TERMO DE REFERÊNCIA

Processo Nº 3000008462.000050/2025-52

1. DO OBJETO

1.1. Contratação de empresa para aquisição de solução integrada e gerenciada de software de proteção antivírus e *antispyware (antimalware*), por meio de Dispensa Eletrônica de Licitação com fundamento no art. 75, inc. II da Lei nº 14.133/21, visando atender as necessidades da Secretaria de Planejamento, Gestão e Desenvolvimento Regional – SEPLAG, conforme as condições, especificações, quantidades e exigências contidas neste Termo de Referência.

1.1. O objeto desta contratação não se enquadra como sendo bem de luxo, conforme definição do art. 8º do Decreto nº 51.652/ 2021.

1.2**.** As especificações e os quantitativos do objeto desta dispensa estão descritos conforme quadro abaixo:

Item	Código E-Fisco	Descrição	Quantidade	Unidade de medida/ fornecimento	Valor Unitário estimado	Valor total estimado
01	579237 - 1	LICENCA DE USO DE SOFTWARE - TIPO ANTIVIRUS/ANTIMALWARE,PARA ESTACOES DE TRABALHO, SERVIDORES, TABLETS E SMARTPHONES,COM ATUALIZACAO AUTOMATICA DO SOFTWARE E VACINAS,VERSAO ATUALIZADA	300	unidade	R$ 113,77	R$ 34.131,00
VALOR TOTAL: R$ 34.131,00						

2. DAS JUSTIFICATIVAS

2.1**.** JUSTIFICATIVADA NECESSIDADE DA CONTRATAÇÃO

2.1.1. A presente contratação se dará em função da necessidade, da aquisição de solução integrada e gerenciada de software de proteção antivírus e *antispyware (antimalware*), a fim de atender ao Núcleo Setorial de Informática NSI/Seplag, uma vez que, considerando o término da vigência das licenças do Antivírus ESET utilizadas pelos computadores e servidores da SEPLAG, em 03/06/2025, e considerando ainda, que o processo de elaboração de uma nova Ata de Registro de Preços Corporativa pela SAD - Secretaria de Administração, se encontra em fase interna de licitação, conforme consulta ao portal wikipedia da ATI (https://www.wiki.pe.gov.br.), justificando portanto a necessidade da presente contratação, tudo de acordo com as especificações e quantidades constantes neste Termo de Referência.

Informe-se, por oportuno, que tal objeto atenderá o dever legal exposto no art. 75, II da Lei Federal nº 14.133/21.

2.2. JUSTIFICATIVA DO QUANTITATIVO ESTIMADO

2.2.1. Os quantitativos previstos no presente Termo de Referência foram definidos no documento SEI Nº 3000008462.000050/2025-52, fundamentado, na CI/NSI-Seplag, (Id. 66151428), conforme os tabela apresentada abaixo:

Item	Descrição	Quantidade	Unidade de medida/ fornecimento
01	LICENÇA DE USO DE SOFTWARE - TIPO ANTIVÍRUS/ANTIMALWARE, PARA ESTAÇÕES DE TRABALHO, SERVIDORES, TABLETS E SMARTPHONES, COM ATUALIZAÇÃO AUTOMÁTICA DO SOFTWARE E VACINAS, VERSÃO ATUALIZADA	300	unidade

2.3. JUSTIFICATIVA DA CONTRATAÇÃO POR DISPENSA DE LICITAÇÃO

2.3.1. A presente contratação será formalizada por meio de dispensa de licitação, conforme permissivo legal contido no art. 75, II da Lei Federal nº 14.133/21, que permite contratação direta que envolva valores inferiores a R$ 62.725,59 (Sessenta e dois mil, setecentos e vinte e cinco reais e cinquenta e nove centavos), no caso de serviços em geral e compras, conforme atualizado pelo Decreto nº 12.343, de 30 de dezembro de 2024;

2.3.1. Nesse sentido, uma vez que a contratação pretendida corresponde a valor inferior ao referido na lei e a despesa não constitui fracionamento indevido, bem como o somatório das despesas realizadas com objetos idênticos ou de mesma natureza (do mesmo ramo de atividade), no mesmo exercício financeiro, por esta unidade gestora, não ultrapassa o limite estabelecido pelo art. 75, II da Lei Federal nº 14.133/21, destaca-se o pleno atendimento dos requisitos legais.

2.3 RAZÃO DA ESCOLHA DO CONTRATADO

2.4.1. Conforme preconiza o art. 7º, inciso II, do Decreto nº 56.586/2024, o contratado será definido utilizando-se do critério de julgamento menor preço, (item 4.4.1.), deste Termo de Referência);

2.4.2. Quando do encerramento do prazo de recebimento de propostas, o sistema de processamento da contratação direta (PE-Integrado) realizará o ranqueamento automático dos valores recebidos em ordem crescente, possibilitando ao agente público responsável pelo processamento a visualização da proposta mais bem classificada. Após convocação e negociação, caso o fornecedor envie sua proposta e documentos de habilitação, e estes sejam analisados como conformes com as disposições deste Termo de Referência (art. 14 ao 18 do Decreto nº 56.586/2024), será considerado apto à contratação, a qual só será realizada após o reconhecimento da regularidade formal do procedimento pela autorização da autoridade competente (art. 20 e 21 do Decreto nº 56.586/2024).

2.4 JUSTIFICATIVA DO PREÇO A SER CONTRATADO

2.5.1. Levando-se em consideração o disposto no art. 14 do Decreto nº estadual nº 56.586/2024, o valor a ser contratado será aquele que refletir a melhor proposta ranqueada automaticamente pelo sistema segundo o critério menor preço por item, tomando-se como limite máximo os preços obtidos no orçamento estimado da presente contratação direta (Doc. Sei nº 3000008462.000050/2025-52 (Mapa de Preços – Id. Nº 66392151) e após negociação com o fornecedor (art. 15, § 1º, do Decreto nº estadual nº 56.586/2024).

3. DAS ESPECIFICAÇÕES DO OBJETO

3.1 - Console de gerenciamento centralizada

3.1.1. O software deve dispor de gerenciamento com administração centralizada, com facilidades para instalação, administração, monitoramento, atualização e configuração, com todos os módulos de um único fornecedor.

3.1.2. O acesso ao Console de Gerenciamento deve ser efetuado via tecnologia Web segura (HTTPS) compatível, no mínimo, com os navegadores Google Chrome, Mozilla Firefox, Microsoft Edge, Opera e Safari.

3.1.3. O acesso ao Console deve suportar várias sessões simultâneas.

3.1.4. Mecanismo de comunicação (via push) em tempo real entre servidor e clientes, para entrega de configurações e assinaturas.

3.1.5. Mecanismo de comunicação randômico (pull) entre o cliente e o servidor, para consulta de novas configurações e assinaturas, evitando sobrecarga de rede e/ou no servidor.

