado.

A solução deverá prover segurança para ambientes virtualizados com a utilização ou não de agentes.

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 clientes (estações de trabalho e servidores) baseados nas plataformas:

a) Windows 7 (32 e 64 bits) e superior;

b) Windows Server 2008 (32 e 64 bits) e superior;

c) Mac OS X 10.7 e superior;

d) Red Hat Enterprise Linux 6 / CentOS 6 e superior;

A solução ofertada deve estar na linha atual de comercialização e suporte do fabricante.

A solução poderá ser entregue em formato de licença de software ou suíte com módulos, desde que sejam contempladas todas as especificações técnicas descritas neste Termo de Referência.

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.

Detecção e remoção de programas maliciosos como spyware, adware, trojans, etc.

Monitoramento em tempo real, processos na memória, para a captura de vírus e/ou itens maliciosos.

- Funcionalidades de Atualização e Instalação:

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 em máquinas novas na rede via Console Central de Gerenciamento da Solução ofertada.

Atualizar o produto e vacinas emergenciais 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, ou seja, efetivar atualizações com frequência igual ou inferior a 24 horas.

A solução deve possuir agente replicador de atualizações e configurações com capacidade de gerar localmente versões incrementais das vacinas a serem replicadas com demais agentes locais, de forma a reduzir o consumo de banda do processo de execução da tarefa de atualização.

Permitir conexão através de servidor proxy para efetuar as atualizações.

- Funcionalidades de Segurança de Nova Geração:

Não deve depender exclusivamente de base de assinaturas ou hashes para identificação de ameaças.

Deve prover identificação e proteção contra ameaças e comportamento de ameaças em programas, arquivos e processos maliciosos, conhecidos e desconhecidos.

Deve identificar e neutralizar as ameaças, incluindo códigos executáveis, scripts e exploits.

Deve ser capaz de dar proteção mínima contra ferramentas de injeção de código malicioso, além de detectar e evitar a execução de backdoors.

A solução deve oferecer os recursos de “machine learning” e inteligência artificial, ou seja, avaliar ameaças por meio de assinaturas de vírus e outras ameaças, por meio de avaliação do comportamento dos ataques e ser capaz de bloqueá-los antes do efetivo ataque.

Possuir anti Exploit baseado em engine de inteligência artificial e “machine learning”.

Deve possuir capacidade automática de análise de códigos dos arquivos, identificando as características e comportamentos e, caso sejam verificados programas maliciosos, a execução não deve ser permitida, devendo ser bloqueada a execução de códigos executáveis, scripts ou comandos.

Ter funcionalidade para análise de ameaças em background, com análises periódicas no disco para detecção de ameaças inativas.

Deve prover detecção e prevenção de ameaças avançadas em tempo real, independente da máquina estar conectada ou não com a internet.

Deve identificar ameaças avançadas, conhecidas como ameaças de “zero day” e “zero second”, sem necessariamente possuir base de assinaturas e suas atualizações, tendo detecção por heurística, por comportamento ou “sandboxing”.

Capacidade de verificar a reputação de arquivos, correlacionando no mínimo as seguintes características:

- Origem confiável;
- Origem não confiável;
- Comportamento do arquivo;
- Funcionalidades de Varredura e Proteção:

Possibilitar executar varredura em tempo real: de arquivos (gravação e/ou leitura), de processos em memória.

Possibilitar executar varredura manual com interface Gráfica, configurável, com opção de limpeza.

A varredura deve possuir as seguintes funcionalidades:

- Negar acesso ao arquivo infectado e prosseguir;
- Limpar o arquivo;
- Mover o arquivo infectado para quarentena.
- Apagar o arquivo infectado (caso desejado);

Deve possuir capacidade de análise em arquivos compactados como em ZIP; RAR; WAR; JAR, etc.

Possibilitar o bloqueio das portas USB nos clientes ou a varredura automática ao usar as portas USB.

