Processo nº: 8331/2023

Fls:_____ Rubrica:_____

TERMO DE REFERÊNCIA

IDENTIFICAÇÃO DO DEMANDANTE:

Solicitação feita pela Secretaria Municipal de Gestão, Inovação e Tecnologia, localizada na Rua Coronel Madureira, n° 77 – Centro – Saquarema - RJ, CEP 28990-756.

1. DO OBJETO

1.1. O presente Termo de Referência tem por finalidade fornecer elementos necessários e suficientes para realização de procedimento licitatório visando formalizar ata de registro de preços (ARP) para a **CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NO FORNECIMENTO, POR SUBSCRIÇÃO DE SOLUÇÃO DE PROTEÇÃO, DETECÇÃO E RESPOSTA A INCIDENTE DE ENDPOINT PARA A PROTEÇÃO E SEGURANÇA DE DADOS E INFORMAÇÕES DOS COMPUTADORES DA PREFEITURA MUNICIPAL DE SAQUAREMA, INCLUINDO ATUALIZAÇÕES, GARANTIA E SUPORTE TÉCNICO, PELO PERÍODO DE 36 (TRINTA E SEIS) MESES**, conforme especificações técnicas, quantidades e demais condições constantes neste Termo de Referência.

1.2. A natureza do objeto a ser contratado é de **serviço comum** cujo padrão de desempenho e qualidade pode ser aferido por especificações usuais de mercado, enquadrando-se, portanto, nos termos do parágrafo único, do artigo 1º da Lei 10.520/2002.

1.3. Trata-se de **serviço contínuo**, sem dedicação de mão de obra exclusiva, essencial para manter o funcionamento das atividades finalísticas da Prefeitura Municipal de Saquarema, de modo que sua interrupção comprometerá a prestação de serviço público do Município e pelo fato de eventual paralisação da atividade contratada implicar em prejuízo ao exercício das atividades da Administração, conforme art. 15, da Instrução Normativa SEGES/MP nº 5/2017, transcrito abaixo:

> *"Art. 15. Os serviços prestados de forma contínua são aqueles que, pela sua essencialidade, visam atender à necessidade pública de forma permanente e contínua, por mais de um exercício financeiro, assegurando a integridade do patrimônio público ou o funcionamento das atividades finalísticas do órgão ou entidade, de modo que sua interrupção possa comprometer a prestação de um serviço público ou o cumprimento da missão institucional. "*

1.3.1. O caráter contínuo se deve ao fato da necessidade de pleno funcionamento da solução, destinados a atender as necessidades e segurança do Município.

1.4. Os serviços deverão ser executados observando-se todo o regramento legal relativo ao tema de que trata a Lei nº 13.709/2018, incluindo normas técnicas, demais instrumentos normativos e regulamentações posteriores da Autoridade Nacional de Proteção de Dados.

1.5. **Bens e serviços que compõem a solução:**

ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QUANTIDADE PARA REGISTRO
01	**SOLUÇÃO DE PROTEÇÃO, DETECÇÃO E RESPOSTA A INCIDENTE DE ENDPOINT**, subscrição pelo período de 36 (trinta e seis) meses, em sua versão mais recente, incluindo atualizações, garantia e suporte técnico durante todo o período, conforme descritivo técnico constante no item 3 do Termo de Referência.	Licenças (subscrição)	3.500

1.5.1. O serviço compreende as atividades de planejamento, instalação, configuração da solução nos ambientes de produção e testes da CONTRATANTE, migração e operação assistida.

1.5.2. A CONTRATADA deverá apoiar a equipe técnica da CONTRATANTE na customização e uso do software no conhecimento da arquitetura e de suas funcionalidades, esclarecendo dúvidas a respeito de configurações, ajustes (tuning) e segurança. (suporte técnico).

1.5.3. Subscrição – É um dos modelos mais tradicionais de comercialização de licença de software, na qual a solução não é comercializada como um ativo (exemplo, licença perpétua) e sim como um serviço. O usuário pode utilizar e atualizar a versão do software enquanto o contrato de subscrição estiver válido. Dependendo do contrato, após o vencimento, o usuário poderá continuar a utilizar o software (sem atualização de versão) ou não, de acordo com o termo de uso da subscrição.

1.5.4. Suporte de autoatendimento – Suporte com acesso às ferramentas de autoajuda oferecidas no suporte online, tais como informações sobre compatibilidade de produto, correções publicadas anteriormente, soluções alternativas, documentos informativos e outras soluções de produto.

1.5.5. Upgrade (Atualizações) - incluem revisões de Documentação, CORREÇÕES DE ERRO, PACOTES DE SERVIÇO, VERSÕES e RELEASES do software para o qual é fornecido o SUPORTE TÉCNICO, e não incluem opções ou produtos que sejam licenciados separadamente.

1.5.5.1. Tais Atualizações poderão ser denominadas como “atualizações de produto” ou “atualizações de software”.

1.5.6. O treinamento deverá ser ministrado de forma remota, ao vivo, em turma fechada para a CONTRATANTE, utilizando ferramenta de videoconferência que permita a participação e interação dos participantes, sendo de responsabilidade da CONTRATADA o fornecimento de toda a infraestrutura de videoconferência ou Webconferência necessária para o instrutor.

1.5.6.1. O treinamento deverá contemplar a instalação, customização, operação e administração da solução de Antivírus para 4 (quatro) especialistas da CONTRATANTE.

1.5.6.2. A CONTRATADA deverá disponibilizar um laboratório para realização do treinamento, com acesso via INTERNET. Os recursos de infraestrutura (hardware e software) do laboratório e o local de instalação serão de responsabilidade da CONTRATADA. O data center da CONTRATANTE não poderá ser utilizado nesta atividade.

1.5.6.3. A CONTRATADA poderá realizar o treinamento de forma presencial, em Saquarema, em comum acordo, desde que sem ônus adicional para a CONTRATANTE.

1.5.6.4. Todo treinamento será executado em idioma Português do Brasil

1.5.6.5. Definição das datas e horários em que ocorrerão os treinamentos serão acordados entre a CONTRATANTE e a CONTRATADA, sendo que deverão ocorrer obrigatoriamente em dias úteis, no horário comercial de 09:00 horas às 17:00 horas.

1.5.6.6. O conteúdo dos cursos de treinamento deverá abranger, minimamente, os seguintes tópicos:

1.5.6.6.1. Configuração – acesso e navegação na solução; comando de configurações básicas e avançadas, para implantação e operação do software nos ambientes desktop Windows.

2. DAS JUSTIFICATIVAS

2.1. No âmbito desta Administração Municipal, as atividades administrativas são amparadas fortemente no uso de soluções de TI - equipamentos, softwares e sistemas de informação - que se tornaram vitais para o funcionamento e melhoria dos serviços prestados aos Usuários, Munícipes e Contribuintes. Como consequência, a proteção do ambiente tornou-se fator essencial para manutenção da disponibilidade e estabilidade dos serviços de TI e do funcionamento da Administração Pública, bem como para manutenção da confidencialidade, integridade, disponibilidade e autenticidade dos dados.

2.2. O uso de soluções de TI na Administração Municipal provocou uma mudança significativa nos processos internos de trabalho e contribuiu para aumentar a celeridade e produtividade na prestação dos serviços, bem como assegurou o amplo acesso aos diversos serviços. Atualmente são disponibilizados por meio da rede mundial de computadores, tanto para o público interno como externo, diversos sistemas e serviços acessíveis por dispositivos como computadores, tablets ou celulares.

2.3. Para mitigar os riscos de invasão e contaminação dos sistemas informatizados, há no mercado soluções que atuam diretamente no gerenciamento e proteção de estações de trabalho, servidores e dispositivos móveis.

2.4. Dessa forma, faz-se necessário contratar a subscrição de licença do software com suporte técnico da solução de forma a assegurar a atualização do produto e das listas de definição de ameaças para reduzir vulnerabilidades e assegurar a confidencialidade e integridade dos dados tratados pela CONTRATANTE.

2.5. **Resultados e benefícios a serem alcançados**

2.5.1. Maximizar a disponibilidade dos serviços de TI oferecidos pela Administração Municipal.

2.5.2. Minimizar a probabilidade de ocorrência de incidentes em sistemas.

2.5.3. Melhor aproveitamento de recursos de tecnologia da informação com a otimização da infraestrutura.

2.5.4. Manutenção de índices de satisfação dos clientes internos e externos com os serviços e sistemas de TI.

2.5.5. Atendimento de objetivos estratégicos da Administração Municipal.

3. DAS ESPECIFICAÇÕES TÉCNICAS DETALHADAS DO OBJETO

3.1. SOLUÇÃO DE PROTEÇÃO, DETECÇÃO E RESPOSTA A INCIDENTE DE ENDPOINT

3.1.1. Subscrição pelo período de 36 (trinta e seis) meses, em sua versão mais recente, incluindo atualizações e suporte técnico durante todo o período.

