TERMO DE REFERERÊNCIA
ANEXO 01

1. DO OBJETO

1.1. Aquisição de **LICENCIAMENTO DE ANTIVÍRUS 12X (DOZE MESES).**

2. ESPECIFICAÇÃO / PREÇO MÁXIMO

2.1. Descritivo da contratação:

ITEM	*DESCRIÇÃO*	*QNTD*	*VALOR UNIT.*	*VALOR TOTAL*
1	**LICENCIAMENTO DE ANTIVIRUS 12X (DOZE MESES) FOR BUSINESS.** CARACTERISTICAS: COMPATIBILIDADE: Microsoft Windows Server 2008 x64 e R2; Microsoft Windows Small Business Server 2008 (Todas edições); Microsoft Windows Server 2012 e R2 (Todas edições); Microsoft Windows Server 2016 e R2 (Todas edições); Microsoft Windows Server 2019 e R2 (Todas edições); Microsoft Windows XP Professional x64 SP2, SP3 ou superior; Microsoft Windows Vista Business / Enterprise / Ultimate SP1 ou posterior; Microsoft Windows Vista Business / Enterprise / Ultimate SP1 x64 ou posterior; Microsoft Windows 7 Starter/ Home Basic/Home Premium/Professional/Enterprise e Ultimate; Microsoft Windows 7, x64, Starter/ Home Basic/Home Premium/Professional/Enterprise e Ultimate; Microsoft Windows 8 Professional / Enterprise; Microsoft Windows 8 Professional / Enterprise x64; Microsoft Windows 8.1 Professional / Enterprise; Microsoft Windows 8.1 Professional / Enterprise x64. Microsoft Windows 10 Professional / Enterprise x64; Suportar as seguintes plataformas virtuais: VMware: Workstation 9.x, Workstation 10.x, ESXi 5.5, ESXi 6.0 e superior; Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2 e 2016; Oracle VM VirtualBox 4.0.4 e Superior (Somente logon como convidado); Citrix XenServer 6.0 e Acropolishypervisor. A console deve ser acessada via WEB (HTTPS) ou MMC; Console deve ser baseada no modelo cliente/servidor; Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus; Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, patch management e MDM; 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; Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores; Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory; Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria; A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas; Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador; Deve integrar com Active Directory e ler acessos específicos de usuários por permissões em grupos de gerenciamento; A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle; Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário; Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux) protegidos pela solução antivírus; Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto; Capacidade de atualizar os pacotes	**130**	**R$ 138,22**	**R$ 17.968,60**