O sistema de varredura deverá contemplar todos os dispositivos conectados ao USB reconhecidos como dispositivos de armazenamento. Exemplo: dispositivos Android; Apple IOS; Still Image (câmeras); USB de armazenamento (HD Externo CD, DVD, Pen Drive);

Todos os tipos de varredura (tempo real, manual, etc.) devem possuir, no mínimo, as seguintes opções:

- Escopo: todos os drives locais, drives específicos, ou pastas específicas.
- Ação: alertar, limpar/apagar, deixar arquivos suspeitos em quarentena.
- Frequência: diária, semanal, mensal.
- 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.

Capacidade de detectar vírus de macros;

Verificar pastas/arquivos via menu de contexto similar ao do Windows.

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;

- Funcionalidades do Módulo de Firewall:

Deve possuir módulo de Firewall com as seguintes características:

- Capacidade de distinguir diferentes sub-nets e conceder opção de ativar ou não o firewall;
- Filtragem de pacotes por portas, protocolos ou direções de conexão com possibilidade de bloqueio/permissão;

- Filtragem por aplicativos e nome, podendo ser efetivada em módulo de Controle de Aplicações.
- Funcionalidades do Módulo IPS (Intrusion Prevention System):

Deve possuir módulo IPS (Intrusion Prevention System) para proteção contra port scans e exploração de vulnerabilidades de softwares.

A base de dados de análise deve ser atualizada juntamente com as vacinas;

- Funcionalidades da Central e Módulo de Gerenciamento:

A Central ou Console de gerenciamento deve ser capaz de:

Exportar os logs de varredura e detecção em tempo real no padrão SYSLOG.

Permitir a instalação e atualização remota da solução.

Deve instalar a solução com parâmetros de configuração e distribuição, como instalação silenciosa e definição de diretório.

Permitir a visualização do número de licenças gerenciadas.

Permitir visualizar eventos, gerenciar políticas e criar painéis de controle.

Possibilitar notificações de eventos críticos e alertas de segurança através de mensagem visual para usuário e via e-mail para administrador.

Solução única para proteção contra malwares em geral, incluindo vírus, trojans, worms, adware, rootkits, spywares, ransoware, aplicações potencialmente indesejadas e softwares potencialmente perigosos.

Possuir algum método de desinstalação e desativação temporária do antivírus dentro de suas funcionalidades.

Possuir instalação através de Policies do Active Directory ou script de logon.

Possuir área de quarentena com as seguintes funcionalidades:

- Verificar novamente o arquivo na quarentena;
- Exibir propriedades do arquivo na quarentena;
- Restaurar o arquivo;
- Adicionar arquivo suspeito à quarentena;
- 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.

Suporte à instalação em Sistemas Operacionais de Servidor, tanto em máquinas físicas quanto virtuais.

Suportar o gerenciamento de, no mínimo, 5.000 máquinas (endpoints) 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, manual ou automática, da estrutura de domínios do Active Directory e 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 o acesso a console de gerenciamento Web, com acesso através de protocolo seguro;

Console Web compatível com Internet Explorer; Mozilla Firefox; e Google Chrome;

Permitir diferentes níveis na administração do console de gerenciamento utilizando usuários do domínio.

A permissão de diferentes níveis de administração, com administradores e/ou grupos de administradores que gerenciam, em níveis diferentes de privilégios, grupos/subgrupos de máquinas e diferentes partes do ambiente, tendo grupo de administradores com visão completa de todo o ambiente instalado.

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:

- Máquinas com a lista de definições de vírus desatualizada.
- Qual a versão do software instalado ou indicação de versão atualizada ou desatualizada em cada máquina.
- Os vírus que foram detectados.
- Máquinas com eventos suspeitos
- Sumário das ameaças identificadas;

A solução deve permitir a visualização de relatórios de status de proteção, erros, eventos, vírus, ataques, aplicativos instalados, vulnerabilidades e atualizações de softwares.

Possuir a capacidade de geração de relatórios gráficos.