3.1.2. FUNCIONALIDADES PARA SERVIDOR DE ADMINISTRAÇÃO E CONSOLE GERENCIAMENTO

3.1.2.1. Deve ser compatível com:

3.1.2.1.1. Microsoft Storage Server 2012 e Server R2 x64;

3.1.2.1.2. Microsoft Windows Server 2012 e R2 Standard / Core / Datacenter x64;

3.1.2.1.3. Microsoft Windows Server 2016 Standard / Core / Datacenter x64;

3.1.2.1.4. Microsoft Windows Server 2019 Standard / Core / Datacenter x64;

3.1.2.1.5. Microsoft Windows Server 2022 Standard / Core / Datacenter x64;

3.1.2.1.6. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;

3.1.2.1.7. Microsoft Windows 8 Professional / Enterprise x64;

3.1.2.1.8. Microsoft Windows 8.1 Professional / Enterprise x32/x64;

3.1.2.1.9. Microsoft Windows 10 x32/x64;

3.1.2.1.10. Windows 11 Home / Pro / Enterprise / Education x64.

3.1.2.2. Deve suportar as seguintes plataformas virtuais:

3.1.2.2.1. Vmware: Workstation 16 Pro, vSphere 6.7, vSphere 7.0;

3.1.2.2.2. Microsoft Hyper-V: 2012, 2012 R2, 2016, 2019 x64 e 2022 x64;

3.1.2.2.3. Parallels Desktop 17;

3.1.2.2.4. Citrix XenServer 7.1, 8.x;

3.1.2.2.5. Oracle VM VirtualBox 6.

3.1.2.3. Deve possuir as seguintes características:

3.1.2.3.1. A console deve ser acessada via WEB (HTTPS) ou MMC;

3.1.2.3.2. A console deve suportar arquitetura on-premise e arquitetura cloud-based;

3.1.2.3.3. Console deve ser baseada no modelo cliente/servidor;

3.1.2.3.4. A console deve suportar autenticação de dois fatores;

3.1.2.3.5. Deve possuir compatibilidade com Windows Failover Clustering;

3.1.2.3.6. O servidor de administração deve possui modelo de cluster ativo-passivo;

3.1.2.3.7. Deve permitir a atribuição de perfis para os administradores da solução de Antivírus;

3.1.2.3.8. Deve permitir incluir usuários do AD para logarem na console de administração

3.1.2.3.9. Console deve ser totalmente integrada com suas funções e módulos, caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, gerenciamento de vulnerabilidades, detecção e resposta de endpoint, avaliação de vulnerabilidades, gerenciamento de dispositivos moveis;

3.1.2.3.10. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;

3.1.2.3.11. Deverá ser possível buscar novos produtos e soluções a partir da console;

3.1.2.3.12. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;

3.1.2.3.13. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, através da console de gerenciamento e GPO de AD.

3.1.2.3.14. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

3.1.2.3.15. Deve armazenar histórico das alterações feitas em políticas;

3.1.2.3.16. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;

3.1.2.3.17. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;

3.1.2.3.18. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

3.1.2.3.19. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;

3.1.2.3.20. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

3.1.2.3.21. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por sub-rede com os seguintes parâmetros: KB/s e horário;

3.1.2.3.22. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;

3.1.2.3.23. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;

3.1.2.3.24. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;

3.1.2.3.25. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;

3.1.2.3.26. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

3.1.2.3.27. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;

3.1.2.3.28. A comunicação entre o cliente e o servidor de administração deve ser criptografada;

3.1.2.3.29. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

3.1.2.3.30. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

- Nome do computador;
- Nome do domínio;
- Range de IP;
- Sistema Operacional;
- Máquina virtual.

3.1.2.3.31. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

3.1.2.3.32. Deve ter a capacidade de descobrir novos dispositivos na rede, utilizando as seguintes técnicas:

- Pesquisa de rede (Windows pooling);
- Pesquisa ativa do AD (AD pooling);
- Pesquisa de IP (IP pooling);
- Pesquisa de rede (Zeroconf pooling);

3.1.2.3.33. Deve permitir, por meio da console de gerenciamento, extrair um artefato em área de backup de um cliente sem a necessidade de um servidor ou console de quarentena adicional;

3.1.2.3.34. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;

3.1.2.3.35. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;

3.1.2.3.36. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

3.1.2.3.37. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc;

3.1.2.3.38. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;

3.1.2.3.39. Deve fornecer as seguintes informações dos computadores:

- Se o antivírus está instalado;
- Se o antivírus está iniciado;
- Se o antivírus está atualizado;
- Minutos/horas desde a última conexão da máquina com o servidor administrativo;
- Minutos/horas desde a última atualização de vacinas;
- Data e horário da última verificação executada na máquina;
- Versão do antivírus instalado na máquina;
- Se é necessário reiniciar o computador para aplicar mudanças;
- Quantidade de vírus encontrados (contador) na máquina;
- Nome do computador;
- Domínio ou grupo de trabalho do computador;
- Data e horário da última atualização de vacinas;
- Sistema operacional com Service Pack;
- Quantidade de processadores;

- Quantidade de memória RAM;

- Sessões de usuários, com informações de contato (caso disponíveis no Active Directory);

- Endereço IP;

- Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;

- Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD e placa mãe;

- Vulnerabilidades de aplicativos instalados na máquina;

3.1.2.3.40. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;

3.1.2.3.41. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

- Alteração de Gateway Padrão;

- Alteração de subrede;

- Alteração de domínio;

- Alteração de servidor DHCP;

- Alteração de servidor DNS;

- Alteração de servidor WINS;

- Resolução de Nome;

- Disponibilidade de endereço de conexão SSL;

3.1.2.3.42. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

3.1.2.3.43. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;

3.1.2.3.44. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;

3.1.2.3.45. A console de gerenciamento deve suportar funções de controle de acesso com base na função (RBAC) para a hierarquia de servidores;

3.1.2.3.46. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;

3.1.2.3.47. Capacidade de herança de configuração de tarefas, políticas e relatórios na estrutura de hierarquia de servidores on-premisse com servidor em cloud.

3.1.2.3.48. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;

3.1.2.3.49. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;

3.1.2.3.50. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;

3.1.2.3.51. Capacidade de monitoramento do sistema através de um SNMP client;

3.1.2.3.52. Capacidade enviar eventos através de protocolo de syslog;

3.1.2.3.53. Capacidade exportar eventos para sistemas de SIEM no formato LEEF e CEF.

3.1.2.3.54. Deve ser capas de enviar os eventos para sistemas de SIEM em canal encriptado.

3.1.2.3.55. Dever ter a capacidade de exportar eventos para sistemas de SIEM, compatível com Qradar, ArcSight e Splunk.

3.1.2.3.56. Capacidade de enviar e-mails para contas específicas em caso de algum evento;

3.1.2.3.57. Listar em um único local, todos os computadores não gerenciados na rede;

3.1.2.3.58. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;

3.1.2.3.59. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente

3.1.2.3.60. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;

3.1.2.3.61. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);

3.1.2.3.62. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo, porém sem comprometer o desempenho do computador;

3.1.2.3.63. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);

3.1.2.3.64. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;

3.1.2.3.65. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

3.1.2.3.66. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

- Nome do vírus;
- Nome do arquivo infectado;

- Data e hora da detecção;
- Nome da máquina ou endereço IP;
- Ação realizada.

3.1.2.3.67. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

3.1.2.3.68. Capacidade de listar updates nas máquinas com o respectivo link para download;

3.1.2.3.69. Deve criar um backup de todos arquivos deletados em computadores durante a desinfecção para que possam ser restaurados;

3.1.2.3.70. Deve ter uma área de backup na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;

3.1.2.3.71. Capacidade de realizar resumo de hardware de cada máquina cliente;

3.1.2.3.72. Capacidade de diferenciar máquinas virtuais de máquinas físicas

3.1.3. FUNCIONALIDADES PARA SISTEMAS OPERACIONAIS WINDOWS

3.1.3.1. Deve ser compatível com os seguintes sistemas de estação de trabalho:

3.1.3.1.1. Microsoft Windows 7 Home/Professional/Enterprise/Ultimate SP1;

3.1.3.1.2. Microsoft Windows 8 Professional/Enterprise;

3.1.3.1.3. Microsoft Windows 8.1 Professional / Enterprise;

3.1.3.1.4. Microsoft Windows 10 Pro / Enterprise / Home / Education;

3.1.3.1.5. Microsoft Windows 11 Pro / Enterprise / Home / Education.

3.1.3.2. Deve ser compatível com os seguintes sistemas servidores:

3.1.3.2.1. Windows Small Business Server 2011 Essentials / Standard (64-bit);

3.1.3.2.2. Windows MultiPoint Server 2011 (64-bit);

3.1.3.2.3. Windows Server 2008 R2 Standard/Enterprise/Datacenter SP 1 e superior;

3.1.3.2.4. Windows Server 2012 e R2 Foundation / Essentials / Standard / Datacenter;

3.1.3.2.5. Windows Server 2016 Essentials / Standard / Datacenter;

3.1.3.2.6. Windows Server 2019 Essentials / Standard / Datacenter;

3.1.3.2.7. Windows Server 2022.

3.1.3.3. Deve suportar as seguintes plataformas virtuais:

3.1.3.3.1. Vmware Workstation 16.2.3;

3.1.3.3.2. Vmware ESXi 7.0 Update 3d;

3.1.3.3.3. Microsoft Hyper-V Server 2019;

3.1.3.3.4. Citrix Virtual Apps and Desktops 7 2203;

3.1.3.3.5. Critrix Provisioning 2203;

3.1.3.3.6. Citrix Hypervisor 8.2.

3.1.3.4. Deve possuir as seguintes características:

3.1.3.4.1. Deve prover as seguintes proteções:

- Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
- Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
- O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
- Deve possui modulo dedicado contra prevenção de intrusão, Prevenção de intrusão do host;
- Autoproteção (contra-ataques aos serviços/processos do antivírus);

- Controle de dispositivos externos;
- Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;
- Controle de acesso a sites por horário;
- Controle de acesso a sites por usuários;
- Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de vídeo e áudio;
- Controle de execução de aplicativos;
- Controle de vulnerabilidades do Windows e dos aplicativos instalados;

3.1.3.4.2. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

3.1.3.4.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

3.1.3.4.4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

3.1.3.4.5. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

3.1.3.4.6. Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;

3.1.3.4.7. Deverá possuir módulo dedicado para proteção contra port scanning;

3.1.3.4.8. Deverá possuir módulo dedicado para proteção contra network flooding;

3.1.3.4.9. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

3.1.3.4.10. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

3.1.3.4.11. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

3.1.3.4.12. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;

3.1.3.4.13. Deverá possuir módulo para proteção contra malwares que tenta realizar criptografia de arquivos em pastas compartilhadas.