	de instalação com as últimas vacinas; 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; A comunicação entre o cliente e o servidor de administração deve ser criptografada; Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes; Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros: Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas (varredura); Nome do computador; Nome do domínio; Range de IP; Sistema Operacional; Máquina virtual. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional; Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção; 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; 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 possua, deverá instalar o antivírus automaticamente; 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 X dias, etc.; 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; 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; Data e horário de quando a máquina foi ligada; 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; Usuário(s) logado(s) naquele momento, com informações de contato (caso disponível 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; Atualizações do Windows Update instaladas; Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD; Vulnerabilidades de aplicativos instalados na máquina; Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las; 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; Alteração de subrede; Resolução de Nome; Disponibilidade de endereço de conexão SSL; Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet; Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes; Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus; Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos; 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; 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; Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML; Capacidade de gerar traps SNMP para monitoramento de eventos; Capacidade de enviar emails para contas específicas em caso de algum evento; Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server; Deve possuir compatibilidade com Cisco Prime Infrastructure - Version: 3.1 ou superior; Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo); 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; Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo); Capacidade de realizar atualização incremental de vacinas nos computadores clientes; 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. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores; Capacidade de realizar inventário de hardware de todas as máquinas clientes; Capacidade de realizar inventário de aplicativos de todas as máquinas clientes; Capacidade de diferenciar máquinas virtuais de máquinas físicas. Estações Windows: Compatibilidade: Microsoft Windows Embedded 8.0 Standard x64; Microsoft Windows Embedded 8.1 Industry Pro x64; Microsoft Windows Embedded Standard 7 x86 / x64 SP1; Microsoft Windows XP Professional x86 SP3 e superior; Microsoft Windows Vista x86 / x64SP2 e posterior; Microsoft Windows 7 Starter/ Home Basic/Home Premium/Professional/Enterprise e Ultimate x86 / x64 e posterior; Microsoft Windows 8 Professional/Enterprise x86 / x64; Microsoft Windows 8.1 Pro / Enterprise x86 / x64 (Todas as Versões); Microsoft Windows 10 Pro / Enterprise x86 / x64 (Todas as Versões). Características: Deve prover as seguintes proteções: Antivírus de Arquivos Residentes (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 Email (módulo para verificação de emails recebidos e enviados, assim como seus anexos); Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, MSN, por exemplo); O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza; Firewall com IDS; Autoproteção (contra-ataques aos serviços/processos do antivírus); Controle de dispositivos externos (cartões de memória, pen drive, etc); Controle de acesso a sites por categoria; Controle de acesso a sites por horário; Controle de acesso a sites por usuários; Controle de execução de aplicativos; Controle de vulnerabilidades do Windows e dos aplicativos instalados; Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota; As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários em no máximo, 02 (duas) em 02 (duas) horas independentemente do nível das ameaças encontradas no período (alta, média ou baixa) ou de forma definida pela SEFAZ; Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação; 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 (falso positivo); 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; Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks); Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento; 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 Capacidade de verificar somente arquivos novos e alterados; de verificar objetos usando heurística; Capacidade de agendar uma pausa na verificação; Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias; Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado; 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 quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador). Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto; Capacidade de verificar emails recebidos e enviados nos protocolos POP3, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL); Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings; Capacidade de verificar links inseridos em emails contra phishings; Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Google Chrome, Opera, etc.; Capacidade de verificação de corpo e anexos de emails usando heurística; O antivírus de email, ao encontrar um objeto potencialmente perigoso, deve: Perguntar o que fazer, ou; Bloquear o email; Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador); Caso positivo de desinfecção: Restaurar o email para o usuário; Caso negativo de desinfecção: Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador); Caso o email contenha código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena; Possibilidade de verificar somente emails recebidos ou recebidos e enviados; Capacidade de filtrar anexos de email, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador; Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas; Deve ter suporte total ao protocolo IPv6; Capacidade de alterar as portas monitoradas pelos módulos de Web e Email. 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; 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. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web; 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; Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa; 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; Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-PhishingWorkingGroup (www.antiphising.org); Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica; Deve possuir módulo IDS (IntrusionDetection System) para proteção contra portscans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas; 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 à rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados. 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 smartcard; Dispositivos de sincronização via ActiveSync (Windows CE, WindowS Mobile, etc); Wi-Fi; Adaptadores de rede externos; Dispositivos MP3 ou smartphones; Dispositivos Bluetooth; Câmeras e Scanners. 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; Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário; Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento; Capacidade de configurar novos dispositivos por Class ID/Hardware ID; Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc.), com possibilidade de configuração por usuário ou grupos de usuários e agendamento; 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.); Capacidade de bloquear execução de aplicativo que está em armazenamento externo; 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; 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; 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. Servidores Windows: Compatibilidade com Plataforma 32-bits: Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior); Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior). Compatibilidade com Plataforma 64-bits: Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior); Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior); Microsoft Windows Server 2008 R2 Standard / Enterprise / DataCenter (SP1 ou posterior); Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter (SP1 ou posterior); Microsoft Windows Storage Server 2008 R2; Microsoft Windows Hyper-V Server 2008 R2 (SP1 ou posterior); Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter; Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter; Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter; Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter; Microsoft Windows Storage Server 2012 (Todas edições); Microsoft Windows Storage Server 2012 R2 (Todas edições); Microsoft Windows Hyper-V Server 2012; Microsoft Windows			