3.1.6. Permitir o agrupamento dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio.

3.1.7. O servidor de gerenciamento deve possuir compatibilidade para instalação nos seguintes

sistemas operacionais em todas as versões/distribuições/releases e Hypervisors:

a) Microsoft Windows 10;

b) Microsoft Windows 11;

c) Microsoft Windows Server 2012;

d) Microsoft Windows Server 2012 R2;

e) Microsoft Windows Server 2016;

f) Microsoft Windows Server 2019;

g) Microsoft Windows Server 2022;

h) Ubuntu 18.04.1 LTS x64 Desktop;

i) Ubuntu 18.04.1 LTS x64 Server;

j) Ubuntu 20.04 LTS x64;

k) RHEL Server 7 x64;

l) RHEL Server 8 x64;

m) CentOS 7 x64;

n) Debian 10 x64;

o) Rocky Linux 9;

p) VMware vSphere/ESXi 6.5 e posterior;

q) VMware Workstation 9 e posterior;

r) VMware Player 7 e posterior;

s) Microsoft Hyper-V Server 2012, 2012 R2, 2016, 2019, 2022;

t) Oracle VirtualBox 6.0 e posterior;

u) Citrix 7.0 e posterior;

3.1.8. O servidor de gerenciamento deve possuir compatibilidade para instalação em sistemas operacional de 64-bits tanto em ambiente virtual quanto físico, disponibilizado pela CONTRATANTE.

3.1.9. A console de gerenciamento deve oferecer gerenciamento em nuvem, disponibilizado pela CONTRATADA.

3.1.10. Possuir integração com LDAP e Active Directory, para importação da estrutura organizacional e autenticação dos Administradores.

3.1.11. Possibilidade de aplicar regras diferenciadas baseando na localidade lógica da rede.

3.1.12. Possibilidade de criar grupos separando as regras aplicadas a cada dispositivo.

3.1.13. Possibilidade de instalação dos clientes em estações de trabalho e servidores podendo estes ser físicos ou virtualizados, via console de gerenciamento, de forma remota, sem intervenção do usuário (modo silencioso).

3.1.14. Possibilitar a remoção, de forma automatizada das soluções dos principais fabricantes atualmente instalados nas estações de trabalho e ou servidores da CONTRATANTE.

3.1.15. Deve ter a funcionalidade de descobrir automaticamente as estações da rede que não possuem o cliente instalado através de funcionalidade integrada ao console de gerenciamento.

3.1.16. Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado com opção de instalação remota.

3.1.17. A console de gerenciamento deve apresentar funcionalidade que impeça o usuário de alterar as configurações do cliente gerenciado de modo que não se possa alterar, importar e exportar configurações, abrir a console do cliente, desinstalar ou parar o serviço do cliente.

3.1.18. A console de gerenciamento deve possuir capacidade de criação de contas de usuário com diferentes perfis de acesso (minimamente os níveis de operador e administrador).

3.1.19. A solução deve possuir sistema RBAC (Role Based Access Control) para definir acessos customizados de usuários adicionais no console, oferecendo granularidade para configuração dos acessos, para segregar os acessos, limitando os acessos, não exclusivamente a políticas, tarefas, e demais objetos do console.

3.1.20. A console de gerenciamento deve possuir log centralizado e conter, no mínimo, as seguintes informações:

a) Nome da ameaça;

b) Nome do arquivo infectado;

c) Caminho da detecção;

d) HASH do arquivo;

e) Data e hora da infecção;

f) Ação tomada;

g) Endereço de IP da máquina;

h) Usuário autenticado na máquina;

i) Origem da ameaça (IP ou hostname da máquina) caso a ameaça tenha se propagado;

3.1.21. A console de gerenciamento deve fornecer, em tempo real, o status atualizado das estações de trabalho, com pelo menos as seguintes informações:

a) Nome da máquina;

b) Endereço IP da máquina;

c) Malwares não removidos;

d) Status da conexão;

e) Data da vacina;

f) Versão do antivírus instalado.

3.1.22. O console de gerenciamento deve prover alertas de segurança via E-mail, com informações de infecção de máquinas e ataques. Suportando no mínimo alertas dos seguintes módulos:

a) Detecções de Malware;

b) Detecções de Firewall;

c) Detecções via EDR;

3.2. O console de gerenciamento deve utilizar o protocolo HTTPS para comunicação entre console de gerenciamento e o cliente gerenciado.

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

3.4. A interface do console de gerenciamento deve ser totalmente em português do Brasil.

3.5. A solução deve permitir a criação do backup da base de dados do servidor de gerenciamento.

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

3.7. A console deverá funcionar também através de um Appliance Virtual, cuja imagem será fornecida pelo fabricante.

3.8. O acesso ao console de administração do antivírus deve ter a possibilidade de ser feito com duplo fator de autenticação, configurado dentro do console, onde seja possível ativá-lo sem a necessidade de nenhum add-on.

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

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

3.11. Atualização de vacinas sem a necessidade de reinicialização, tanto em desktops quanto em servidores.

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

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

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

3.15. A solução deve oferecer recurso para criação de grupos e subgrupos de máquinas baseada na hierarquia do Active Directory e LDAP e em identificador único de clientes, tal como endereço IP;

3.16. A solução deve permitir forçar a configuração determinada no servidor para os clientes, protegendo o software cliente de alterações pelos usuários, com senha pré-determinada na console de gerenciamento.

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

3.18. A solução deve permitir a criação de tarefas de rastreamento de malwares em períodos de tempo pré-determinados e na inicialização do sistema operacional.

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

3.20. A solução deve possuir ferramentas próprias para centralizar e distribuir atualizações de software e atualizações dos módulos, não será aceito o uso de ferramentas de terceiros;

3.21. A solução deve permitir criação das tarefas para uma máquina, um grupo de máquinas e/ou para todas as máquinas.

3.22. A solução deve possuir no mínimo 42 modelos de relatórios pré configurados com filtros e conjuntos de filtros na console de gerenciamento.

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

3.24. A solução deve permitir a geração de relatórios, permitindo a customização dos mesmos e a exportação para, pelo menos, os seguintes formatos:

a) CSV;

b) PDF;

3.25. A solução deve permitir a geração de relatórios que contenham as seguintes informações:

a) Máquinas com a lista de definições de vírus desatualizada, bem como de todas as máquinas e suas respectivas versões da lista de definições de vírus;

b) Versão do software de proteção instalado em cada máquina;

c) Vírus que mais foram detectados;

d) Máquinas que mais sofreram infecções em um determinado período;

3.26. A solução deve permitir o armazenamento em um banco de dados centralizado das informações coletadas nos clientes, sendo no mínimo:

a) Registro de eventos (log);

b) Relatórios de eventos de vírus e status dos clientes;

c) Relatórios de todos os softwares instalados;

d) Relatórios de todos os componentes de hardware encontrados;

3.27. A solução deve ter a capacidade de enviar eventos para um servidor SIEM ou Syslog, suportando no mínimo os seguintes formatos:
a) JSON;
b) LEEF;
c) CEF;
3.28. A solução deve fornecer, em tempo real, o status atualizado da solução de proteção nas estações de trabalho e servidores;

3.29. A solução deve possibilitar a exportação, em formato PDF e CSV, de relatórios que atuem com inventário de hardware e software de todas as estações e servidores ativos na estrutura da console de gerenciamento.