3.1.3.4.14. Deve ter a capacidade de detectar ameaças instaladas na BIOS ROM do endpoint.

3.1.3.4.15. Deverá realizar scanner de firmaware em busca de rootkits.

3.1.3.4.16. Ao detectar uma ameaça, a solução deve exibir informações:

3.1.3.4.17. Do objeto SHA256;

3.1.3.4.18. Do objeto MD5.

3.1.3.4.19. Capacidade de verificar somente arquivos novos e alterados;

3.1.3.4.20. Capacidade de verificar objetos usando heurística;

3.1.3.4.21. Capacidade de agendar uma pausa na verificação;

3.1.3.4.22. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;

3.1.3.4.23. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

3.1.3.4.24. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

- Perguntar o que fazer, ou;
- Bloquear acesso ao objeto;

- Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

- Caso positivo de desinfecção:

o Restaurar o objeto para uso;

- Caso negativo de desinfecção:

o Mover para uma área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

3.1.3.4.25. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

3.1.3.4.26. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI;

3.1.3.4.27. Capacidade de verificar links inseridos em e-mails contra phishings;

3.1.3.4.28. Capacidade de verificar todo o tráfego web de acessos à internet nos protocolos HTTP, HTTPS e FTP, utilizando técnicas de banco de dados, serviços da nuvem do fabricante e analise de heurística bloqueado arquivos, sites de phishing e URL maliciosas;

3.1.3.4.29. Capacidade de verificação de corpo e anexos de e-mails usando heurística;

3.1.3.4.30. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

- Perguntar o que fazer, ou;

- Bloquear o e-mail;

- Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

- Caso positivo de desinfecção:

o Restaurar o e-mail para o usuário;

- Caso negativo de desinfecção:

- Mover para uma área de backup ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

3.1.3.4.31. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;

3.1.3.4.32. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;

3.1.3.4.33. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc);

3.1.3.4.34. Deve ser possível realizar o monitoramento das atividades de rede em tempo real, visualizando portas UDP/TCP e Trafego de rede por aplicativo.

3.1.3.4.35. Capacidade de alterar as portas monitoradas pelos módulos de ameaças web, controle de acesso à web e e-mail;

3.1.3.4.36. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

- Perguntar o que fazer, ou;
- Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
- Permitir acesso ao objeto;

3.1.3.4.37. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

- Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;
- Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;

3.1.3.4.38. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;

3.1.3.4.39. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências

características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

3.1.3.4.40. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;

3.1.3.4.41. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/);

3.1.3.4.42. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;

3.1.3.4.43. Deve possuir módulo para proteção contra port scans, network flooding e MAC spoofing. A base de dados de análise deve ser atualizada juntamente com as vacinas;

3.1.3.4.44. Deve permitir a importação e exportação de listas de regras e exclusões para as aplicações no formato XML;

3.1.3.4.45. Deve permitir a criação de zonas confiáveis locais independentes por parte do usuário.

3.1.3.4.46. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

- Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

- Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

3.1.3.4.47. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

- Discos de armazenamento locais;

- Armazenamento removível;

- Impressoras;

- CD/DVD;
- Drives de disquete;
- Modems;
- Dispositivos de fita;
- Dispositivos multifuncionais;
- Leitores de smart card;
- Wi-Fi;
- Adaptadores de rede externos;
- Dispositivos MP3 ou smartphones;
- Dispositivos Bluetooth;
- Câmeras e Scanners.

3.1.3.4.48. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;

3.1.3.4.49. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;

3.1.3.4.50. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;

3.1.3.4.51. Deve permitir controlar o acesso a dispositivos externos com base em prioridade de regras.

3.1.3.4.52. Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc.

3.1.3.4.53. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;

3.1.3.4.54. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo,

fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);

3.1.3.4.55. Ter a capacidade de detectar a modificação de firmware em dispositivos USB mal-intencionado.

3.1.3.4.56. Deverá realizar a validação dos dispositivos que se conectam via USB que emulam teclados;

3.1.3.4.57. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

- Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

- White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

3.1.3.4.58. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

3.1.3.4.59. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;

3.1.3.4.60. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;

3.1.3.4.61. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

3.1.3.4.62. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.

3.1.3.4.63. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

3.1.3.4.64. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

3.1.3.4.65. Capacidade de integração com a Antimalware Scan Interface (AMSI).

3.1.3.4.66. Deve permitir realizar o gerenciamento por meio de integração via REST API.

3.1.3.4.67. Deve permitir o gerenciamento remoto da solução por meio de aplicativos de administração remota.

3.1.4. FUNCIONALIDADES PARA ESTAÇÕES DE TRABALHO MAC OS X

3.1.4.1. Deve ser compatível com:

3.1.4.1.1. macOS Mojave 10.14;

3.1.4.1.2. macOS Catalina 10.15;

3.1.4.1.3. macOS Big Sur 11.0;

3.1.4.1.4. macOS Monterey 12.

3.1.4.2. Deve possuir as seguintes características:

3.1.4.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

3.1.4.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possíbilidade de analisar endereços https;

3.1.4.2.3. Possuir módulo de bloqueio á ataques na rede;

3.1.4.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;

3.1.4.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;

3.1.4.2.6. Possibilidade de importar uma chave no pacote de instalação;

3.1.4.2.7. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

3.1.4.2.8. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

3.1.4.2.9. Capacidade de voltar para a base de dados de vacina anterior;

3.1.4.2.10. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

3.1.4.2.11. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

3.1.4.2.12. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

3.1.4.2.13. Capacidade de verificar somente arquivos novos e alterados;

3.1.4.2.14. Capacidade de verificar objetos usando heurística;

3.1.4.2.15. Capacidade de agendar uma pausa na verificação;

3.1.4.2.16. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

- Perguntar o que fazer, ou;
- Bloquear acesso ao objeto;
- Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
- Caso positivo de desinfecção:
  - Restaurar o objeto para uso;
- Caso negativo de desinfecção:

o Mover para área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

3.1.4.2.17. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

3.1.4.2.18. Capacidade de verificar arquivos de formato de e-mail;

3.1.4.2.19. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;

3.1.4.2.20. Capacidade de, através da mesma console central de gerenciamento:

- Ser instalado;
- Ser removido;
- Ser gerenciado;

3.1.5. FUNCIONALIDADES PARA SISTEMAS OPERACIONAIS LINUX

3.1.5.1. Deve ser compatível com:

3.1.5.1.1. Plataforma 32-bits:

- Red Hat Linux 6.7 e superior;
- CentOS 6.7 e superior;
- Debian 9.4 e superior;
- Debian 10.1 e superior;
- Debian 11.1 e superior;
- Linux Mint 19 e superior;
- Mageia 4;

3.1.5.1.2. Plataforma 64-bits:

- Ubuntu 18.04 e superior;
- Ubuntu 20.04;
- Red Hat Enterprise Linux 6.7;
- Red Hat Enterprise Linux 7.2;
- Red Hat Enterprise Linux 8.0;
- CentOS 6.7 e superior;
- CentOS 7.2 e superior;
- CentOS 8.0 e superior;
- Debian 9.4 e superior;
- Debian 10.1 e superior;
- OracleLinux 7.3 e superior;
- OracleLinux 8 e sueperior;
- SUSE Server 12 e superior
- SUSE Server 15 e superior;
- openSUSE Leap 15;
- Amazon Linux 2;
- Linux Mint 19 e superior;
- Linux Mint 20.1 e superior;
- Oracle Linux 7.3 e superior;
- Oracle Linux 8.0 e superior;
- RED OS 7.2.

3.1.5.2. Deve possuir as seguintes características:

3.1.5.2.1. Deve prover as seguintes proteções:

- 1.6.1.2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

3.1.5.2.2. Deve permitir gerenciamento, no mínimo, das seguintes formas:

- Via linha de comando;
- Via console administrativa;
- Via GUI;
- Via web (remotamente).

3.1.5.2.3. Deve possuir funcionalidade de scan de drives removíveis, tais como:

- CDs;
- DVDs;
- Discos blu-ray;
- Flash drives (pen drives);
- HDs externos;
- Disquetes;

3.1.5.2.4. Deve fornecer os seguintes controles para dispositivos externos conectados ao computador:

- Por tipo de dispositivo;
- Por barramento de conexão.

3.1.5.2.5. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

3.1.5.2.6. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

- Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
- Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
- Leitura de configurações;
- Modificação de configurações;
- Gerenciamento de Backup;
- Visualização de logs;
- Gerenciamento de logs;
- Gerenciamento de ativação da aplicação;
- Gerenciamento de permissões (adicionar/excluir permissões acima);

3.1.5.2.7. Capacidade de criar exclusões por local, máscara e nome da ameaça;

3.1.5.2.8. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

3.1.5.2.9. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

3.1.5.2.10. Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers;

3.1.5.2.11. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

- Alta;
- Média;
- Baixa;
- Recomendado;

3.1.5.2.12. Gerenciamento de backup de arquivos: Fazer backup de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de backup;

3.1.5.2.13. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

3.1.5.2.14. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

3.1.5.2.15. Capacidade de definir o consumo de recursos nas varreduras para não impactar outros aplicativos que necessitem de mais recursos de memória ou processamento;

3.1.5.2.16. Deverá ser possível priorizar a execução de tarefas;

3.1.5.2.17. Capacidade de verificar objetos usando heurística;

3.1.5.2.18. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em malicioso;

3.1.5.2.19. Deve fornecer análise de todo o tráfego HTTP/HTTPS/FTP;

3.1.5.2.20. O módulo de análise de tráfego deve fornecer os seguintes componentes de proteção:

- Detecção de phishing e sites maliciosos;
- Bloqueio de download de arquivos maliciosos;
- Bloqueio de adware;
- Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

3.1.5.2.21. Deve fornecer a possibilidade de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

3.1.5.2.22. Deverá fornecer informações de todas os executáveis das aplicações;

3.1.5.2.23. Deve possuir módulo de proteção contra criptografia maliciosa.

3.1.5.2.24. Deverá possuir controle de execução de aplicações;

3.1.5.2.25. O modulo de controle de aplicação deverá possuir as seguintes funcionalidades:

- Criação de lista de bloqueio de aplicação;
- Criação de lista de permissão de aplicação;

3.1.5.2.26. Deverá realizar busca de ameaças em setores críticos do sistema operacional:

- Setor de inicialização;
- Objetos de inicialização;
- Processos de memória;
- Memória do kernel;

3.1.6. FUNCIONALIDADES PARA COM SERVIDORES WINDOWS

3.1.6.1. Deve possuir compatibilidade com sistemas legados:

3.1.6.1.1. Plataforma x32 ou x64:

- Windows Server 2003 Standard/Enterprise/Datacenter SP2 e posterior;
- Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior;

3.1.6.2. Deve possuir as seguintes características:

3.1.6.2.1. Deve prover as seguintes proteções:

- Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- Autoproteção contra-ataques aos serviços/processos do antivírus;
- Firewall com IDS;
- Controle de vulnerabilidades do Windows e dos aplicativos instalados;

3.1.6.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

3.1.6.2.3. Deve permitir gerenciamento, no mínimo, das seguintes formas:

- Via console administrativa;
- Via web (remotamente);

3.1.6.2.4. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

3.1.6.2.5. Deverá ter a capacidade de customizar o uso de CPU para realização de scanner no dispositivo.

3.1.6.2.6. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

- Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
- Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
- Leitura de configurações;
- Modificação de configurações;
- Gerenciamento de backup;
- Visualização de logs;
- Gerenciamento de logs;
- Gerenciamento de ativação da aplicação;
- Gerenciamento de permissões (adicionar/excluir permissões acima);
- Deve possuir bloqueio de inicialização de aplicativos baseado em whitelists.