Capacidade de exportar os relatórios com possibilidade de agendamento para envio por e-mail.

Possibilidade de aplicar regras diferenciadas baseado na localidade lógica da rede para IP ou faixa de IP; Domínio; Grupo ou Unidade Organizacional.

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 pacote deverá detectar automaticamente a versão do sistema operacional 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, com as últimas vacinas, em um 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.

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 de gerenciamento.

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.

A solução de gerenciamento centralizado deve estar integrada com a solução de segurança para proteção de estações de trabalho (desktops e notebooks), com todos os seus módulos.

Para o caso de módulo de dispositivos móveis será aceito console de gerenciamento separada.

- Funcionalidades de Módulo Antimalware:

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

- Reparar o arquivo;
- Enviar para a quarentena;
- Excluir o arquivo.

A solução deve verificar a reputação de arquivos e URLS.

A solução deverá fornecer proteção contra URLS maliciosas nos protocolos HTTP, HTTPS e FTP.

A proteção contra URLS maliciosas deverá possuir lista de liberação ou bloqueio dessas URLS.

A solução deve detectar e bloquear conexões suspeitas com C&C e efetuar o bloqueio do malware que estiver fazendo a conexão.

A solução deve possibilitar o adicionamento de exceções para endereços IP’s que foram detectados como suspeitos.

- Funcionalidades de Módulo de proteção de memória:

Deve proteger e prevenir ataques como Hijacking; File Injection; File Overflow; In-Memory execution; Exploitation; Process Injection; Escalation e outros.

Deve detectar, analisar e eliminar, automaticamente e, em tempo real, oferecendo opções para Alertar, Bloquear, Encerrar ou Ignorar a execução de programas maliciosos em:

- Processos em execução na memória, para captura de programas maliciosos, sem a necessidade de escrita de arquivo;
- Variantes de malwares que possam ser geradas em tempo real na memória do endpoint, permitindo que seja tomada ação de quarentena.

Deve possuir ações em caso de violação da memória.

Analisar as execuções de ameaças em potencial nas camadas de Memória, prevenindo a entrada de códigos maliciosos.

- Funcionalidades de Módulo de Análise de scripts:

Deve ser capaz de analisar e controlar scripts e ter as seguintes ações:

- Alertar;
- Bloquear.
- Funcionalidade de Controle de Dispositivos:
- Gerenciar o uso de dispositivos USB, 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);
- Permitir criar políticas de bloqueio de dispositivos baseadas na localização atual da estação de trabalho;
- Gerenciamento integrado à console de gerência da solução;
- Funcionalidade de Controle de Aplicações:
- Permitir o bloqueio do uso de aplicações baseado em nome, diretório e hash da aplicação;
- Capacidade de detectar comportamentos anormais de aplicações para encontrar ameaças e vulnerabilidades baseando-se em tecnologias de heurística.
- Controlar a atualização periódica de aplicações comerciais, 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 via Console de Gerenciamento Central da Solução ofertada.
- Funcionalidades de Módulo de Dispositivos Móveis:

A solução deverá possuir módulo ou agentes para proteção de dispositivos móveis para os seguintes sistemas operacionais:

- ANDROID.

A solução deve possuir proteção antimalware para ANDROID.

A solução deve realizar scan de malwares em tempo real do dispositivo e cartão SD, se for o caso.

A solução deve permitir proteção contra ameaças provenientes da WEB.

A solução de segurança mobile deverá possuir aplicativo disponível nas lojas virtuais dos sistemas operacionais elencados.

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 e Garantia.

Detalhamento do serviço

• Serviços de suporte.

Durante a vigência do contrato e da garantia, deverá ser fornecido suporte técnico pela CONTRATADA.

A CONTRATADA deve dar suporte na instalação e pleno funcionamento do software no ambiente demandado da CONTRATANTE.

A CONTRATADA deve fornecer ou intermediar junto ao fabricante da solução 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, 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.