3.30. A solução deve permitir a instalação remota do agente e produto de segurança através de GPO e de SCCM.

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

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

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

3.34. Possibilitar a instalação da solução de segurança nos dispositivos móveis de maneira manual através de QRcode, link gerado pela solução de gerenciamento e envio por e-mail

3.35. Através da console de gerenciamento a solução deve possibilitar a ativação da opção de bloqueio de exploit nas estações e servidores.

3.36. A solução deve permitir a configuração de atualização incremental e on-line das vacinas.

3.37. Atualização em clientes móveis (notebook, laptop, netbook, ultrabook e similares) a partir do site

do fabricante do antimalware, bem como de outra fonte definida pelo administrador.

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

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

3.40. A solução deve oferecer a possibilidade de eleição de qualquer cliente gerenciado como um servidor de distribuição das atualizações, podendo eleger mais de um cliente para esta função.

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

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

3.43. Atualização automática das assinaturas dos servidores de gerenciamento e clientes via Internet, com periodicidade mínima a cada hora (60 minutos).

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

3.45. Solução de Antivírus para estações e servidores

3.45.1. A solução ofertada deve suportar sistemas operacionais com arquitetura 32-bits e 64-bits.

3.45.2. Deve ser gerenciado através de console de gerenciamento centralizado.

3.45.3. Interface do software cliente deve ser fornecido em português do Brasil.

3.45.4. Os manuais da solução devem ser fornecidos em português do Brasil.

3.45.5. O cliente para instalação em estações de trabalho e servidores deverá possuir compatibilidade para instalação com os seguintes sistemas operacionais, minimamente, nas seguintes versões:

a) Microsoft Windows 10;

b) Microsoft Windows 11;

c) Microsoft Windows Server 2012 R2;

d) Microsoft Windows Server 2016 (Server Core e Desktop Experience);

e) Microsoft Windows Server 2019 (Server Core e Desktop Experience);

f) Microsoft Windows Server 2022 (Server Core e Desktop Experience);

g) Ubuntu Desktop 18.04 LTS 64 bits;

h) Ubuntu Desktop 20.04 LTS;

i) Ubuntu Desktop 22.04 LTS;

j) Ubuntu Desktop 24.04 LTS;

k) Red Hat Enterprise Linux 7;

l) Red Hat Enterprise Linux 8;

m) Red Hat Enterprise Linux 9;

n) Linux Mint 20;

o) Linux Mint 21;

p) CentOS 7;

q) Ubuntu Server 18.04 LTS;

r) Ubuntu Server 20.04 LTS;

s) Ubuntu Server 22.04 LTS;

t) Ubuntu Server 24.04 LTS;

u) Debian 10;

v) Debian 11;

w) Debian 12;

x) Alma Linux 8;

y) Alma Linux 9;

z) Rocky Linux 8;

aa) Rocky Linux 9;

bb) SUSE Linux Enterprise Server (SLES) 15;

cc) Oracle Linux 8;

dd) Amazon Linux 2;

ee) MacOS 11 Big Sur;

ff) MacOS 12 Monterey;

gg) MacOS 13 Ventura;

hh) MacOS 14 Sonoma;

ii) Android 6 e versões posteriores;

jj) iOS 9 e versões posteriores;

kk) iPadOS 13 e versões posteriores.

3.46. O cliente deve ter a capacidade de continuar operando, mesmo quando o servidor de gerenciamento não puder ser alcançado pela rede.

3.47. O cliente deve ter a capacidade de atualizar a versão do agente através do servidor de gerenciamento.

3.48. Quando o servidor de gerenciamento estiver inoperante ou o agente estiver incapaz de comunicar-se com o servidor por razões distintas, o agente deve ser capaz de atualizar vacinas e componentes através de comunicação com uma nuvem de dados fornecida pelo fabricante.

3.49. A solução deve possuir recursos para criação de planos de distribuição das atualizações via comunicação segura entre clientes e servidor de gerenciamento.

3.50. Permitir o rastreamento de malware, agendado bem como manual, com a possibilidade de selecionar como alvo uma máquina ou grupo de máquinas.

3.51. O cliente gerenciado deve implementar funcionalidade em que as configurações, alteração, desinstalação, desativação do serviço, importação e exportação de configurações possam ser bloqueadas por senha, através do console de modo a evitar que o usuário da estação de trabalho interfira no funcionamento da solução.

3.52. Atualização de configurações, sem interação (em background), nos clientes sem a necessidade de reinicialização ou logoff.

3.53. Capacidade de bloquear ameaças que exploram a ausência de correções do Sistema Operacional (patches) fazendo com que as ameaças que se utilizam de vulnerabilidades sejam bloqueadas enquanto a correção oficial não esteja instalada/disponível corretamente, possuir análise heurística e inteligência artificial (machine learning) capaz de identificar e bloquear qualquer ameaça externa que se utilize de vulnerabilidades dos sistemas operacionais.

3.54. Caso a solução encontre algum arquivo mal-intencionado (tais como ameaça dia-zero, ameaça persistente), deve possuir capacidade de análise e posterior bloqueio automático.

3.55. A função de Escaneamento de vírus deverá ter a possibilidade de configuração de exceções:

a) Excluir da verificação tipos de arquivos tais como .TXT (arquivo de texto simples).

b) Pastas e arquivos pré-determinados através do caminho bem como Hash.

3.56. Deve permitir a instalação e desinstalação da solução de proteção remotamente, através do console de gerenciamento centralizado.

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

3.58. Programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, com frequência (no mínimo a cada hora) e horários definidos no console de gerenciamento centralizado:

a) Permitir atualização incremental da lista de definições de vírus;

b) Permitir atualização por endereço do próprio fabricante, como opção além do servidor local;

c) Permitir configuração remota de ordem de preferência de endereços de atualização;

d) Permitir configurar conexão do endpoint com o servidor de gerenciamento através de serviço de proxy local;

e) Permitir a atualização da lista de arquivos a serem verificados contra vírus através da lista de definições de vírus;

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

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

3.61. Possuir mecanismo de detecção baseado em ferramentas de análise e detecção como:

a) Machine Learning

b) Instrusion Prevention System

c) Inteligência Artificial

3.62. Rastreamento em tempo real para vírus de macro e arquivos criados, copiados, renomeados, movidos ou modificados, inclusive em sessões DOS abertas pelo Windows.