3.1.6.2.7. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

- Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

- Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

3.1.6.2.8. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;

3.1.6.2.9. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede

3.1.6.2.10. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);

3.1.6.2.11. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;

3.1.6.2.12. Deve possuir funcionalidade de análise personalizada de logs do Windows.

3.1.6.2.13. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;

3.1.6.2.14. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;

3.1.6.2.15. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;

3.1.6.2.16. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

3.1.6.2.17. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

3.1.6.2.18. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

3.1.6.2.19. Capacidade de verificar somente arquivos novos e alterados;

3.1.6.2.20. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);

3.1.6.2.21. Capacidade de verificar objetos usando heurística;

3.1.6.2.22. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

3.1.6.2.23. Capacidade de agendar uma pausa na verificação;

3.1.6.2.24. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

- Perguntar o que fazer, ou;
- Bloquear acesso ao objeto;
- Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
- Caso positivo de desinfecção:
  - Restaurar o objeto para uso;
- Caso negativo de desinfecção:
  - Mover para área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

3.1.6.2.25. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

3.1.6.2.26. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos malicioso em área de backup;

3.1.6.2.27. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

3.1.6.2.28. Em caso de detecção de sinais de uma infecção ativa, deve possuir capacidade de, automaticamente:

- Executar os procedimentos pré-configurados pelo administrador;

- Em caso de ausência de procedimentos pré-configurados, criar tais procedimentos e executá-los.

3.1.6.2.29. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

3.1.6.2.30. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros

3.1.6.2.31. Capacidade de detectar anomalias no comportamento de um software usando análise heurística.

3.1.6.2.32. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

3.1.6.2.33. Deve possuir controle de dispositivos externos.

3.1.7. FUNCIONALIDADES PARA SMARTPHONES E TABLETS

3.1.7.1. Deve ter a seguinte compatibilidade:

3.1.7.1.1. Suportar o Android das versões: 5.0 ao 12.

3.1.7.2. Deve possuir as seguintes características:

3.1.7.2.1. Deve prover as seguintes proteções:

3.1.7.2.2. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

- Proteção contra adware e autodialers;

- Todos os objetos transmitidos;

- Arquivos abertos no smartphone;

- Programas instalados usando a interface do smartphone

- Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;
- Deverá isolar em área de backup os arquivos infectados;
- Deverá atualizar as bases de vacinas de modo agendado;
- Capacidade de desativar por política:
  - Wi-fi;
  - Câmera;
  - Bluetooth.

3.1.7.2.3. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;

3.1.7.2.4. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;

3.1.7.2.5. Deverá ter firewall pessoal;

3.1.7.2.6. Capacidade de tirar fotos quando a senha for inserida incorretamente;

3.1.7.2.7. Capacidade de enviar comandos remotamente de:

3.1.7.2.8. Localizar;

3.1.7.2.9. Bloquear.

3.1.7.2.10. Capacidade de detectar Root nos dispositivos;

3.1.7.2.11. Capacidade de bloquear o acesso a site por categoria em dispositivos;

3.1.7.2.12. Capacidade de bloquear o acesso a sites phishing ou maliciosos;

3.1.7.2.13. Capacidade de configurar White e blacklist de aplicativos;

3.1.7.2.14. Capacidade de localizar o dispositivo quando necessário;

3.1.7.2.15. Permitir atualização das definições quando estiver em “roaming”;

3.1.7.2.16. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;

3.1.7.2.17. Capacidade de agendar uma verificação;

3.1.7.2.18. Capacidade de enviar URL de instalação por e-mail;

3.1.7.2.19. Capacidade de fazer a instalação do agente através de um link QRCode;

3.1.7.2.20. Capacidade de executar as seguintes ações caso a desinfecção falhe:

- Deletar;
- Ignorar;
- Fazer backup;
- Perguntar ao usuário.

3.1.8. FUNCIONALIDADES PARA GERENCIAMENTO DE DISPOSITIVOS MÓVEIS (MDM) - ANDROID

3.1.8.1. Deve possuir as seguintes compatibilidades:

3.1.8.1.1. Dispositivos com os sistemas operacionais:

- Do Android versão 5.0 a 12;

3.1.8.1.2. Deverá possuir integração com sistemas de gerenciamentos:

- VMWare AirWatch 9.3;
- MobileIron;
- IBM Maas360;
- Microsoft Intune;
- SOTI MobiControl;

3.1.8.2. Deve possuir as seguintes características:

3.1.8.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

3.1.8.2.2. Capacidade de ajustar as configurações de:

3.1.8.2.3. Sincronização de e-mail;

3.1.8.2.4. Uso de aplicativos;

3.1.8.2.5. Senha do usuário;

3.1.8.2.6. Criptografia de dados;

3.1.8.2.7. Conexão de mídia removível.

3.1.8.2.8. Capacidade de instalar certificados digitais em dispositivos móveis;

3.1.8.2.9. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;

3.1.8.2.10. Capacidade de desinstalar remotamente o antivírus do dispositivo;

3.1.8.2.11. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;

3.1.8.2.12. Capacidade de sincronizar com Samsung Knox;

3.1.9. FUNCIONALIDADES DE GERENCIAMENTO DE DISPOSITIVOS MÓVEIS (MDM) – IOS

3.1.9.1. Deve possuir as seguintes compatibilidades:

3.1.9.1.1. Ser compatível com dispositivos com os sistemas operacionais:

- iOS 10.0 – 10.3.3;
- iOS 11.0 – 11.3;
- iOS 12.0;
- iOS 13.0;
- IPadOS 13 ao 15;

3.1.9.2. Deve possuir as seguintes características:

3.1.9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

3.1.9.2.2. Capacidade de ajustar as configurações de:

3.1.9.2.3. Sincronização de e-mail;

3.1.9.2.4. Senha do usuário;

3.1.9.2.5. Criptografia de dados;

3.1.9.2.6. Capacidade de instalar certificados digitais em dispositivos móveis;

3.1.9.2.7. Capacidade de instalar as ferramentas necessárias para o gerenciamento dos dispositivos clientes através de:

- Link por e-mail;
- Link por mensagem de texto;
- QR Code.

3.1.9.2.8. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;

3.1.9.2.9. Capacidade de, remotamente, bloquear um dispositivo iOS;

3.1.10. FUNCIONALIDADES PARA CRIPTOGRAFIA

3.1.10.1. Deve ter compatibilidade com os seguintes sistemas operacionais:

3.1.10.1.1. Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;

3.1.10.1.2. Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;

3.1.10.1.3. Microsoft Windows 7 Professional SP1 ou superior x86/x64;

3.1.10.1.4. Microsoft Windows 8 Enterprise x86/x64;

3.1.10.1.5. Microsoft Windows 8 Pro x86/x64;

3.1.10.1.6. Microsoft Windows 8.1 Pro x86/x64;

3.1.10.1.7. Microsoft Windows 8.1 Enterprise x86/x64;

3.1.10.1.8. Microsoft Windows 10 Enterprise x86/x64;

3.1.10.1.9. Microsoft Windows 10 Pro x86/x64;

3.1.10.2. Deve possuir as seguintes características:

3.1.10.2.1. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;

3.1.10.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;

3.1.10.2.3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;

3.1.10.2.4. Capacidade de utilizar Single Sign-On para a autenticação de pré-boot;

3.1.10.2.5. Permitir criar vários usuários de autenticação pré-boot;

3.1.10.2.6. Deve permitir que o usuário monitore a criptografia do disco ou o processo de descriptografia em tempo real;

3.1.10.2.7. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;

3.1.10.2.8. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

3.1.10.2.9. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;

3.1.10.2.10. Criptografar todos os arquivos individualmente;

3.1.10.2.11. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

3.1.10.2.12. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

3.1.10.2.13. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente;

3.1.10.2.14. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;

3.1.10.2.15. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;

3.1.10.2.16. Verifica compatibilidade de hardware antes de aplicar a criptografia;

3.1.10.2.17. Possibilita estabelecer parâmetros para a senha de criptografia;

3.1.10.2.18. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

3.1.10.2.19. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo

3.1.10.2.20. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;

3.1.10.2.21. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;

3.1.10.2.22. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;

3.1.10.2.23. Permite criar um grupo de extensões de arquivos a serem criptografados;

3.1.10.2.24. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;

3.1.10.2.25. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.