Os serviços de manutenção de software deverão prover suporte aos componentes (subscrição das 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.

CONDIÇÕES GERAIS DE CONTRATAÇÃO:

DEFINIÇÕES E CONDIÇÕES GERAIS:

Paradas planejadas são manutenções previamente agendadas entre a CONTRATADA e a CONTRATANTE para manutenções na solução proposta.

Estas paralisações devem ser solicitadas com um mínimo de 05 (cinco) dias úteis de antecedência.

Para apuração do Tempo de Atendimento para solução de problemas, os chamados são classificados em 4 (quatro) Níveis de Severidade, de acordo com a Tabela a seguir:

Severidade	Escopo
1	Um problema que tenha um impacto crítico na capacidade da CONTRATANTE em manter sua infraestrutura ativa. Um número significativo de usuários da solução e/ou da rede é incapaz de executar adequadamente as suas tarefas. A solução e/ou a rede estão inoperantes ou severamente degradados.
2	Um problema que tenha um impacto na capacidade da CONTRATANTE em manter sua infraestrutura ativa, cuja severidade seja significativa, porém não crítica, e que possa ser de natureza repetitiva. O funcionamento do sistema, da rede ou do produto é afetado, mas o desempenho não foi severamente degradado.
3	Um problema que não cause impacto na capacidade da CONTRATANTE em manter sua infraestrutura ativa.
4	Não é um problema e sim suporte para ajustes ou otimizações.

Um chamado somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE.

Solução de Contingência ou de Contorno é uma solução temporária para um problema que não elimina a sua causa raiz. Esta solução restabelece a disponibilidade do ambiente, possibilitando assim a execução plena de suas funções originais, mantendo o mesmo nível de desempenho anterior ao problema.

Para os problemas classificados como de severidade 1 (um), a assistência técnica será prestada em horário comercial, em regime 08x5 (remota), com atendimento em até 2 (duas) horas corridas após o

registro do chamado.

A solução de contingência não poderá ultrapassar 8 (oito) horas corridas após o registro do chamado.

Caso haja necessidade de troca do equipamento ou peça, apenas no caso de fornecimento de appliance, esta deverá ser feita em, no máximo, 24 (vinte e quatro) horas corridas, contadas a partir da abertura do chamado.

Para os problemas classificados como severidade 2 (dois), a assistência técnica será prestada em horário comercial, em regime 08x5 (remota), com atendimento em até 4 (quatro) horas corridas após o registro do chamado.

A solução de contingência não poderá ultrapassar 12 (doze) horas corridas após o registro do chamado.

Caso haja necessidade de troca do equipamento ou peça, apenas no caso de fornecimento de appliance, esta deverá ser feita em no máximo 72 (setenta e duas) horas corridas, contadas a partir da abertura do chamado.

Para os chamados classificados como severidade 3 (três), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 6 (seis) horas úteis após o registro do chamado.

A CONTRATADA terá, no máximo, 40 (quarenta) horas úteis, após o registro do chamado, para implantar uma solução de contingência.

Para os chamados classificados como severidade 4 (quatro), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 6 (seis) horas úteis após o registro do chamado.

A CONTRATADA terá, no máximo, 15 dias corridos para responder ao chamado, após o seu registro.

Para problemas de hardware, apenas no caso de fornecimento de appliance, a solução definitiva não poderá ultrapassar 30 (trinta) dias corridos e para software, 2 (dois) meses.

O descumprimento de qualquer um dos indicadores supracitados acarretará na aplicação de multa de acordo com a legislação em vigor.

Não será aceito, pela CONTRATANTE, a cobrança de eventuais diferenças vinculadas a questões trabalhistas, tais como férias, horas extras, sobreaviso, etc. Adicionalmente, todos os gastos provenientes de deslocamento, estadia e alimentação, caso sejam necessários, já deverão estar incluídos no preço final da proposta.