3.63. Possuir módulo de proteção em tempo real do sistema de arquivos, o qual deve controlar todos os arquivos no sistema a fim de detectar código malicioso quando os arquivos são abertos, criados ou executados.

3.64. Possuir módulo de detecção proativa que forneça proteção contra uma nova ameaça durante a propagação inicial.

3.65. A solução para estações de trabalho Windows deve possuir módulo com funcionalidade de navegador seguro, para proteção de acesso a websites que contenham dados confidenciais. Não serão aceitos módulos convencionais de “Web Protection”, deverá oferecer camada adicional dedicada para tal proteção.

3.66. Empregar proteção baseada em nuvem conectada diretamente aos laboratórios de pesquisa e desenvolvimento do fabricante.

3.67. Possuir módulo nativo de detecção e proteção contra variantes de ransomware existentes no mundo, a fim de atuar como um escudo contra este tipo de ameaça.

3.68. A solução deve ser capaz de fazer a varredura em um estado ocioso para fornecer proteção proativa enquanto o equipamento não está em uso

3.69. Deve permitir diferentes configurações de varredura em tempo real, tornando o produto mais performático, principalmente em máquinas com baixo desempenho de hardware.

3.70. Deve efetuar o rastreamento em tempo real dos processos em memória, para a captura de vírus que são executados em memória sem a necessidade de escrita de arquivo.

3.71. Deve efetuar a detecção em tempo real e limpeza de programas maliciosos como spywares, ransomware, adwares, jokes, discadores, ferramentas de administração remota e programas quebradores de senha, realizando a remoção desses programas e a restauração de áreas do sistema danificados pelos mesmos, com possibilidade de criar uma lista de exclusão dos programas não desejados, onde a administração seja centralizada pela mesma console de gerenciamento do antivírus.

3.72. Deve efetuar o rastreamento manual com interface gráfica, customizável, com opção de limpeza.

3.73. Deve efetuar o rastreamento por linha de comando, parametrizável, com opção de limpeza.

3.74. Deve permitir a programação de rastreamentos de malwares automaticamente com as seguintes opções:

a) Escopo: todos os drives locais, drives específicos, bem como pastas específicas;

b) Ação: somente alertas, limpar automaticamente, apagar automaticamente ou mover automaticamente para área de segurança;

c) Frequência: diária, semanal e mensal;

d) Exclusões: pastas e arquivos que não devem ser rastreados;

3.75. Possuir área de segurança (quarentena) no computador no qual o cliente estiver executando a proteção.

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

3.77. Proteção contra ameaças via internet. A solução deve conter pelo menos:

a) Ajuste no nível de sensibilidade da detecção;

b) Lista de exceção.

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

3.79. Permitir que a funcionalidade de rastreamento em tempo real na navegação possa ser

desabilitada pelo administrador;

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

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

3.82. A solução deve oferecer recurso de controle de dispositivos, tendo a capacidade de controlar, minimamente, os seguintes dispositivos:

a) PenDrive;

b) HD externo;

c) Celulares;

d) Tablets;

e) CD/DVD;

f) Impressora USB;

g) Armazenamento de FireWire;

h) Dispositivo Bluetooth;

i) Leitor de cartão inteligente;

j) Dispositivo de criação de imagem;

k) Modem;

l) Porta LPT/COM;

m) Dispositivo portátil;

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

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

3.85. O módulo de firewall local da solução de proteção deverá tratar tráfego de entrada e de saída de forma independente.

3.86. O administrador deve ter a capacidade de realizar o bloqueio do “Autorun” nas portas USB bem como bloquear automaticamente a execução de qualquer ameaça em dispositivos móveis.

3.87. A solução deve permitir bloquear a conexão de dispositivos removíveis.

3.88. A solução deve gerar registro (log) dos eventos de vírus em arquivo.

3.89. A solução deve gerar relatórios, ao menos, de:

a) Eventos de vírus;

b) Status da proteção nos clientes;

c) Status dos updates da proteção;

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

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

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

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

3.94. Permitir o bloqueio de dispositivos com base nos seguintes critérios, minimamente:

a) Fabricante;

b) Modelo;

c) Número de série;

3.95. Permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URLs acessadas.

3.96. A solução deve permitir a configuração de quais portas HTTPs serão escaneadas para verificação de conexões criptografadas.

3.97. O Firewall deve oferecer suporte aos protocolos TCP e UDP.

3.98. O Firewall deve reconhecer o tráfego DNS, DHCP e WINS com opção de bloqueio.

3.99. Possuir proteção contra ataques de Denial of Service (DoS), Port-Scan, Spoofing e botnet.

3.100. Deve permitir a criação de criação de assinaturas personalizadas para detecção.

3.101. Deve permitir a criação de novas regras personalizadas no módulo de firewall.

3.102. Deve permitir criar regras diferenciadas por aplicações.

3.103. Deve permitir o bloqueio de ataques baseado na exploração de vulnerabilidades.

3.104. Deve possuir integração com navegadores web para prevenção de ataques.

3.105. Deve realizar proteção usando mecanismo de reputação on-line, reportando ao console de gerenciamento, informações referentes às ameaças durante a navegação web.

3.106. A solução deve prover proteção em tempo real contra vírus, trojans, worms, spyware, adwares e outros tipos de códigos maliciosos.

3.107. As configurações do antimalware deverão ser realizadas através da mesma console da solução.

3.108. A solução deve permitir a criação de listas de exceções de arquivos e diretórios (arquivos ou diretórios que não serão varridos em tempo real).

3.109. A solução deve permitir a verificação das ameaças de maneira manual, agendada e em tempo real detectando ameaças no nível do Kernel do sistema operacional fornecendo a possibilidade de detecção de Rootkits.

3.110. A solução deve possibilitar que, nas varreduras agendadas, o disparo do processo ocorra por grupos com intervalos de tempo determinados, de forma a reduzir impacto no ambiente.

3.111. A solução deve permitir configurar ações a serem tomadas na ocorrência de ameaças, incluindo Reparar, Deletar e Ignorar.

3.112. A solução deve possuir funcionalidades que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos mesmo que sejam compactados.

3.113. Detecção, análise e reparação de vírus em arquivos compactados, automaticamente, incluindo pelo menos 05 níveis de compactação.

3.114. Deve suportar varredura de, no mínimo, os seguintes padrões de compactação:

a. CAB;

b. ZIP;

c. RAR;

d. LHA;

e. ARJ;

f. TAR;

3.115. A solução deve possuir a capacidade de terminar o processo e serviço da ameaça no momento de detecção.

3.116. A solução deve possuir a capacidade de identificação da origem da infecção, para malwares que utilizam compartilhamento de arquivos como forma de propagação, informando nome ou endereço IP da origem com opção de bloqueio da comunicação via rede.