3.1.10.2.26. Capacidade de deletar arquivos de forma segura após a criptografia;

3.1.10.2.27. Capacidade de criptografar somente o espaço em disco utilizado;

3.1.10.2.28. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;

3.1.10.2.29. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;

3.1.10.2.30. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;

3.1.10.2.31. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;

3.1.10.2.32. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;

3.1.10.2.33. Capacidade de fazer "Hardware encryption";

3.1.11. FUNCIONALIDADES DE GERENCIAMENTO DE SISTEMAS

3.1.11.1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal;

3.1.11.2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;

3.1.11.3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;

3.1.11.4. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;

3.1.11.5. Capacidade de gerenciar licenças de softwares de terceiros;

3.1.11.6. Capacidade de atualizar informações sobre hardware presentes nos relatórios após mudanças de hardware nas máquinas gerenciadas;

3.1.11.7. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc);

3.1.11.8. Possibilita fazer distribuição de software de forma manual e agendada;

3.1.11.9. Suporta modo de instalação silenciosa;

3.1.11.10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;

3.1.11.11. Possibilita fazer a distribuição através de agentes de atualização;

3.1.11.12. Utiliza tecnologia multicast para evitar tráfego na rede;

3.1.11.13. Possibilita criar um inventário centralizado de imagens;

3.1.11.14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;

3.1.11.15. Suporte a WakeOnLan para deploy de imagens;

3.1.11.16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;

3.1.11.17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;

3.1.11.18. Capacidade de gerar relatórios de vulnerabilidades e patches;

3.1.11.19. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;

3.1.11.20. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;

3.1.11.21. Permite baixar atualizações para o computador sem efetuar a instalação

3.1.11.22. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;

3.1.11.23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;

3.1.11.24. Permite selecionar produtos a serem atualizados pela console de gerenciamento;

3.1.11.25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;

3.1.11.26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;

3.1.11.27. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;

3.1.11.28. Capacidade de configurar o reinicio do computador após a aplicação das atualizações e correções de vulnerabilidades;

3.1.11.29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;

3.1.11.30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;

3.1.12. FUNCIONALIDADES DE DETECÇÃO E RESPOSTA

3.1.12.1. Deve ser compatível com os seguintes sistemas de estação de trabalho:

3.1.12.1.1. Microsoft Windows 7 Home/Professional/Enterprise/Ultimate SP1;

3.1.12.1.2. Microsoft Windows 8 Professional/Enterprise;

3.1.12.1.3. Microsoft Windows 8.1 Professional / Enterprise;

3.1.12.1.4. Microsoft Windows 10 Pro / Enterprise / Home / Education;

3.1.12.1.5. Microsoft Windows 11 Pro / Enterprise / Home / Education;

3.1.12.2. Deve ser compatível com os seguintes sistemas servidores:

3.1.12.2.1. Windows Small Business Server 2011 Essentials / Standard (64-bit)

3.1.12.2.2. Windows MultiPoint Server 2011 (64-bit);

3.1.12.2.3. Windows Server 2008 R2 Standard/Enterprise/Datacenter SP 1 e superior;

3.1.12.2.4. Windows Server 2012 e R2 Foundation / Essentials / Standard / Datacenter;

3.1.12.2.5. Windows Server 2016 Essentials / Standard / Datacenter;

3.1.12.2.6. Windows Server 2019 Essentials / Standard / Datacenter;

3.1.12.2.7. Windows Server 2022.

3.1.12.3. Deve possuir as seguintes características:

3.1.12.3.1. As funcionalidades relacionadas a detecção e resposta solicitadas nesse item, devem ser operadas na mesma console de gerenciamento da solução de endpoint;

3.1.12.3.2. A solução deve oferecer módulo focado em capacidades de EDR "Endpoint Detection and Response", incluindo no mínimo as seguintes capacidades:

3.1.12.3.3. O agente deve ter capacidade de coletar e processar dados relacionadas ao veredito e ao contexto da ameaça;

3.1.12.3.4. Deve fornecer graficamente a visualização da cadeia do ataque;

3.1.12.3.5. Deve possuir a capacidade de varredura, para identificar a presença de um artefato detectado em outros dispositivos na rede, através de indicadores de comprometimento (IoC).

3.1.12.3.6. A varredura deve oferecer opções de resposta automatizada (sem intervenção do administrador), para serem executadas caso o IoC seja encontrado em outro dispositivo, com no mínimo as seguintes opções:

- Isolar o host;
- Iniciar uma varredura nas áreas críticas;
- Quarentenar o objeto;

3.1.12.3.7. 13.1.2 A solução deve criar um report detalhado sobre o incidente, tendo a capacidade de incluir no mínimo os seguintes dados:

- Visibilidade das detecções provenientes de endpoint;
- Processos;
- Conexões remotas;

- Alterações de registros;
- Objetos baixados
- Capacidade de integração com a solução de sandbox cloud do fabricante;
- Varredura por todos os dispositivos executada a partir de indicador de comprometimento (IoC) gerado através da solução e importado pelo administrador.

3.1.12.3.8. Deverá possuir informações de assinaturas digitais da ameaça;

3.1.12.3.9. Deve ser capaz de trazer informações do arquivo sobre sua geolocalização;

3.1.12.3.10. Possibilidade de informar quando o arquivo foi detectado pela base de conhecimento;

3.1.12.3.11. Trazer a identificação de comportamento e/ou descrição sobre o arquivo;

3.1.12.3.12. A solução deve oferecer no mínimo as seguintes opções de resposta:

- Prevenir a execução de um arquivo;
- Quarentenar um arquivo;
- Iniciar uma varredura por IoC;
- Parar um processo;
- Executar um processo;
- Ferramenta que possibilite o isolamento do host infectado com no mínimo as características abaixo:

o A opção de isolamento deve estar disponível junto a visualização do incidente;

o Na análise do incidente a ferramenta deverá apresentar recomendações de ações que o analista precisa executar para remediar o incidente;

o As recomendações devem ser guiadas juntamente com guias das opções selecionadas pelo analista, apresentando pop-up guiando as ações.

3.1.12.3.13. Deverá ser possível remover a máquina do isolamento a partir do incidente;

3.1.12.3.14. Na configuração padrão, o isolamento deve ser feito de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra;

3.1.12.3.15. Deve oferecer informações de inteligência de ameaças do próprio fabricante;

3.1.12.3.16. Deverá possuir detecção baseada em sandbox do tipo cloud;

3.1.12.3.17. Deverá suportar IoC de terceiros em formatos OpenIOC;

3.1.13. **SUPORTE TÉCNICO**

3.1.14. O suporte técnico deverá ser disponibilizado pela CONTRATADA à CONTRATANTE a partir da assinatura do instrumento contratual e recebimento da ordem de início dos serviços.

3.1.15. Deverão ser informados à CONTRATANTE os contatos do suporte técnico relacionados à solução de antivírus contratada, prestados por meio dos canais: central de atendimento 0800, e-mail ou presencial (caso o problema não possa ser resolvido por meio eletrônico), em dias úteis, observando, no mínimo, o horário das 09:00h às 17:00h.

3.1.16. Após disponibilizado, o suporte técnico deverá permanecer disponível por todo o período de vigência contratual, apto a atender as dúvidas dos usuários da solução na CONTRATANTE, dúvidas e problemas relacionados às atualizações e correções da solução, além de eventuais problemas com o gerenciamento de licenças relacionados aos produtos adquiridos e mantidos.

3.1.17. Durante o período de vigência da licença da solução, a CONTRATADA deverá oferecer suporte técnico à equipe técnica da CONTRATANTE, formada por 5 (cinco) membros, quanto à gestão e uso das seguintes funcionalidades:

- Implementação de agentes
- Implementação de Endpoint e EDR
- Criação de políticas de gestão
- Criação de políticas de Segurança (EPP)
- Criação de políticas de EDR
- Tarefas de verificação de vulnerabilidades
- Tarefas de correção de pacotes de atualização ou vulnerabilidades
- Ativação e distribuição de licenças
- Ativação de avisos e notificações
- Relatórios de ameaças
- Fluxograma de incidentes
- Tratamento e mitigação de ameaças
- Tarefas de IOCs

- Atualização de recursos de segurança.

3.1.18. A CONTRATADA deve assegurar para que o atendimento do suporte técnico ocorra de forma compatível com a solução contratada pela CONTRATANTE.

3.1.19. Além do atendimento ilimitado, o Suporte deverá contar com prioridade no atendimento e o seu Tempo de Resposta deverá ser de até 8 horas úteis, que poderá ser realizado através Whatsapp, Microsoft Teams ou outra ferramenta disponibilizada pela CONTRATADA. Suas resoluções de chamados serão realizadas remotamente ou pela Plataforma de Helpdesk disponibilizada pela CONTRATADA.

3.2. MODALIDADE DE LICENCIAMENTO

3.2.1. Os softwares deverão ser oferecidos nas modalidades de licenciamento escolhidas. O pagamento das licenças deve consistir em uma única operação a ser realizada após o recebimento e a aceitação do produto. Não se incluem aqui, obviamente, como restrições a obrigações futuras, o respeito às leis da propriedade intelectual e às políticas de licenciamento dos fabricantes.

3.3. VERSÃO DA SOLUÇÃO A SER ENTREGUE

3.3.1. Deverá ser entregue a última versão lançada até a data da entrega, independentemente da versão cotada por ocasião do procedimento licitatório.

3.4. APRESENTAÇÃO

3.4.1. O produto deverá ser fornecido satisfazendo todas as condições expressamente estabelecidas oficialmente pelo fabricante do software, para a modalidade de licenciamento adotada. Deve ser fornecido pelo fabricante ou pelo fornecedor o código de ativação do produto com, no mínimo, 01 (um) CD/DVD ou conjunto de CD/DVDs de instalação, ou um link para download do software, conforme o caso.

3.5. ATUALIZAÇÕES

3.5.1. As atualizações deverão contemplar as novas versões do produto, além de receber correções, novas tecnologias desenvolvidas e evoluções de segurança.

3.5.2. A CONTRATADA deverá disponibilizar as novas versões e atualizações do produto à CONTRATANTE, no mesmo momento em que elas forem disponibilizadas ao mercado pelo fabricante.

3.5.3. Deverá ser informado à CONTRATANTE o endereço eletrônico de internet do fabricante do produto, sempre que possível, para o fim de realizar download de versões originais dos softwares, atualizações e pacotes de segurança.

3.5.4. Toda manutenção corretiva, preventiva, evolutiva e adaptativa ficará a cargo da CONTRATADA.

3.5.5. Todas as licenças que compõem a solução devem contar com manutenções corretivas, sem ônus adicional para a CONTRATANTE, durante o ciclo de vida do software indicado pelo fabricante, para o caso de vícios, defeitos ou falhas.

3.6. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

3.6.1. As licenças contratadas deverão ser corretamente mantidas de modo a garantir a disponibilidade e integridade das informações nelas contidas.

3.6.2. Os técnicos da CONTRATANTE que administrarão a solução deverão possuir o conhecimento necessário para a utilização adequada.

3.6.3. A CONTRATADA não poderá se utilizar da presente aquisição para obter qualquer acesso não autorizado às informações de propriedade da CONTRATANTE

3.6.4. A CONTRATADA não poderá obter, capturar, copiar ou transferir qualquer tipo informação de propriedade da CONTRATANTE, sem autorização.

3.6.5. A CONTRATADA deverá atender às Políticas de Segurança da Informação e demais normativos correlatos publicados pela CONTRATANTE.

3.6.6. Se for necessário acesso ao ambiente da CONTRATANTE, deverá ser estabelecido um canal de comunicação seguro.

3.6.7. É proibido o uso de informações da CONTRATANTE, pela CONTRATADA, para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado.