A tabela a seguir relaciona, resumidamente, os níveis de severidade e os tempos de atendimento requeridos:

Severidade				
	Regime	**Prazo**	**Solução de Contingência**	
1	Horário comercial, no regime 8x5 (remota)	Até 2 (duas) horas corridas*	Até 8 (oito) horas corridas*	
2	Horário comercial, no regime 8x5 (remota)	Até 4 (quatro) horas corridas*	Até 12 (doze) horas corridas*	
3	Horário comercial, no regime 8x5 (remota)	Até 6 (seis) horas úteis*	Até 40 (quarenta) horas úteis*	

4	Horário comercial, no regime 8x5 (remota)	Até 6 (seis) horas úteis*	*Suporte/Resposta ao chamado:* Até 15 (quinze) dias corridos*	

Tabela 2 – Níveis de Severidade

(*) prazo após o registro do chamado

PRAZO DE ATENDIMENTO DA MANUTENÇÃO E SUPORTE TÉCNICO:

ICSP – Índice de CHAMADOS solucionados no prazo previsto	
Atributo	**Valor**
Descrição	Percentual de CHAMADOS solucionados, pela CONTRATANTE, no prazo previsto em relação a todos os CHAMADOS efetuados durante o período de apuração.
Objetivo	Reduzir os atrasos na resolução de problemas, defeitos e no esclarecimento de dúvidas e questionamentos técnicos pela CONTRATADA.
Meta	95%
Periodicidade	Mensal
Unidade de Representação	Valor percentual
Forma de Cálculo	**ICSP = (TCP / TC) x 100** **onde:** TCP = Total de chamados SOLUCIONADOS dentro do prazo máximo definido neste edital, durante o período de apuração. TC = Total de chamados ABERTOS durante o período de apuração.
Mecanismo de Medição e Gestão	O mecanismo de medição e a forma de gestão deste indicador estão descrito no item "**GESTÃO DOS NÍVEIS DE SERVIÇO"** deste anexo.
Proporcionalização do Pagamento	Meta não atingida implicará em desconto no valor do pagamento mensal, pela CONTRATANTE, do serviço correspondente ou da garantia contratual ou simplesmente garantia especificada neste edital, caso o serviço correspondente tenha sido, de alguma forma, quitado pela CONTRATANTE antecipadamente.

	O desconto total será calculado aplicando acumulativamente o desconto referente a cada indicador de qualidade especificado neste item e aplicável no período de apuração correspondente. Considera-se a seguinte tabela para o cálculo do desconto referente a este indicador de qualidade: - Sem desconto, se 95% ≤ ICSP ≤ 100% - Desconto de 5%, se 90% ≤ ICSP < 95% - Desconto de 10%, se 85% ≤ ICSP < 90% - Desconto de 15%, se 80% ≤ ICSP < 85% - Desconto de 20%, se ICSP < 80%

GESTÃO DOS NÍVEIS DE SERVIÇO:

Pelo menos um dos seguintes mecanismos deve ser disponibilizado pela CONTRATADA para ABERTURA (REGISTRO) de CHAMADOS: telefone, com atendimento em português, sem custo adicional, sem limite de chamados; mensagem eletrônica (e-mail), sítio na Internet.

No caso de ligações telefônicas, o número para contato para a abertura/registro de CHAMADOS deverá ser único para todos os módulos, componentes e funcionalidades da SOLUÇÃO.

Na ABERTURA (REGISTRO) dos CHAMADOS, a CONTRATANTE irá comunicar, via mensagem eletrônica (e-mail), à CONTRATADA as seguintes informações:

- · Data e hora de abertura do CHAMADO.
- · Código alfanumérico de identificação do CHAMADO.
- · Descrição do CHAMADO.
- · Nível de Severidade do CHAMADO.
- · Identificação (nome completo e matrícula) do solicitante da CONTRATANTE.
- · Identificação do atendente da CONTRATADA.