3.117. A solução deve permitir bloquear a verificação de malware em recursos mapeados da rede.

3.118. A solução deve possuir capacidade de realizar monitoramento em tempo real por heurística correlacionando com a reputação de arquivos.

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

3.120. A solução deve permitir o bloqueio da execução de aplicações baseado em nome e pasta.

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

3.122. A solução deve possuir capacidade de detecção de keyloggers por comportamento dos processos em memória.

3.123. A solução deve possuir reconhecimento de comportamento malicioso de modificação da configuração de DNS e arquivo Hosts.

3.124. A solução deve possuir capacidade de detecção de Trojans e Worms por comportamento dos processos em memória, com opção de níveis distintos de sensibilidade de detecção.

3.125. A solução deve realizar inspeção de ameaças em ambiente isolado, com o emprego de ferramentas como:

a) Aprendizado de máquina;

b) Deep Learning;

c) Análise estatística e dinâmica;

d) Detecção baseada em comportamento;

e) Introspecção na memória;

3.126. A solução deve ter a capacidade de realizar a detecção do malware por DNA do vírus.

3.127. A solução deve ter a capacidade de atualizar os patches do sistema operacional.

3.128. A solução deve ser capaz de detectar o uso do Hyper-V e ter uma verificação de malware específica disponível para este hypervisor.

3.129. Em servidores que usam “OneDrive for Business” deve ser possível explorar os arquivos armazenados nesta nuvem, procurando por arquivos comprometidos ou possível malware.

3.130. A solução de proteção de servidor deve incluir a detecção e bloqueio de intrusões, adicionando à lista negra os endereços que foram identificados com este comportamento malicioso.

3.131. A solução deve adicionar exclusões automaticamente para aplicativos de servidor críticos.

3.132. A solução deve possuir otimização de desempenho para infraestruturas mistas (física e virtual), podendo eliminar a duplicação de verificações de arquivos, excluindo arquivos já verificados e limpos.

3.133. A solução deve controlar acesso a sites, possibilitando o bloqueio dos mesmos.

3.134. A solução deve permitir criar políticas de bloqueio com base em categorias e lista de URL.

3.135. A solução deve permitir gerar relatórios de sites acessados e bloqueados.

3.136. A solução deve permitir a personalização das mensagens exibidas quando um ou mais sites forem bloqueados.

3.137. A solução deve possuir um plug-in que faça integração com clientes de correio eletrônico como Outlook e Windows Mail.

3.138. A solução deve possuir recurso de verificação de malwares nas mensagens de correio eletrônico, pelo antimalware da estação de trabalho, suportando clientes Outlook e outros clientes de e-mail, que utilizem minimamente os seguintes protocolos:

a) POP3;

b) POP3S;

c) IMAP;

d) IMAPS;

3.139. A solução deve permitir a configuração de ações personalizadas para detecções realizadas pelo módulo de proteção de e-mail, suportando minimamente as seguintes ações:

a) Mover o e-mail para uma pasta;

b) Excluir o e-mail;

c) Manter o e-mail;

3.140. Em equipamentos macOS, a solução deve possuir módulo para proteção de e-mails de entrada e saída.

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

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

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

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

3.145. Outros requerimentos gerais.

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

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

3.145.3. O fabricante deverá ter suporte local em idioma português do Brasil.

3.145.4. O fabricante da solução deve dispor de laboratório próprio para desenvolvimento de vacinas e engines e possuir analista dedicado a pesquisa de defesas contra ameaças e malwares originados no Brasil. Esta informação deve ser comprovada pelo Fabricante através de documentação oficial.

3.145.5. O fabricante deve possuir um laboratório de análise e detecção de malware na América Latina.

3.145.6. O fabricante deve possuir escritório próprio no Brasil.

3.145.7. Possuir manuais de apoio sobre a solução em português do Brasil e Inglês.

3.145.8. O fabricante deverá ter documentação publicada na internet no idioma português do Brasil.

3.145.9. O fabricante deve ser citado nos relatórios do MITRE ATT&CK como contribuinte de informações e técnicas de detecção nos últimos anos.

3.145.10. O fabricante deve contar com a certificação ISO 9001 para o departamento de suporte técnico das soluções de segurança.

3.145.11. O fabricante deve contar com a certificação de segurança ISO 27001.

As especificações contidas neste Termo de Referência são as especificações mínimas que o produto ofertado deve atender, ela é soberana em relação às descritas no código do item do E-Fisco.

3.146. DA ENTREGA DO OBJETO

A Contratada deverá efetuar o fornecimento e a entrega do produto na sede da SEPLAG, conforme os seguintes requisitos:

3.146.1. A entrega será realizada de forma integral, no prazo de até 15 (quinze) dias contados do recebimento da Ordem de Fornecimento ou Nota de Empenho pela Contratada.

3.146.2. A entrega será realizada nas instalações da Secretaria Estadual de Planejamento, Gestão e Desenvolvimento Regional - SEPLAG, especificamente no Núcleo Setorial de Informática - NSI, localizado no endereço – Rua da Aurora, nº 1377 - Santo Amaro - Recife-PE, mediante solicitação da Contratante e agendamento prévio, no horário das 8h às 17h, em dias úteis de segunda-feira a sexta-feira, onde o produto será conferido e recebido.

3.146.3. O recebimento do objeto fica sob responsabilidade do Núcleo Setorial de Informática - NSI, que deverá acompanhar, fiscalizar e verificar a conformidade do fornecimento, cabendo-lhe:

a. Fiscalizar a regularidade e adequação do fornecimento;

b. Verificar a conformidade do produto fornecido com as especificações contidas neste Termo de Referência, recusando o fornecimento de objeto diverso, salvo quando de qualidade superior e devidamente aceito pelo Contratante;

c. Receber o objeto adquirido e atestar a respectiva fatura, encaminhando-a para pagamento; e

d. Comunicar por escrito à autoridade competente irregularidades cometidas pela empresa passíveis de penalidade.