3.6.8. A CONTRATADA deverá notificar, imediatamente, à CONTRATANTE os incidentes cibernéticos contra os serviços ou dados sob a sua custódia.

3.6.9. A CONTRATADA deverá possuir procedimentos necessários para preservação de evidências, conforme legislação.

3.7. REQUISITOS DE IMPLANTAÇÃO

3.7.1. A CONTRATADA deve disponibilizar a solução à CONTRATANTE em pleno funcionamento em até 15 (quinze) dias contados da assinatura do instrumento contratual e recebimento da ordem de fornecimento.

3.7.2. A equipe técnica de infraestrutura de TI da CONTRATANTE realizará a instalação da solução nos equipamentos disponíveis para os usuários da solução.

3.7.3. A CONTRATADA fica obrigada a prestar todas as informações necessárias para tanto, além de prestar todo o auxílio e suporte, inclusive com profissionais especializados, para que a solução possa ser adequadamente instalada e entre em funcionamento na CONTRATANTE dentro do prazo previsto.

4. DO LOCAL DE EXECUÇÃO DOS SERVIÇOS

4.1.1. Os serviços serão executados no endereço da Sede da CONTRATANTE, localizado à Rua Coronel Madureira, n° 77 – Centro – Saquarema - RJ, CEP 28990-756, bem como das secretarias participantes, que são: Av. Saquarema, 4427 - Porto da Roça, Saquarema - RJ, 28891-350 e Rua Frutuoso de Oliveira – Centro, Saquarema - RJ, 28990-764 de segunda a sexta-feira, no horário das 09:00 às 17:00 horas.

4.1.2. Eventuais reuniões serão realizadas no endereço acima informado. Caso seja acordado previamente entre as partes, as reuniões poderão ser realizadas virtualmente.

5. DOS PRAZOS E CRONOGRAMA DE EXECUÇÃO DO OBJETO

5.1.1. O **prazo de vigência do contrato decorrente da ARP terá vigência por 36 (trinta e seis) meses consecutivos**, contados a partir da assinatura do respectivo instrumento contratual e recebimento da licença de subscrição, após emitida ordem de fornecimento, a ser emitida pelo Gestor do Contrato, sendo admitida a sua prorrogação nos termos da Lei nº 8.666/93.

5.1.2. O valor do Contrato poderá ser reajustado com periodicidade mínima de 12 (doze) meses, com base na variação do IPCA (Índice de Preços ao Consumidor), ficando desde já estabelecido que o índice substituto será o INPC (Índice Nacional de Preços ao Consumidor) ou outro índice que vier a substituir os índices atuais, incidindo apenas sobre o valor do Contrato, sem customização e taxa de retorno.

5.1.3. O pagamento dos itens contratados será realizado em uma única parcela por subscrição, após o devido recebimento definitivo da licença.

6. DO SIGILO DE INFORMAÇÕES

6.1. Todas as informações relativas à CONTRATANTE e constantes do cadastro da CONTRATADA deverão ser tratadas como confidenciais e somente poderão ser fornecidas quando solicitadas:

6.1.1. Pela CONTRATANTE;

6.1.2. Em decorrência de determinação judicial.

6.2. Os conhecimentos, dados e informações de propriedade da CONTRATANTE, relativos a aspectos econômico-financeiros, tecnológicos e administrativos, tais como: produtos, sistemas, técnicas, estratégias, métodos de operação e todos e quaisquer outros, repassados por força do objeto do presente Termo de Referência, constituem informação privilegiada e como tal, tem caráter de confidencialidade, só podendo ser utilizados, exclusivamente, no cumprimento e execução das condições estabelecidas neste Termo, sendo expressamente vedado à CONTRATADA:

6.2.1. Utilizá-los para outros fins não previstos neste Instrumento;

6.2.2. Repassá-los a terceiros e empregados não vinculados diretamente ao objeto proposto.

7. DOS CRITÉRIOS DE QUALIFICAÇÃO TÉCNICA

7.1. Comprovação de capacidade operacional da empresa licitante, mediante a apresentação de atestado(s) em nome da licitante, emitidos pela contratante titular, obrigatoriamente pessoa jurídica de direito público ou privado, comprovando ter prestado ou estar prestando serviços compatíveis em características, prazos e em quantidades com objeto desta contratação ou com o item pertinente.

7.2. A empresa licitante poderá apresentar mais de um atestado para fim de composição e comprovação da qualificação técnica.

7.3. A CONTRATANTE reserva-se no direito de executar diligências para verificar e validar as informações prestadas no(s) atestado(s) de capacidade técnica fornecido(s) pelo vencedor do certame. Também poderão ser requeridos cópia do(s) contrato(s), nota(s)

fiscal(is) ou qualquer outro documento que comprove, inequivocamente, a veracidade do(s) atestado(s).

7.4. O documento apresentado pela licitante para comprovação de sua qualificação técnica, além de possuir informações técnicas e operacionais suficientes para qualificar o escopo realizado, deverá conter dados que possibilitem à CONTRATANTE, por intermédio de seu Pregoeiro, caso julgue necessário, confirmar sua veracidade junto ao cedente emissor.

7.5. No caso de atestados emitidos por pessoas jurídicas de direito privado, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa licitante vencedora.

7.6. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa licitante, empresas controladas ou controladoras da empresa licitante, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa licitante.

8. DOS CRITÉRIOS DE ACEITAÇÃO E RECEBIMENTO

8.1. O objeto deste Termo poderá ser rejeitado, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo Fiscal do Contrato, às custas da CONTRATADA, sem prejuízo da aplicação de penalidades.

8.2. O recebimento provisório será feito no ato de entrega dos produtos, mediante recibo, não configurando aceite. Executado, o objeto será recebido na forma prevista no artigo 73, inciso II, alíneas “a” e “b” da Lei 8.666/93, após a conferência quantitativa devidamente atestada na(s) Nota(s) Fiscal(is) correspondente(s) não excluindo a responsabilidade civil a ele relativa, nem a ético-profissional.

8.3. Salvo exigência a ser cumprida pelo adjudicatário, o aceite referente ao recebimento definitivo está sujeito a exame qualitativo e quantitativo a ser realizado pela CONTRATANTE e será processado em até 30 (trinta) dias, contados da entrega da(s) Nota(s) Fiscal(is).

8.4. Licenças e CD-ROM(s) de instalação deverão estar disponibilizadas para utilização pela CONTRATANTE no prazo máximo de 15 (quinze) dias contados da assinatura do instrumento contratual e recebimento da ordem de fornecimento.

9. DO CRITÉRIO DE JULGAMENTO

9.1. O julgamento da licitação será realizado pelo critério do **MENOR PREÇO POR ITEM**, observadas as regras de aceitação das propostas e justificativas elencadas neste termo de referência.

9.2. A adjudicação do objeto será realizada segundo o critério de julgamento fixado no item anterior, observada a decisão final de julgamento do certame pelo Pregoeiro.

9.3. O Regime de execução será o de **EMPREITADA POR PREÇO UNITÁRIO,** considerando o fornecimento de cada subscrição para efeitos de pagamento.

10. DA PROPOSTA DE PREÇOS DOS LICITANTES

10.1. A proposta de preços da licitante deverá conter as seguintes informações, entre outras:

10.1.1. Indicar o prazo de validade que será, no mínimo, de 60 (sessenta) dias corridos.

10.1.2. O preço ofertado deve ter a inclusão dos tributos, fretes, tarifas e as despesas decorrentes da execução do objeto da ser licitado.

10.1.3. Indicar expressamente endereço completo da licitante, inclusive eletrônico (e-mail da empresa) bem como telefones para contados, para fins de futuras notificações e intimações de obrigações relativas à futura contratação.

11. DA DOTAÇÃO ORÇAMENTÁRIA

11.1. A despesa orçamentária decorrente da execução dos serviços de que trata o objeto deste Termo, neste exercício, com dotação suficiente para atender esta finalidade correrá à conta da Natureza de Despesa abaixo informada, referentes à Secretaria Gestora e Participantes.

PROGRAMA DE TRABALHO	ELEMENTO DE DESPESA	FONTE DE RECURSOS
20.001 – 04.126.0024.2.057	339040	170401 Royalties - Lei 9478/97
07.010 - 08.126.0024.2.065	339040	170401 Royalties - Lei 9478/97
16.020 - 10.126.0024.2.059	339040	163500 - Royalties Vinculados à Saúde
08.002 - 12.361.0024.2.062	339040	157300 - Royalties Vinculados à Educação
08.002 - 12.365.0024.2.063	339040	157300 - Royalties Vinculados à Educação
08.002 - 12.365.0024.2.064	339040	157300 - Royalties Vinculados à Educação
08.004 - 13.126.0024.2.057	339040	170401 Royalties - Lei 9478/97

11.2. A despesa para o exercício fiscal subsequente será alocada na dotação orçamentária prevista para atendimento dessa finalidade, a ser consignada à CONTRATANTE, na Lei Orçamentaria Anual, quando for o caso.

12. DAS CONDIÇÕES DE FATURAMENTO E DO PAGAMENTO

12.1. A CONTRATADA deverá entregar sem ônus para o CONTRATANTE documento de cobrança referente aos serviços faturados. O documento de cobrança deve ser entregue com antecedência mínima de 10 (dez) dias da data de vencimento.

12.2. A CONTRATANTE poderá contestar junto à CONTRATADA os valores contra ela lançados, contado o prazo para a contestação a partir da data da cobrança considerada indevida.

12.3. CONTRATADA deve permitir o pagamento dos valores não contestados, emitindo, sem ônus para a CONTRATANTE, novo documento de cobrança, com prazo adicional para pagamento. O documento de cobrança deve ser entregue com antecedência mínima de 10 (dez) dias da data de vencimento.

12.4. A CONTRATADA deverá destacar na Nota Fiscal/Fatura as retenções tributárias, conforme legislação pertinente, e a CONTRATANTE, quando a legislação assim exigir, efetuará o recolhimento de tributos, contribuições sociais e fiscais.

12.5. A CONTRATADA deverá fornecer, sempre que solicitado pela CONTRATANTE, os documentos que comprovem o correto e tempestivo pagamento de todos os encargos previdenciários, trabalhistas, fiscais e comerciais decorrentes da execução dos serviços contratados.