Caso o CHAMADO tenha sido aberto via ligação telefônica, a CONTRATADA deverá confirmar, via mensagem eletrônica (e-mail), a ABERTURA (REGISTRO) do CHAMADO, incluindo as seguintes informações:

- · Código alfanumérico de identificação do CHAMADO.
- · Nível de Severidade do CHAMADO.
- · Data e hora de início do ATENDIMENTO.
- · Descrição do serviço a executar.
- · Identificação do responsável pelo serviço a executar.

O CONTIGENCIAMENTO do CHAMADO será confirmado através do aceite pela CONTRATANTE na ordem de serviço (OS) correspondente, desde que incluso as seguintes informações:

- · Código alfanumérico de identificação do CHAMADO.
- · Data e hora de conclusão do contingenciamento.

- · Descrição detalhada do serviço executado.

A CONCLUSÃO definitiva do CHAMADO será confirmada através do aceite pela CONTRATANTE na ordem de serviço (OS) correspondente, desde que incluso as seguintes informações:

- · Código alfanumérico de identificação do CHAMADO.
- · Data e hora de conclusão do serviço executado.
- · Descrição detalhada do serviço executado.

A CONTRATADA deverá elaborar e enviar à CONTRATANTE até o 5º (quinto) dia útil do mês, o RELATÓRIO DE APURAÇÃO DE NÍVEIS DE SERVIÇO, conforme o modelo apresentado no Anexo – Modelos de Documentos deste edital.

Neste relatório serão apresentados os resultados referentes a todos os INDICADORES DE QUALIDADE cujo período de apuração se encerra no mês que precede à data de sua emissão.

Caso não ocorra nenhum CHAMADO no período de apuração, a emissão deste relatório será dispensada, considerando, neste caso, que todos os INDICADORES DE QUALIDADE alcançaram a meta prevista.

Durante o período de garantia, a CONTRATANTE deverá ter a opção de abrir chamado de suporte técnico diretamente ao fabricante da solução, através de central de atendimento no Brasil.

A CONTRATANTE deverá ter acesso direto à base de dados de conhecimento do fabricante da solução. Base esta que contenha informações, orientações e assistência para instalação, desinstalação, configuração e atualização de firmware e software, aplicação de correções, diagnósticos, avaliações e resolução de problemas e demais atividades relacionadas à correta operação e funcionamento dos equipamentos.

3. ATUALIZACAO DAS LICENÇAS:

A Contratada deverá prover toda e qualquer atualização ao produto durante a vigência do contrato e da Garantia.

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.

4. JUSTIFICATIVA DA AQUISIÇÃO:

A aquisição de Subscrição de licenças de solução de segurança para endpoint’s e servidores 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 Subscrição 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.

5. DAS AMOSTRAS

RECEPÇÃO TÉCNICA:

Para os lotes 01 e 02, no prazo de até 02 (dois) dias úteis, após a suspensão da sessão de lances, o fornecedor detentor da melhor oferta deverá encaminhar amostra do produto ofertado, devidamente identificado, para realização de Recepção Técnica com objetivo de averiguação do atendimento às especificações técnicas indicadas no Anexo I – Termo de Referência.

A amostra deverá ser encaminhada ou direcionada para a Diretoria Central de Gestão de Recursos de TIC/Superintendência Central de Governança Eletrônica no seguinte endereço: Rodovia Papa João Paulo II, 3.777, Serra Verde, Belo Horizonte, MG – CEP 31630-903 – Prédio Gerais – SEPLAG, no horário de 08H00MIN (oito) às 17H00MIN (dezessete) horas.

As características definidas nos Lotes 01 e 02 deverão ser comprovadas por meio de documentação técnica a elas referenciada e por meio da realização de testes de aceitação a serem efetivados pela área demandante: Diretoria Central de Gestão de Recursos de TIC/Superintendência Central de Governança Eletrônica/SEPLAG em conjunto com a Companhia de Tecnologia da Informação do Estado de Minas Gerais – PRODEMGE/MG.