3.146.4. Para a entrega do objeto, é imprescindível apresentar a Nota Fiscal;

a. As despesas de frete e embalagem deverão estar inclusas no preço proposto, e em hipótese alguma poderão ser destacadas quando da emissão da nota fiscal/fatura;

b. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade ético-profissional da Contratada pela perfeita execução do contrato, nem a responsabilidade pelos prejuízos resultantes da incorreta execução do contrato;

c. A Contratada deve comunicar à Contratante, no prazo máximo de 2 (dois) dias útil(eis) que antecedam a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, se for o caso, com a devida comprovação;

d. O objeto desta contratação poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com este Termo de Referência.

e. A Contratada deve substituir, reparar ou complementar, às suas expensas, no todo ou em parte, conforme o caso, no prazo de até 3 (três) dia(s) útil(eis), contados da notificação feita pelo fiscal, os itens que apresentarem vícios, defeitos ou qualquer irregularidade;

4. DO VALOR ESTIMADO DA CONTRATAÇÃO, DA CLASSIFICAÇÃO ORÇAMENTÁRIA DA DESPESA, DO BENEFÍCIO PREVISTO NA LEI COMPLEMENTAR Nº 123/2006 E DO CRITÉRIO DE JULGAMENTO

4.1. O valor estimado global da contratação é de R$ 34.131,00 (trinta e quatro mil cento e trinta e um reais);

4.1.1. No preço total do objeto deverão estar inclusos todos os tributos (impostos, taxas e contribuições), sejam federais, estaduais e municipais, bem como frete, comissões, pessoal, embalagem, seguros, encargos sociais e trabalhistas, assim como demais insumos inerentes que incidam ou venham a incidir sobre o objeto, sejam de que naturezas forem;

4.1.2. Os preços finais unitários e totais propostos pelos fornecedores não poderão ultrapassar o preço unitário e total estimado pela Administração.

4.2. CLASSIFICAÇÃO ORÇAMENTÁRIA DA DESPESA

4.2.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento do Estado de Pernambuco, para o presente exercício, na classificação abaixo:

Fonte: 0500000000

Unidade: 0119-Seplag

Programa: 04.122.0452.4388.0000

Ação: 43880000

Elemento de Despesa: 3.3.90

Categoria Econômica: 3390

4.3. JUSTIFICATIVA PARA APLICAÇÃO OU NÃO DO BENEFÍCIO PREVISTO NA LEI COMPLEMENTAR Nº 123/2006

4.3.1. As contratações por dispensa em razão do valor previstas no inciso II do art. 2º do Decreto Estadual nº 56.586/2024 que não excedam R$ 80.000,00 (oitenta mil reais) deverão ser destinadas exclusivamente à participação de microempresas e empresas de pequeno porte, nos termos da Lei Complementar Federal nº 123, de 14 de dezembro de 2006, salvo nas hipóteses previstas nos incisos II e III do art. 49 da Lei Complementar nº 123/ 2006.

4.4. CRITÉRIO DE JULGAMENTO

4.4.1. O critério de julgamento será o MENOR GLOBAL.

5. PROPOSTA

5.1 PRAZO DE VALIDADE DA PROPOSTA

5.1.1. As propostas deverão ter validade de, no mínimo, 60 (sessenta) dias, contados da data da sua apresentação, independente de declaração da empresa.

6. DOS DOCUMENTOS DE HABILITAÇÃO

6.1. A proponente deverá apresentar os seguintes documentos, nos termos e prazo previstos neste Termo de referência:

6.1.1. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

6.1.2. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

6.1.3. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

6.1.4. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

6.1.5. Sociedades estrangeiras que não funcionem no País devem apresentar documentos de habilitação equivalentes, na forma de regulamento emitido pelo Poder Executivo Federal, inicialmente em tradução livre.

6.1.6. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

6.1.7. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz.

6.1.8. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

6.2**.** REGULARIDADE FISCAL, SOCIAL E TRABALHISTA:

6.2.1. Prova de regularidade fiscal perante a Fazenda Nacional, através da Certidão Negativa de Débitos relativos a Créditos Tributários Federais e à Dívida Ativa da União (CND), expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, ou Certidão Positiva com Efeitos de Negativa;

6.2.2. Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviço – FGTS, comprovada através de apresentação de certidão fornecida pela Caixa Econômica Federal.

6.2.3. Prova de regularidade para com a Fazenda Estadual, comprovada através de Certidão de Regularidade Fiscal – CRF, emitida pela Secretaria da Fazenda do domicílio ou sede da proponente. Considerando-se o proponente com filial no Estado de Pernambuco, deverá apresentar, também, a CRF de Pernambuco.

6.2.4. Prova de regularidade perante a Justiça do Trabalho, através de Certidão Negava de Débitos Trabalhistas – CNDT ou Certidão Positiva com efeitos de Negativa, de acordo com a Lei nº 12.440/2011 e Resolução Administrava nº 1.470/2011 do TST.

6.2.5. Declaração de comprovação do cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal.

6.3**.** QUALIFICAÇÃO ECONÔMICO FINANCEIRA

6.3.1. Certidão Negativa de Falência, expedida pelo distribuidor ou distribuidores (caso exista mais de um) da sede ou domicílio da proponente;

6.3.2. Certidão Negativa de Falência referente aos processos distribuídos pelo PJE (processos judiciais eletrônicos) da sede ou domicílio da proponente;

6.3.2.1. A certidão descrita no item acima somente é exigível quando a certidão negativa de Falência da sede ou do domicílio da proponente contiver a ressalva expressa de que não abrange os processos judiciais eletrônicos.

6.4**.** DOCUMENTOS COMPLEMENTARES:

6.4.1. Declaração de cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal, de acordo com o modelo estabelecido no Anexo E deste Termo de Referência.

6.5**.** DAS REGRAS GERAIS RELATIVAS AOS DOCUMENTOS DE HABILITAÇÃO

6.5.1. Inexistindo preceito legal ou prazo de validade fixado no próprio instrumento, os documentos/certidões serão considerados válidos por um período de 90 (noventa) dias contados da sua emissão, exceto quando se tratar de Certidão Negativa de Falência, que terá validade de 180 (cento e oitenta) dias da sua expedição;

6.5.1.1. Caso haja previsão de prazo diverso em lei ou em norma infralegal municipal, de outros estados da federação ou internacional, a proponente ficará responsável por juntar a respectiva comprovação;

6.5.2. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira poderá ser substituída pelo Certificado de Registro de Fornecedor emitido pelo CADFOR-PE, desde que os documentos contemplados estejam dentro do prazo de validade, ou pelo certificado de registro cadastral unificado disponível no Portal Nacional de Contratações Públicas - PNCP, nos termos do regulamento próprio.

7. DO CONTRATO

7.1**.** A presente contratação será formalizada por instrumento hábil, ficando dispensada a celebração de instrumento contratual, em conformidade com o art. 95 da Lei nº 13.144/2021.

7.2**.** OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE

7.2.1. Receber o objeto deste termo, verificando se a qualidade e os quantitativos dos serviços prestados pela CONTRATADA estão em conformidade com as especificações exigidas no Processo de Contratação em epígrafe, emitindo atesto de recebimento na nota fiscal eletrônica;

7.2.2. Eencaminhar a fatura devidamente atestada para liberação de pagamento;

7.2.3. Efetuar os pagamentos no prazo e nas condições indicados neste termo, comunicando à CONTRATADA quaisquer irregularidades ou problemas que possam inviabilizá-los;

7.2.4. Acompanhar e fiscalizar a execução do serviço e aplicar as medidas corretivas necessárias, inclusive as penalidades contratual e legalmente previstas, comunicando, por escrito, à CONTRATADA as ocorrências que a seu critério exijam medidas corretivas;

7.2.5. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA.