12.6. Para fins de pagamento, cabe à CONTRATANTE verificar nos moldes da lei a regularidade fiscal, trabalhista e previdenciária da CONTRATADA.

12.7. O pagamento relativo às licenças de uso do software contratado será realizado, em regra, em até 30 (trinta) dias após o adimplemento da obrigação e apresentação da Nota Fiscal/Fatura devidamente atestada por, no mínimo, dois servidores designados pela CONTRATANTE, conforme Art. 40, inciso XIV, “a”, da Lei Federal 8.666/93, e Periodicidade de Pagamento constante no ANEXO III.

13. DA SUBCONTRATAÇÃO

13.1. Fica permitida a subcontratação para a execução dos serviços de suporte técnico.

13.2. A subcontratação só será autorizada pela CONTRATANTE após a comprovação da capacidade técnica da empresa para executar os serviços pretendidos e de sua regularidade fiscal.

14. DAS REGRAS BÁSICAS DO REGISTRO DE PREÇOS

14.1. As contratações decorrentes do registro de preços formalizado por intermédio deste procedimento de contratação serão realizadas segundo as regras da Ata de Registro de Preços (ARP), observadas no Decreto Municipal nº 1150/2011 e na Lei Federal nº 8.666, de 21 de junho de 1993.

14.2. A Ata de Registro de Preços (ARP) terá vigência de 12 (doze) meses, improrrogáveis, a contar da data de sua publicação.

14.3. A existência de preços registrados não obriga a Administração a firmar as contratações que deles poderão advir, não estando obrigada a adquirir uma quantidade mínima, facultando-se a realização de licitação específica para a contratação pretendida, sendo assegurada ao beneficiário do Registro a preferência de fornecimento em igualdade de condições.

14.4. Os quantitativos solicitados são estimados e representam as previsões das Secretarias para contratações durante o prazo de vigência da ARP.

14.5. É vedado efetuar acréscimos nos quantitativos fixados pela Ata de Registro de Preços, inclusive o acréscimo de que trata o § 1º do art. 65 da Lei Federal nº 8.666, de 21 de junho de 1993.

14.6. O Órgão Gerenciador da Ata de Registro de Preços a ser firmada mediante a realização de Pregão Presencial é a **Secretaria Municipal de Gestão, Inovação e Tecnologia**.

14.7. **São participantes deste Registro de Preços, os seguintes Órgãos:**

14.7.1. Secretaria Municipal de Saúde

14.7.2. Secretaria Municipal de Educação, Cultura, Inclusão, Ciência e Tecnologia

14.7.3. Secretaria Municipal de Desenvolvimento Social

14.7.4. Secretaria Municipal de Gestão, Inovação e Tecnologia, concentrando o restante da estrutura municipal.

14.8. A escolha pela realização de procedimento licitatório utilizando o Sistema de Registro de Preços para a contratação pretendida se dá pelo fato de que a execução do objeto deste instrumento será realizada de forma parcelada por mais de um Órgão Público do Município de Saquarema, de acordo com o art. 3º, inciso III, do Decreto Federal nº 7892/2013, *in verbis*:

> *"Art. 3º O Sistema de Registro de Preços poderá ser adotado nas seguintes hipóteses:*
>
> *[...]*
>
> *III - quando for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou a programas de governo; ou"*

15. DAS OBRIGAÇÕES DA CONTRATADA

15.1. Cumprir todas as disposições referentes ao objeto deste termo de referência e assumir, de forma irrevogável e sem ressalvas, a integral responsabilidade pela execução do contrato, de acordo com as obrigações legais, técnicas e contratuais.

15.2. Responsabilizar-se pela qualidade dos serviços executados e dos recursos empregados, em conformidade com as especificações deste Termo de Referência, sem ônus para a CONTRATANTE e sem prejuízo da aplicação das sanções cabíveis.

15.3. Cumprir os prazos para prestação dos serviços descritos no presente termo de referência e entrega dos materiais correspondentes, quando exigidos.

15.4. Arcar com todos os custos necessários à completa prestação dos serviços, responsabilizando-se por todos os encargos fiscais e comerciais resultantes desta contratação.

15.5. Responsabilizar-se inteira e exclusivamente pelo uso regular de marcas, patentes, registros, processos e licenças relativas à execução desta contratação, eximindo a CONTRATANTE das consequências de qualquer utilização indevida.

15.6. Executar todas as atividades pertinentes a este termo de referência por meio de equipe técnica comprovadamente especializada, com rigorosa observância aos conceitos técnicos estabelecidos nos documentos contratuais e tudo mais que for necessário ao perfeito cumprimento das obrigações previstas neste Termo de Referência.

15.7. Observar, para o cumprimento do objeto deste Termo de Referência, as disposições da Lei nº 13.709/2018 e alterações, bem como as normas técnicas e regulamentações da Autoridade Nacional de Proteção de Dados, quando couber.

15.8. Cumprir o disposto na legislação trabalhista e nas normas regulamentadoras relativas à segurança e medicina do trabalho, na legislação ordinária federal, estadual e municipal, aplicáveis ao objeto deste Termo de Referência, bem como os acordos e convenções coletivas de trabalho das categorias profissionais envolvidas.

15.9. Responsabilizar-se inteiramente pelo pessoal alocado na prestação dos serviços objeto deste Termo de Referência, observando rigorosamente todas as prescrições relativas às leis sociais, fiscais, comerciais, trabalhistas e previdenciárias, sendo considerada, em qualquer circunstância, como a única empregadora responsável e também por qualquer adicional relativo à remuneração desse pessoal que seja ou venha a ser devido.

15.10. Respeitar as normas e procedimentos de controle interno, inclusive de acesso às dependências da CONTRATANTE.

15.11. Responder pelos danos causados diretamente à Administração ou aos bens da CONTRATANTE, ou ainda a terceiros, decorrentes de sua culpa ou dolo, durante a execução do contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pela CONTRATANTE.

15.12. Comunicar à CONTRATANTE qualquer anormalidade constatada durante a prestação dos serviços e prestar os esclarecimentos solicitados.

15.13. Manter, durante o período de vigência do contrato, o atendimento a todas as condições de habilitação e qualificação exigidas na licitação.

15.14. Autorizar e assegurar à CONTRATANTE o direito irrestrito de fiscalizar, sustar, recusar, mandar desfazer ou refazer qualquer serviço que não esteja de acordo com a técnica e as especificações deste termo de referência.

15.15. Manter sigilo sobre toda e qualquer informação confidencial, reservada ou exclusiva, incluindo informações técnicas, de negócios ou financeira, comunicada pela CONTRATANTE em função do contrato.

15.16. A CONTRATADA deverá assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em

ocorrência da espécie forem vítimas os seus empregados durante a execução do contrato, ainda que ocorrido nas dependências da CONTRATANTE.

15.17. A inadimplência da CONTRATADA, com referência aos encargos sociais, comerciais e fiscais não transfere a responsabilidade por seu pagamento à CONTRATANTE, nem poderá onerar o objeto desta contratação.

16. DAS OBRIGAÇÕES DA CONTRATANTE

16.1. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta.

16.2. Exercer o acompanhamento e a fiscalização, por servidor(es) especialmente designado(s), anotando em registro próprio as falhas detectadas e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

16.3. Notificar a CONTRATADA por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas.

16.4. Ter pessoal disponível para o recebimento dos produtos contratados no horário e local previsto para entrega, quando couber.

16.5. Receber os produtos de acordo com as especificações descritas neste documento, rejeitando, no todo ou em parte, o serviço executado em desacordo com o contratado.

16.6. Pagar à CONTRATADA o valor resultante da execução dos serviços, no prazo e condições estabelecidas neste Termo de Referência.

16.7. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da CONTRATADA, no que couber, em conformidade com a legislação vigente.

16.8. Fornecer por escrito as informações necessárias para o desenvolvimento do objeto do Contrato.

16.9. Arquivar, entre outros documentos, projetos, especificações técnicas, orçamentos, termos de recebimento, contratos e aditamentos, relatórios de inspeções técnicas após o recebimento do objeto e notificações expedidas.

16.10. Possibilitar o acesso da equipe técnica da CONTRATADA aos locais de instalação, quando couber, orientando-a sobre dúvidas referentes às características técnicas do objeto.

16.11. Notificar, formal e tempestivamente, a CONTRATADA sobre as irregularidades observadas no cumprimento do Contrato.

16.12. Notificar a CONTRATADA, por escrito e com antecedência, sobre multas, penalidades e quaisquer débitos de sua responsabilidade.

17. DA GARANTIA:

17.1. As subscrições possuem direito de atualização e suporte técnico durante 36 (trinta e seis) meses após o aceite da recepção técnica das licenças entregues.

17.2. A CONTRATADA deverá apoiar a equipe técnica da CONTRATANTE na customização e uso do software no conhecimento da arquitetura e de suas funcionalidades, esclarecendo dúvidas a respeito de configurações, ajustes (tuning) e segurança.

17.3. A garantia deverá contemplar serviço de manutenção que consiste no conjunto de ações necessárias para restaurar as condições de funcionamento do ambiente, garantindo alto desempenho e permitindo a sua utilização na capacidade máxima, com solução de eventuais problemas, danos ou defeitos existentes, contemplando:

17.3.1. Correções de erro de código para corrigir desvios das especificações então aplicáveis que tenham sido relatados, sem ônus adicional para a CONTRATANTE.

17.3.2. Atualizações de código: com distribuição periódica de correções de código, aprimoramentos funcionais (inclusive modificações para cumprir exigências governamentais), podendo compreender atualizações de contingência, pacotes de serviços, novas versões e releases, sem ônus adicional para a CONTRATANTE.

17.4. Estes serviços podem ser executados de forma proativa, desde que devidamente comunicado, ou após a abertura de um chamado técnico pela CONTRATANTE.

17.5. Para a execução dos serviços de garantia, a CONTRATADA deverá:

17.5.1. Identificar falhas e defeitos e executar serviços especializados de manutenção, para restabelecer as perfeitas condições de uso, permitindo sua utilização na capacidade máxima.

17.5.2. Realizar suporte remoto via internet, sempre que o software apresentar problema, ou de forma presencial, caso o problema não seja sanado, conforme definido nas cláusulas de níveis de serviços, detalhados nesse anexo.