	Hyper-V Server 2012 R2. Microsoft Windows Server 2016 (Todas edições); Microsoft Windows Server 2016 R2 (Todas edições); Microsoft Windows Server 2019 (Todas edições); Microsoft Windows Server 2019 R2 (Todas edições); Microsoft Windows Hyper-V Server 2019 e R2 (Todas edições); Microsoft Windows Storage Server 2019 e R2 (Todas edições); Características: Deve prover as seguintes proteções: Antivírus de Arquivos Residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado; Auto-proteção contra- ataques aos serviços/processos do antivírus; Firewall com IDS; Controle de vulnerabilidades do Windows e dos aplicativos instalados; Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota; As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora; 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 e Quarentena; Visualização de relatórios; Gerenciamento de relatórios; Gerenciamento de chaves de licença; Gerenciamento de permissões (adicionar/excluir permissões acima). 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; 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; Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc.); Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS); Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares; Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor; Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor; Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas; Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação; 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; Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento; 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; Capacidade de verificar somente arquivos novos e alterados; Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.); Capacidade de verificar objetos usando heurística; Capacidade de configurar diferentes ações para diferentes tipos de ameaças; Capacidade de agendar uma pausa na verificação; Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado. 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 quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador); Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto; Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena; Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa. Servidores Linux: Compatibilidade com Plataforma 64-bits: RedHat Enterprise Linux Server 7 e Superiores; CentOS-7.0 e Superiores; SUSE Linux Enterprise Server 12 e Superiores; Novell Open Enterprise Server 11 SP2 e Superiores; Ubuntu Server 14.04 LTS e Superiores; Ubuntu Server 14.10 e Superiores; Oracle Linux 6.5 e Superiores; Debian GNU/Linux 7.5, 7.6, 7.7 e Superiores; 5.6.1.9. openSUSE® 13.1 e superiores. Características – Deve prover as seguintes proteções: Antivírus de Arquivos Residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado; As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora; 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 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; Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena; Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados; Em caso de erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares; Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento; 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; Capacidade de verificar objetos usando heurística; Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena; Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados; Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux). Criptografia: Compatibilidade: Microsoft Windows XP Professional sp3 ou superior; Microsoft Windows Vista Business/Enterprise/ultimate sp2; Microsoft Windows Vista Business/Enterprise/ultimate x64 sp2; Microsoft Windows 7 Starter/ Home Basic/Home Premium/Professional/Enterprise e Ultimate; Microsoft Windows 7 Starter/ Home Basic/Home Premium/Professional/Enterprise e Ultimate x64; Microsoft Windows 8 Professional/Enterprise; Microsoft Windows 8 Professional/Enterprise x64; Microsoft Windows 8.1 Professional / Enterprise; Microsoft Windows 8.1 Professional / Enterprise x64; Microsoft Windows 10 Pro x86 / x64; Microsoft Windows 10 Enterprise x86 /x64. Características: O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso que o usuário tenha esquecido a senha, através de procedimentos de recuperação; Utilizar, no mínimo, algoritmo AES com chave de 256 bits; Deve ter a capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário; Deve ter a capacidade de utilizar single sign-on para a autenticação de pré-boot; Permitir criar vários usuários de autenticação pré-boot; Deve ter a capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir			

	da console de gerenciamento; Deve ter a capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções: Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes; Criptografar todos os arquivos individualmente; Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas; Criptografar o dispositivo removível, em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha; Deve ter a capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários; Deve ter a capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados; Deve ter a capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados; Verificar compatibilidade de hardware antes de aplicar a criptografia; Deve ter a capacidade de estabelecer parâmetros para a senha de criptografia; Bloquear o reuso de senhas; Bloquear a senha após um número de tentativas pré-estabelecidas; Deve ter a capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados; Permitir criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo; Permitir criptografar as seguintes pastas pré-definidas: “meus documentos”, “favoritos”, “desktop”, “arquivos temporários” e “arquivos do outlook”; Permitir utilizar variáveis de ambiente para criptografar pastas customizadas; Deve ter a capacidade de criptografar arquivos por grupos de extensão, tais como: documentos do office, documentos .txt, arquivos de áudio, etc.; Permitir criar um grupo de extensões de arquivos a serem criptografados; Deve ter a capacidade de criar regra de criptografia para arquivos gerados por aplicações; Permitir criptografia de dispositivos móveis mesmo quando o Endpoint não possuir comunicação com a console de gerenciamento. Gerenciamento de Sistemas: Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis; 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; Capacidade de gerenciar licenças de softwares de terceiros; Capacidade de registrar mudanças de hardware nas máquinas gerenciadas; Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, servicetag, número de identificação e outros; Possibilitar fazer distribuição de software de forma manual e agendada; Suportar modo de instalação silenciosa; Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis; Possibilitar fazer a distribuição através de agentes de atualização; Utilizar tecnologia multicast para evitar tráfego na rede; Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches; Suportar modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento; Capacidade de gerar relatórios de vulnerabilidades e patches; Possibilitar criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração; Permitir iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador; Permitir baixar atualizações para o computador sem efetuar a instalação; Permitir o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas; Ter capacidade de instalar correções de vulnerabilidades de acordo com a severidade; Permitir selecionar produtos a serem atualizados pela console de gerenciamento; Permitir selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers,			