O endereço da efetivação da Recepção Técnica será na Sede da PRODEMGE: Rua da Bahia, 2277 - Lourdes - BH/MG.

Os testes de aceitação serão definidos pela área técnica de acordo com o item 2.2 - ESPECIFICAÇÕES TÉCNICAS E REQUISITOS MÍNIMOS DO OBJETO do Anexo I – Termo de Referência.

Serão escolhidos de forma aleatória 05 testes práticos para validação entre os requisitos descritos no item 2.2 do Anexo I – Termo de Referência.

A Especificação do Ambiente de Testes é:

01 Máquina Virtual (VM) para o módulo gerenciador com a seguinte configuração: 02 vCPUs, 08 GB de vRAM e 100 GB de vDISK (ou vHD);

01 VM para a estação de trabalho virtual que irá cumprir o papel de cliente onde será instalado o antimalware client com a seguinte configuração: 01 vCPU, 04 GB de vRAM e 60 GB de vDISK (ou vHD).

As VMs terão comunicação via rede IP para testes das funções de atualização e gerenciamento.

Todos os componentes de software da solução deverão ser instalados nessa configuração. Caso a solução ofertada seja composta de equipamento do tipo Appliance, este deverá ser disponibilizado e configurado pela proponente com a melhor oferta nos mesmos prazos anteriormente informados e deverá ser retirado após a realização da recepção técnica. Nem a PRODEMGE e nem a SEPLAG poderão se responsabilizar pela guarda dos equipamentos entregues à sua posse durante o período em que os mesmos estiverem disponíveis para testes. Nesse sentido é essencial que o equipamento disponibilizado seja objeto de seguro específico contra furto, roubo, descargas elétricas, intempéries, quedas, transporte e manejo inadequados e riscos afins. O licitante detentor do melhor preço, nesse caso, se obriga a informar com antecedência mínima de 02 (dois) dias úteis, sobre todos os requisitos necessários para a correta instalação física, elétrica e lógica dos equipamentos. Além disso, informará também sobre a necessidade adicional de criação e configuração de máquinas virtuais a serem providas pela PRODEMGE/SEPLAG.

O prazo para conclusão da Recepção Técnica é de 05 (cinco) dias úteis, a contar do recebimento da amostra pelo fornecedor da melhor oferta.

Após a Recepção Técnica, a amostra deverá ser retirada pelo fornecedor.

6. 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; da quantidade, o fornecimento de, no mínimo, 10% (dez por cento) da quantidade de licenças ofertadas 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 que solicitado, a última versão atualizada pelo fabricante.

7. 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 contratantes, 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 (dez) dias úteis.

8. PRAZO DE EXECUÇÃO:

Os Kits de instalação e Subscrições de 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 Subscrições de licenças fornecidas pela Contratada durante a execução do contrato deverão ser entregues com o respectivo documento fiscal.

9**.** GARANTIA:

A garantia do software adquirido deverá possuir, no mínimo, 12 (doze) 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.

10**.** GARANTIA CONTRATUAL:

I - A CONTRATADA prestará garantia dos serviços durante a execução do contrato, nos termos do artigo 56 da Lei nº. 8.666/93, em uma das modalidades abaixo citadas, no montante de 5% (cinco por cento) do valor contratado, no prazo de 10 (dez) dias úteis, contados da data de assinatura deste contrato:

a) caução em dinheiro;

b) caução em Título da Dívida Pública, considerando apenas o seu valor de mercado certificado por Bolsa de Valores;

c) seguro garantia, no qual deverá constar cláusula de cancelamento do seguro somente com a anuência do CONTRATANTE; sendo que uma cópia autenticada desta apólice deverá ser encaminhada à Diretoria de Administração Financeira e Contábil da Superintendência de Gestão e Finanças ou unidade equivalente.

d) fiança bancária fornecida por banco regularmente cadastrado pelo Banco Central-BACEN.