17.5.3. Identificar componentes de software que devem ser atualizados e agendar com a CONTRATANTE a atualização.

17.5.4. Durante a vigência do contrato, a CONTRATANTE terá direito a atualização da versão dos softwares e patches de correção. Caberá à CONTRATADA a disponibilização destas novas versões. A atualização será realizada pela CONTRATANTE com suporte da CONTRATADA;

18. DA FISCALIZAÇÃO E ACOMPANHAMENTO DO CONTRATO

18.1. Não obstante a CONTRATADA seja a única e exclusiva responsável pela execução dos serviços contratados, a CONTRATANTE reserva-se ao direito de exercer a mais ampla e completa fiscalização sobre a execução desses serviços, não restringindo em nada a responsabilidade da CONTRATADA.

18.2. Nos termos do Art. 67, §1º, da Lei Federal nº 8.666/93, a CONTRATANTE designará servidor (es) para acompanhar e fiscalizar a execução do Contrato, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização das falhas ou defeitos observados.

18.3. As decisões e providências que ultrapassarem a competência do (s) servidor (es) designado (s) deverão ser encaminhadas ao Gestor do Contrato, em tempo hábil para adoção das medidas convenientes.

18.4. A execução dos serviços contratados será fiscalizada por equipe de servidores especificamente designada para essa finalidade pela CONTRATANTE, cujas atribuições básicas são:

18.4.1. Solicitar à CONTRATADA e ao Gestor do Contrato por ela indicado todas as providências necessárias ao bom andamento dos serviços;

18.4.2. Solicitar à CONTRATADA a regularização de serviços que não atendam às especificações definidas neste instrumento e/ou às necessidades requeridas para execução destes;

18.4.3. Quaisquer outras atribuições necessárias ao bom desempenho dos serviços contratados.

18.5. Da mesma forma, a CONTRATADA deverá indicar um preposto para representá-la na execução do Contrato.

18.6. Quaisquer exigências da fiscalização, inerentes ao objeto do Contrato, deverão ser prontamente atendidas pela CONTRATADA, sem ônus para a CONTRATANTE.

19. DAS HIPÓTESES DE RESCISÃO

19.1. O futuro Contrato poderá ser rescindido, a critério da CONTRATANTE, nas hipóteses de inadimplemento parcial ou total de quaisquer obrigações contidas neste termo de referência, nos termos do art. 77 da Lei 8.666/93, desde que efetivamente reste comprovado prejuízo à finalidade pública pretendida com a contratação.

19.2. Cabe à parte prejudicada ou interessada a comprovação do efetivo prejuízo que justifique a rescisão contratual, caso ocorra quaisquer dos motivos indicados art. 78 da Lei 8.666/93.

19.3. A rescisão contratual será processada nos autos de processo administrativo, sempre se garantindo o contraditório e a ampla defesa.

19.4. Na ocorrência de rescisão contratual, ficam assegurados os direitos da Administração contidos no art. 80 da Lei 8.666/93, sem prejuízo de quaisquer outros previstos pela legislação.

20. DAS SANÇÕES ADMINISTRATIVAS - PENALIDADES

20.1. Serão aplicadas as sanções contratuais sobre as condutas típicas, caso necessário, de acordo com art. 78 e seguintes da Lei Federal 8.666/93.

20.2. A multa estabelecida será de acordo com art. 7º, Lei n.10.520/02; art.86 a 88, Lei Federal 8.666/93; art. 55, VII, Lei Federal 8666/93; art. 80, III, Lei Federal 8.666/93.

20.3. A aplicação de qualquer penalidade prevista pela Administração Pública realizar-se-á em processo administrativo, que assegurará o contraditório e a ampla defesa à CONTRATADA.

20.4. O Contrato, sem prejuízo das multas e demais cominações legais nele previstas, poderá ser rescindido unilateralmente, por ato formal da Administração, nos casos enumerados no art. 78, incisos I a XII e XVII, da Lei nº 8.666/93.

21. DAS CONDIÇÕES GERAIS

19.1 A CONTRATANTE poderá a qualquer tempo recusar o serviço/fornecimento, no todo ou em parte, sempre que não atender ao estipulado neste Termo ou aos padrões técnicos de qualidade exigíveis.

19.2 No interesse da CONTRATANTE, o contrato poderá sofrer acréscimos ou supressões, nos termos do artigo 65, da Lei nº 8.666/93 e alterações posteriores, com a apresentação das devidas justificativas.

19.2.1 Nenhum acréscimo ou supressão poderá exceder o limite estabelecido em lei, exceto as supressões resultantes de acordo entre as partes.

19.3 De acordo com o art. 48 da Lei de Licitações e Contratos Administrativos, as propostas que apresentem valores incompatíveis com os preços praticados no mercado ou que apresentem valores excessivos, superiores àqueles fixados no ato convocatório como sendo o maior valor que a Administração está disposta a desembolsar, serão desclassificadas, acaso não haja a sua readequação.

19.4 Nos preços propostos e nos lances que vierem a ofertar deverão estar inclusos todos os custos necessários a execução dos serviços objeto do presente Termo e da licitação, bem como todos os impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, deslocamento de pessoal, transporte, garantia dos materiais/acessórios e quaisquer outros que incidam ou venham a incidir sobre o objeto licitado constante da proposta. Não será permitido, portanto, que tais encargos sejam discriminados em separado.

19.5 É de responsabilidade da CONTRATANTE a elaboração de Contratos e Termos Aditivos em todas as fases da concepção à concretização (imprime, colhe assinaturas, envia aos órgãos da Administração Pública).

19.6 As solicitações de instalação, alteração e configuração dos serviços contratados deverão ser intermediadas exclusivamente pela CONTRATANTE.

19.7 Em caso de cisão, fusão ou incorporação da CONTRATADA, deverá ser assegurada a continuidade do objeto descrito no presente Termo de Referência, nos termos da legislação vigente.

19.8 A CONTRATADA deverá atender os indicadores de qualidade, exceto em situações decorrentes de casos fortuitos ou força maior, os quais serão analisados conjuntamente pela equipe técnica da CONTRATADA e da CONTRATANTE.

Saquarema, 02 de outubro de 2023.

Elaborado por:

CARLA SANT`ANNA DOS SANTOS
Diretora Adjunta de Informática
Matrícula 928914

De acordo:

ÉLIDA DA SILVA ALVES
Secretária Municipal de Gestão, Inovação e Tecnologia
Matrícula 958938-3

ANEXO I – MEMÓRIA DE CÁLCULO

ITEM	ESPECIFICAÇÃO TÉCNICA	UNIDADE	QUANTIDADE PARA REGISTRO	Secretaria Municipal de Gestão, Inovação e Tecnologia	Secretaria Municipal de Educação, Inclusão, Ciência e Tecnologia	Secretaria Municipal de Saúde	Secretaria Municipal de Desenvolvimento Social
01	LICENÇA DE USO DO SOFTWARE **ANTIVÍRUS ENTERPRISE**, subscrição pelo período de 36 (trinta e seis) meses, em sua versão mais recente, incluindo atualizações e suporte durante o período.	Licenças (subscrição)	**3500**	1205	2000	143	152

Processo nº: 8331/2023

Fls:_____ Rubrica:_____

ANEXO II – MODELO DE PROPOSTA DE PREÇOS

(Papel timbrado da empresa)

À
PREFEITURA MUNICIPAL DE SAQUAREMA

PROCESSO: XXX/2023
PREGÃO PRESENCIAL nº _____/2023
OBJETO: CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA O FORNECIMENTO DE SUBSCRIÇÃO DE LICENÇAS DE SOFTWARES, SISTEMAS OPERACIONAIS E SERVIÇOS ASSOCIADOS, DESTINADOS A ATENDER AS NECESSIDADES DA PREFEITURA MUNICIPAL DE SAQUAREMA.

DADOS DA EMPRESA		
Razão Social:		
CNPJ:		
Endereço:		
Nº:	Bairro:	
CEP:		
Conta bancária:		
Banco:	Agência:	Conta Corrente:

ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QTD	VALOR UNITÁRIO	VALOR TOTAL
01	SOLUÇÃO DE PROTEÇÃO, DETECÇÃO E RESPOSTA A INCIDENTE DE ENDPOINT, subscrição pelo período de 36 (trinta e seis) meses, em sua versão mais recente, incluindo atualizações, garantia e suporte técnico durante todo o período, conforme descritivo técnico constante no item 3 do Termo de Referência.	Licenças (subscrição)	3500	R$	R$
VALOR TOTAL PROPOSTO					**R$**

Demais condições:

1. Assim sendo, o valor total da proposta é de R$ _____ (por extenso).
2. A presente proposta é baseada nas especificações, condições e prazos estabelecidos no edital de Pregão Presencial nº _____/2023, os quais nos comprometemos a cumprir integralmente.
3. O prazo de validade da Proposta deverá ser de no mínimo 60 (sessenta) dias.

4. Declaramos que estamos de pleno acordo com todas as condições estabelecidas no Edital e seus Anexos, bem como aceitamos todas as obrigações e responsabilidades especificadas no Termo de Referência.

5. Declaramos que nos preços cotados estão incluídas todas as despesas que, direta ou indiretamente, fazem parte do presente objeto, tais como gastos da empresa com suporte técnico e administrativo, impostos, seguros, taxas, ou quaisquer outros que possam incidir sobre gastos da empresa, sem quaisquer acréscimos em virtude de expectativa inflacionária e deduzidos os descontos eventualmente concedidos.

Local e data: _____, _____ de _____de 2023

_____

Identificação e Assinatura do Representante Legal da Empresa Proponente

Processo nº: 8331/2023

Fls:_____ Rubrica:_____

ANEXO III – PERIODICIDADE DE PAGAMENTO

ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	PERIODICIDADE DE PAGAMENTO
01	SOLUÇÃO DE PROTEÇÃO, DETECÇÃO E RESPOSTA A INCIDENTE DE ENDPOINT, subscrição pelo período de 36 (trinta e seis) meses, em sua versão mais recente, incluindo atualizações, garantia e suporte técnico durante todo o período, conforme descritivo técnico constante no item 3 do Termo de Referência.	Licenças (subscrição)	PARCELA ÚNICA POR SUBSCRIÇÃO