	etc. Da Garantia e Suporte: Os objetos deverão possuir garantia técnica mínima de 12 (doze) meses, sob a responsabilidade da CONTRATADA. A CONTRATADA deverá disponibilizar assistência técnica no período da garantia técnica; No período de vigência, o CISVIR não pode ter ônus de nenhuma natureza quando da apresentação de defeito do objeto. É ainda de total responsabilidade do fornecedor qualquer despesa de envio e coleta do mesmo; Todas as licenças de software utilizadas para atender o objeto deverão possuir garantia de 12 (doze) meses; A Licitante vencedora deverá prestar suporte técnico e operacional durante o período de vigência da licença, com atendimento através do serviço telefônico (0800), acesso remoto, email ou WEB, para esclarecimento de dúvidas, abertura de chamados, e envio de arquivos para análise (Zero-day). Os prazos relativos aos chamados deverão obedecer ao seguinte nível de serviço: 24 x 7 (vinte e quatro horas por dia, sete dias por semana, dias úteis e horário comercial); O serviço de Suporte Técnico garante: Reinstalação, reconfiguração e auxilio na utilização de recursos ou solução de problemas relacionados aos sistemas ofertados; O direito de receber toda e qualquer atualização de todos os softwares ou patches corretivos de componentes adquiridos após a assinatura do contrato, para a versão mais atual das ferramentas. A CONTRATADA deverá prestar atendimento técnico em regime de garantia. ***MODELO DE REFERÊNCIA*:** KASPERSKY END-POINT SECURITY FOR BUSINESS - SELECT BRAZILIAN EDITION – GOVERNAMENTAL.			

2.1.1. Para julgamento será adotado o critério de **MENOR PREÇO POR LOTE** e a disputa será pelo valor total do lote.

2.1.2. O valor total para a execução do objeto descrito acima é de R$ 17.968,60 (dezessete mil, novecentos e sessenta e oito reais, e sessenta centavos) considerando os valores obtidos na pesquisa de mercado, conforme mapa de preço anexo ao Processo Administrativo acima referenciado.

3. JUSTIFICATIVAS

3.1. Justificativa para escolha da modalidade:

3.1.1. A Lei nº 14.133/2021, o artigo 75 traz a as possibilidades de que o gestor dispõe para dispensar a licitação, seja em razão de valor, seja de acordo com o objeto, seja no caso de licitação deserta ou fracassada. Especificamente, quanto à dispensa de licitação dos incisos I e II, do art. 75, trazem a previsão de que, respectivamente, para contratações de obras e serviços de engenharia ou serviços de manutenção de veículos automotores, poderá ser dispensa a licitação para contratações com valores inferiores a R$ 100.000,00; e, para contratações de demais serviços e compras, esse valor limite é de R$ 50.000,00. Sendo os referidos valores duplicados nos casos de contratos firmados por consórcio público, ou por autarquia ou fundação qualificada, como agências executivas definidas em lei, o que torna a modalidade de Dispensa de Licitação pertinentes diante da escolha do objeto e do amparo legal em conformidade com o disposto em lei.

3.2. Justificativa da necessidade:

3.2.1. Com o intuito de fortificar a segurança das informações internas, assim também como, evitar invasões de hackers ou o recebimento de arquivos maliciosos, que poderiam danificar os computadores e os servidores, faz-se necessário a aquisição de licenciamento de software de antivírus, gerando assim, um ambiente de trabalho mais confiável e protegido.

3.3. Justificativa do preço:

3.3.1. Os preços praticados são de mercado, itens que demonstram, sem maiores aprofundamentos, que os valores estão adequados ao praticado, notadamente considerando-se a pesquisa de preço em apenso aos autos.

4. CONDIÇÕES DE EXECUÇÃO DO OBJETO

4.1. Prazo de entrega/Local de Entrega:

Prazo de Entrega/Dias:	10	15	30	60	Pedido(s) serão feitos de forma fracionada?	SIM	NÃO
	☒	☐	☐	☐		☐	☒

O fornecedor participante precisa dar garantia de que o produto está em estoque e em condições de envio, visto que o prazo de execução do recurso já está pré-estipulado?	SIM	NÃO
	☒	☐

Local de Entrega:	
☒	Avenida Santa Catarina, 1325, Jardim Apucarana, Apucarana, PR, 86.804-015
☐	Avenida Arapongas, 02, Centro, Arapongas, Paraná, 86.700-050
☐	R. Natal, 525, Cambira - PR, 86890-000

4.2. Condições de recebimento do objeto:

4.2.1. Quando se tratar de **produto(s)**, o(s) item(s) deverão ser entregue(s) com no **mínimo** 75% (setenta e cinco por cento) de sua validade total a contar da data da entrega, não sendo inferior a 06 (seis) meses;

4.2.2. Em se tratando de **bem durável/equipamentos**, será exigida garantia e/ou validade do objeto de, no **mínimo**, 12 (doze) meses, contado(s) do seu recebimento definitivo.