7.3**.** OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

7.3.1. Fornecer o produto de acordo com as especificações contidas neste Termo de Referência;

7.3.2. Arcar com todas as despesas decorrentes da execução do objeto do presente ajuste, tais como impostos, frete, taxas, seguros, materiais, incidentes, enfim, tudo o que for necessário ao fornecimento e entrega do produto à Contratante;

7.3.3. Responsabilizar-se por quaisquer danos ou prejuízos ao patrimônio da Contratante ou a terceiros, por ação ou omissão na execução do objeto, ficando obrigada a substituir, reparar ou reembolsar o que danificar, com a urgência requerida;

7.3.4. Emitir e encaminhar fatura em conformidade com o produto fornecido, em termos qualitativos e quantitativos, bem como disponibilizar os documentos necessários para sua validação;

7.3.5. Abster-se de quaisquer iniciativas que impliquem em ônus para a Contratante, se não previstas neste instrumento e expressamente autorizadas;

7.3.6. Cumprir rigorosamente os prazos e condições especificados neste instrumento, sujeitando-se às sanções estabelecidas.

7.3.7. Afastar ou substituir, a seu critério ou por recomendação do CONTRATANTE, qualquer empregado que comprovadamente causar embaraço à boa execução deste instrumento, por ineficiência, má conduta ou falta de respeito para com os funcionários do CONTRATANTE ou terceiros;

7.3.8. Responsabilizar-se por todo e qualquer acidente de trabalho, bem como sobre o respectivo seguro, de que venham a ser vítimas os seus empregados atuantes na execução do objeto do presente instrumento;

7.3.9. Utilizar equipamentos próprios necessários à perfeita e completa execução deste instrumento;

7.3.10. Corrigir e substituir a suas expensas, total ou parcialmente, os equipamentos que apresentem defeitos ou incorreções;

7.3.11. Obedecer às especificações do Objeto;

7.3.12. Responsabilizar-se pelos danos causados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo na execução do CONTRATO, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo Órgão. CONTRATANTE;

7.3.13. Manter, durante toda a execução do objeto, todas as condições de habilitação e qualificação exigidas na licitação, em compatibilidades com as obrigações assumidas;

7.3.14. Seguir as normas e políticas de segurança do CONTRATANTE;

7.3.15. Entregar o objeto contratados no prazo estabelecido, abstendo-se a parcelar a entrega do objeto para além desse prazo;

7.3.16. Entregar o objeto no local indicado pelo CONTRATANTE.

7.3.17. Cumprir com os termos estabelecidos neste Termo de Referência no que se refere à confidencialidade, ao sigilo e à segurança das informações.

7.4**.** JUSTIFICATIVA PARA VEDAÇÃO DA SUBCONTRATAÇÃO DO OBJETO

7.4.1. Não será permitida a subcontratação de qualquer parcela do objeto da presente dispensa, uma vez que, em pesquisa ao mercado, foi constatado que o fornecimento pretendido pode ser fornecido na sua integralidade por qualquer empresa do ramo, sem que se demande especialização, concentração de mercado ou racionalização de atividades que inviabilizem tal execução. Ademais, neste caso, a subcontratação não se mostra vantajosa técnica e economicamente para a Administração Pública.

7.5**.** MODELO DE GESTÃO DO CONTRATO

7.5.1. A execução contratual será acompanhada e fiscalizada pelo órgão Contratante, devendo a CONTRATADA fornecer todas as informações solicitadas no prazo máximo de 05 (cinco) dias úteis após o recebimento da solicitação.

7.5.2. As obrigações dos agentes responsáveis pela gestão e fiscalização da presente contratação estão detalhadas no Decreto Estadual nº 51.651/2021.

7.5.3. A comunicação entre a Contratante e a Contratada se dará por meio de e-mail: nsi@seplag.pe.gov.br, sem prejuízo de outros meios disponíveis.

7.5.4. A contratada deverá apresentar a Nota Fiscal ou fatura para atesto da Administração no seguinte endereço: Rua da Aurora nº 1377- Santo Amaro – Recife/PE. CEP nº 50040090

8. DOS CRITÉRIOS E PRAZOS PARA PAGAMENTO

8.1. O empenhamento somente será efetuado, e consequentemente paga a despesa, na forma prevista neste termo de referência, se a contratada estiver inscrita no CADASTRO DE FORNECEDORES DO ESTADO DE PERNAMBUCO – CADFOR.

8.2. O pagamento deverá ser efetuado à Contratada, em até 30 (trinta) dias corridos, à vista de termo de recebimento definitivo dos bens ou de recibo, conforme o caso, acompanhado da apresentação de Nota Fiscal / fatura discriminativa, devidamente atestada pelo servidor competente.

8.3. Nos casos de eventuais atrasos de pagamento, verificados por culpa única e exclusiva da CONTRATANTE, fica convencionado que a taxa de atualização financeira, devida pela Contratante entre o prazo referido no item anterior e o correspondente ao efetivo adimplemento da parcela, será calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP

Onde:

EM = Encargos Moratórios

N = Número de dias entre a data prevista para pagamento e a do efetivo pagamento

VP = Valor da parcela a ser paga

I = Índice de atualização financeira. Assim apurado:

I =(TX/100) 365 TX = Índice Nacional de Preços ao Consumidor Amplo – IPCA

8.4. A atualização financeira prevista nesta condição será incluída na Nota Fiscal/Fatura do mês seguinte ao da ocorrência.

8.5. Nenhum pagamento será efetuado à Contratada, cuja situação junto ao Cadastro de Fornecedores do Estado de Pernambuco esteja irregular e enquanto pendente de liquidação ou qualquer obrigação financeira que lhe for imposta, em virtude de penalidade.

8.6. A Contratada é responsável pelos pagamentos de quaisquer tributos, sejam eles sociais, trabalhistas, previdenciários, fiscais, comerciais ou de qualquer outra natureza resultantes da execução do contrato.

8.7. A CONTRATANTE solicitará à CONTRATADA, na hipótese de glosas e/ou incorreções de valores, a correspondente retificação objetivando a emissão da nota fiscal/fatura.