II - Se a modalidade escolhida for à caução em dinheiro, este deverá ser recolhido pela CONTRATADA junto ao Tesouro do Estado de Minas Gerais, por meio de Documento de Arrecadação Estadual (DAE), e, quando da devolução, após a execução do contrato, será atualizado monetariamente de acordo com a variação “pro-rata-tempore” do IPCA.

III - A CONTRATADA deverá apresentar o comprovante de depósito bancário à Superintendência de Gestão e Finanças ou unidade equivalente.

IV - Se a opção recair por fiança bancária, deverá constar do documento a expressa renúncia pelo fiador dos benefícios previstos nos artigos 827 e seguintes do Código Civil.

V - A garantia prestada pela CONTRATADA deverá garantir a continuidade do serviço contratado, bem como as obrigações assumidas pela CONTRATADA, durante todo o período de vigência deste contrato.

VI - Se o valor da garantia for utilizado em pagamento de qualquer obrigação, inclusive indenização a terceiros, ou reduzido em termos reais por desvalorização da moeda de forma que não mais representante 5% (cinco por cento) do valor total do contrato, a CONTRATADA se obriga a fazer a respectiva reposição, no prazo máximo de 72 (setenta e duas) horas, a contar da data em que for notificado.

VII - A garantia será liberada ou restituída após a execução do contrato, quando as obrigações forem consideradas cumpridas em todos os termos deste contrato e aditivos, caso ocorram. Considerar-se-á executado o contrato quando da emissão de declaração pelo CONTRATANTE de que a prestação dos serviços encerrou-se de maneira satisfatória, o que deverá ocorrer após o término da vigência contratual e comprovação pela CONTRATADA do recolhimento de todos os tributos e encargos trabalhistas.

VIII - A liberação da caução em dinheiro ou carta de fiança bancária somente ocorrerá após expressa autorização do CONTRATANTE.

IX - É facultado à CONTRATADA, no curso da execução deste contrato, substituir a modalidade de garantia por outra, dentre as previstas nesta cláusula, mediante autorização expressa do CONTRATANTE.

11. 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

12. DA PARTICIPAÇÃO DE CONSÓRCIOS:

Não será permitida a participação de empresas reunidas em consórcio, devido à baixa complexidade do objeto a ser adquirido, considerando que as empresas que atuam no mercado têm condições de fornecer os bens de forma independente.

13. VIGÊNCIA:

Os contratos têm vigência de 12 (doze) meses, contados a partir de sua publicação, sendo passiveis de prorrogação, no interesse da Administração, até o máximo de 48 (quarenta e oito) meses, conforme artigo 57, da Lei Federal n° 8.666/93.

14. 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 as subscrições de 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 as subscrições de 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 as subscrições de 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, as subscrições de softwares 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, à 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 as subscrições de 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.

ANEXO II - TERMO DE REFERÊNCIA

MODELOS DE DOCUMENTOS

RELATÓRIO DE APURAÇÃO DE NÍVEIS DE SERVIÇO

Identificação do Contrato

Contrato: _____ Data de Emissão: ___/___/___

Indicadores de Qualidade

Código do Indicador: _____

Nome: _____

Período de Apuração: ___ /___ /___ a ___ /___ /___

Valor Apurado: _____

Desconto no Pagamento: ( ) sem desconto (meta atingida)

( ) desconto de R$_____ (_____) na parcela devida no mês ou na garantia contratual ou na garantia, conforme estipulado no contrato correspondente a este serviço.

Chamados no Período

Código do Chamado	Abertura		Severidade		Contigenciamento		Encerramento	
	Data	Hora			Data	Hora	Data	Hora

Código do Indicador: _____

Nome: _____

Documento assinado eletronicamente por **Thiago Santos de Miranda Nunes**, **Servidor(a) Público(a)**, em 05/04/2018, às 11:07, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Documento assinado eletronicamente por **Weslley Costa Nogueira**, **Diretor(a)**, em 05/04/2018, às 11:09, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

Referência: Processo nº 1500.01.0000773/2017-42 SEI nº 0501743