Parágrafo Único: Deverá a licitante responsabilizar-se pela qualidade e procedência dos produtos, bem como pela inviolabilidade de suas embalagens até a entrega dos mesmos à CONTRATANTE, garantindo que o seu transporte, mesmo quando realizado por terceiros, se faça segundo as condições estabelecidas pelo fabricante, notadamente no que se refere às temperaturas mínimas e máximas, empilhamento e umidade; os bens poderão ser rejeitados no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência, devendo ser substituídos no prazo de 05 (cinco) dias úteis, a contar da notificação à Contratada, às custas desta, sem prejuízo da aplicação das penalidades;

4.3. Prazo de Vigência da Contratação:

4.3.1. O prazo de vigência desta contratação será de 12 (doze) meses, podendo ser prorrogado por iguais e sucessivos períodos de 12 (doze) meses, caso haja interesse da Administração, com a anuência da Contratada, nos termos do art. 107, da Lei Federal 14.133/21.

5. DAS CONDIÇÕES DE RECEBIMENTO DO OBJETO:

5.1. O objeto da presente contratação será recebido **provisoriamente** em até **05** (**cinco**) **dias úteis**, contados da data da entrega dos bens, no local e endereço indicados no subitem 2 do item anterior, acompanhado da respectiva nota fiscal/fatura e sob supervisão do Fiscal de Contrato.

5.2. Por ocasião da entrega, a Contratada deverá colher no comprovante respectivo a data, o nome, o cargo, a assinatura e o número do Registro Geral (RG), emitido pelo Consórcio Intermunicipal de Saúde do vale do Ivaí e Região - CISVIR, do servidor do Contratante responsável pelo recebimento.

5.3. Constatadas irregularidades no objeto contratual, o Contratante poderá:

a) se disser respeito à especificação, rejeitá-lo no todo ou em parte, determinando sua substituição ou rescindindo a contratação, sem prejuízo das penalidades cabíveis;

a.1) na hipótese de substituição, a Contratada deverá fazê-la em conformidade com a indicação da Administração, no prazo máximo de **05 (cinco) dias**, contados da notificação por escrito, mantido o preço inicialmente contratado;

b) se disser respeito à diferença de quantidade ou de partes, determinar sua complementação ou rescindir a contratação, sem prejuízo das penalidades cabíveis;

b.1) na hipótese de complementação, a Contratada deverá fazê-la em conformidade com a indicação do Contratante, no prazo máximo de **05 (cinco) dias**, contados da notificação por escrito, mantido o preço inicialmente contratado.

5.4. O recebimento do objeto dar-se-á **definitivamente** no prazo de até **10 (dez) dias úteis** após o recebimento provisório, uma vez verificado o atendimento integral da quantidade e das especificações contratadas, mediante Termo de Recebimento Definitivo ou Recibo, firmado pelo servidor responsável.

6. SANÇÕES ADMINISTRATIVAS

6.1. São aplicáveis as sanções previstas no Título IV, capítulo I, da Lei Federal nº 14.133/21 e demais normas pertinentes.

6.2. O licitante ou contratado que descumprir qualquer das cláusulas deste aviso ou do instrumento contratual ficará sujeito às penalidades previstas nos artigos 156 e 162 da Lei Federal nº 14.133/21.

6.3. DAS MULTAS – em cada caso, aplicar-se:

6.3.1. Multa de 20% (vinte por cento) do valor estimado para contratação, em razão de injustificada não entrega da documentação nos prazos acordados ou recusa na retirada da Nota de Empenho;

6.3.2. Multa de 0,33% (trinta e três centésimos por cento) por dia de atraso sobre a parcela do objeto, até o limite de 60(sessenta) dias;

6.3.3. Multa de 10% (dez por cento) por inexecução parcial do instrumento contratual sobre o valor da correspondente parcela;

6.3.4. Multa de 20% (vinte por cento) por inexecução total do instrumento contratual sobre o valor;

6.4. Os atrasos por problemas técnicos que perdurarem por mais de 10 (dez) dias serão considerados inexecução parcial para os efeitos das aplicações das penalidades;

6.5. Os atrasos superiores a 60 (sessenta) dias serão considerados inexecução total para efeito de aplicação de penalidade;

6.6. As penalidades serão aplicadas a critério da Administração e são independentes sendo que a aplicação de uma não exclui a das outras, quando cabíveis.