9. DAS SANÇÕES

9.1. Comete infração administrativa, nos termos do art. 155 da Lei nº 14.133/2021, o PROPONENTE e o CONTRATADO que:

9.1.1. Der causa à inexecução parcial do contrato;

9.1.2. Der causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

9.1.3. Der causa à inexecução total do contrato;

9.1.4. Deixar de entregar a documentação exigida para a dispensa;

9.1.5. Não mantiver a proposta, salvo em decorrência de fato superveniente devidamente justificado;

9.1.6. Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

9.1.7. Ensejar o retardamento da execução ou da entrega do objeto da dispensa sem motivo justificado;

9.1.8. Apresentar declaração ou documentação falsa exigida para a dispensa ou prestar declaração falsa durante a dispensa ou a execução do contrato;

9.1.9. Fraudar a dispensa ou praticar ato fraudulento na execução do contrato;

9.1.10. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

9.1.11. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de

participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores/prestadores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances;

9.1.12. Praticar atos ilícitos com vistas a frustrar os objetivos da dispensa;

9.1.13. Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013;

9.2. Ao PROPONENTE e ao CONTRATADO, que cometer qualquer das infrações discriminadas no subitem anterior ficarão sujeitos, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

I. Advertência pela falta do subitem 9.1.1 desta contratação direta, quando não se justificar a imposição de penalidade mais grave;

II. Multa de 10% (dez por cento) sobre o valor do(s) item(s) prejudicado(s) pela conduta do fornecedor/prestador, por qualquer das infrações dos subitens 9.1.1 a 9.1.12;

III. Impedimento de licitar e contratar com o Estado de Pernambuco e descredenciamento do CADFOR-PE, pelo prazo máximo de 3 (três) anos, nos casos dos subitens 9.1.2 a 9.1.7, quando não se justificar a imposição de penalidade mais grave;

IV. Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 9.1.8 a 9.1.12, bem como nos demais casos que justifiquem a imposição da penalidade mais grave.

9.3. Na aplicação das sanções serão considerados:

9.3.1. A natureza e a gravidade da infração cometida;

9.3.2. As peculiaridades do caso concreto;

9.3.3. As circunstâncias agravantes ou atenuantes;

9.3.4. Os danos que dela provierem para a Administração Pública;

9.3.5. A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle;

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

9.3.7. A aplicação das sanções, em hipótese alguma, exime a obrigação de reparação integral do dano causado à Administração Pública;

9.3.8. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções;

9.3.9. Havendo indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013 (Lei Anticorrupção) como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente para apuração da conduta típica em questão;

9.3.10. Nenhuma penalidade será aplicada sem o devido Processo Administrativo de Aplicação de Penalidade - PAAP, que assegurará o contraditório e a ampla defesa ao fornecedor/prestador, observando-se o procedimento previsto na Lei nº 14.133/2021 e no Decreto Estadual nº 42.191, de 1º de outubro de 2015.

10. DAS DEMAIS CONDIÇÕES NECESSÁRIAS AO FORNECIMENTO

10.1. O prazo de garantia do objeto deverá ser de, no mínimo 36 (trinta e seis) meses contados a partir do primeiro dia útil subsequente à data do recebimento do objeto.

10.2. O fornecedor das licenças deverá possuir assistência técnica na cidade do Recife/PE, para eventuais problemas que venham a ser observados durante o período da garantia mínima de 36 (trinta e seis) meses.

10.3. A proposta deverá indicar o fabricante e modelo/versão da solução, de modo que estará vinculada ao fornecimento do referido objeto, não sendo aceita a substituição por modelos em desconformidade com este TR;

10.4. A proposta de preços deverá ser elaborada de acordo com as especificações contidas neste Termo de Referência;

10.5. No preço total do objeto deverão estar inclusos todos os tributos (impostos, taxas e contribuições), sejam federais, estaduais e municipais, bem como frete, comissões, pessoal, embalagem, seguros, encargos sociais e trabalhistas, assim como demais insumos inerentes que incidam ou venham a incidir sobre o objeto, sejam de que naturezas forem.

ANEXOS DO TERMO DE REFERÊNCIA:

Anexo A - Modelo de Proposta

Anexo B – Modelo de Ordem de Fornecimento

Anexo C – Declarações complementares

ANEXO A
MODELO DE PROPOSTA

À

Secretaria _____

Prezados Senhores,

Apresentamos e submetemos à apreciação de V.Sas, nossa Proposta de Preços, para o objeto da presente dispensa, de acordo com as exigências estabelecidas no termo de referência e seus anexos e de acordo com a planilha abaixo detalhada:

Item	Código E-Fisco	Descrição	Unidade	Quantidade (A)	Valor Unitário (B)	Valor Total (C) = (A) x (B)
1					R$	R$
2					R$	R$
VALOR TOTAL				R$		

VALOR GLOBAL DA PROPOSTA: R$ _____ (_____).

VALIDADE DA PROPOSTA: _____ (_____) dias, contados da data da sua apresentação.

DECLARAMOS QUE ESTAMOS DE ACORDO COM TODAS AS CONDIÇÕES ESTABELECIDAS NO TERMO DE REFERÊNCIA E SEUS ANEXOS.

Local, _____ de _____ de 202___

Nome

Assinatura

Cargo

ANEXO B

MODELO DE ORDEM DE FORNECIMENTO

Referente à NOTA DE EMPENHO n° _____

OBJETO:

Item	Material	CÓDIGO DO E-FISCO	Quantidade (Unidade de Fornecimento)
01			
02			
03			
(...)			

VALOR:

PRAZO DE ENTREGA:

LOCAL E HORÁRIO DE ENTREGA:

SERVIDOR DESIGNADO PARA RECEBIMENTO:

Os bens deverão ser entregues em conformidade com as especificações técnicas e demais condições exigidas no Termo de Referência.

Integram este instrumento o termo de referência e seus Anexos, bem como a Proposta apresentada, independentemente de transcrição.

OBSERVAÇÃO PGE: No caso de fornecimento com entrega imediata em que o instrumento de contrato é dispensado, as infrações e sanções devem ser reproduzidas na Ordem de Fornecimento, no que couber.

Local, data.

Assinatura do servidor responsável

ANEXO C

DECLARAÇÃO QUE NÃO EMPREGA MENOR

A empresa _____ , inscrita no CNPJ sob o nº _____ , sediada _____, por intermédio do seu representante legal o(a) Sr(a) _____, sob as penais da lei:

DECLARA que cumpre o disposto no inciso XXXIII do art. 7º da Constituição Federal.

Recife, ___ de _____ de 2025

_____

REPRESENTANTE DA EMPRESA

CNPJ _____

João Rodrigo Teixeira de Souza Coutinho

Superintendente de TI

Documento assinado eletronicamente por **João Rodrigo Teixeira de Souza Coutinho**, em 05/05/2025, às 15:20, conforme horário oficial de Recife, com fundamento no art. 10º, do Decreto nº 45.157, de 23 de outubro de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.pe.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **66424993** e o código CRC **382BEFB3**.