6.7. O prazo para o pagamento das multas será de 05 (cinco) dias úteis a contar da intimação da empresa apenada. Não havendo pagamento, o valor será inscrito como dívida ativa, sujeitando a devedora a processo executivo.

7. FISCAL RESPONSÁVEL PELO ACOMPANHAMENTO DA EXECUÇÃO

7.1. Durante a vigência desta contratação, a execução do objeto será acompanhada e fiscalizada por servidor ou por representante da CONTRATANTE, devidamente designado para esse fim, permitida a assistência de terceiros.

7.2. Durante a vigência deste contrato, a CONTRATADA deve manter preposto, aceito pelo CONTRATANTE, para representá-lo sempre que for necessário.

7.3. A atestação de conformidade da execução do objeto cabe ao titular do setor responsável pela fiscalização do contrato ou a outro servidor designado para esse fim.

7.4. A fiscalização dos serviços de que trata este ato licitatório será exercida pelo Executor do Contrato, designado pelo Órgão Gerenciador.

7.5. Caberá ao CISVIR, por intermédio do Sr(a). **Daniel Felipe Reis**, Matrícula n° **630053-01** o controle e fiscalização da prestação dos serviços, conforme cada área, ou por terceiros designados pelo fiscal indicado, bem como por intermédio dos canais de comunicação com o consórcio por meio da Ouvidoria do CISVIR, podendo ocorrer aleatoriamente vistorias nas dependências da contratada.

7.6. A fiscalização exercida sobre os serviços contratados não eximirá a CONTRATADA da sua plena responsabilidade perante o CONTRATANTE, ou para com os pacientes e terceiros, decorrentes de culpa ou dolo na execução.

7.7. A CONTRATADA deverá facilitar o acompanhamento e a fiscalização permanente dos serviços e prestará todos os esclarecimentos que lhe forem solicitados do CONTRATANTE, designados para tal fim.

7.8. A CONTRATADA deve submeter-se às instruções, ordens e recomendações emitidas pelo CONTRATANTE, no sentido do aperfeiçoamento dos serviços contratados, devendo, ainda a CONTRATADA notificar ao CONTRATANTE eventuais reclamações recebidas de quaisquer alterações no procedimento de prestação dos serviços.

8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

8.1. O pagamento será efetuado com a apresentação da(s) respectiva(s) Nota(s) Fiscal(is), tendo sido cumpridos todos os critérios estabelecidos neste Termo de Referência, devidamente atestada.

8.2. Os valores da(s) Nota(s) Fiscal (is) deverão ser os mesmos consignados na Nota de Empenho, sem o qual não será liberado o respectivo pagamento. Em caso de divergência, será estabelecido prazo para a empresa fornecedora fazer a substituição desta(s) Nota(s) Fiscal(is).

8.3. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a

comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante;

8.4. Quando houver glosa parcial dos serviços, a contratante deverá comunicar a empresa para que emita a nota fiscal ou fatura com o valor exato dimensionado.

8.5. O pagamento será efetuado pela contratante no prazo de até 30 (trinta) dias contados da data do recebimento definitivo pelo CISVIR, e será feito mediante ordem bancária para crédito na conta corrente da empresa contratada, no domicílio bancário por ela expressamente informado na proposta de preço e nota fiscal.

8.6. A contratante efetuará o pagamento somente para a empresa contratada, vedada a negociação dos documentos de cobrança com terceiros, ou a sua colocação em cobrança bancária.

8.7. Caso haja aplicação de multa, o valor será descontado de qualquer nota fiscal ou crédito existente junto a CONTRATANTE em favor da CONTRATADA. Caso a mesma seja superior ao crédito eventualmente existente, a diferença será cobrada administrativamente ou judicialmente, se necessário.

8.8. A CONTRATANTE não fará nenhum pagamento à CONTRATADA, antes de paga ou relevada a multa que porventura lhe tenha sido aplicada.

8.8.1. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido de alguma forma para tanto, fica convencionado que os encargos moratórios devidos pelo Contratante, entre a data acima referida e a correspondente ao efetivo pagamento da nota fiscal/fatura, a serem incluídos na fatura do mês seguinte ao da ocorrência, são calculados por meio da aplicação da seguinte fórmula: EM = I x N x VP, onde:

EM = Encargos moratórios;

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

VP = Valor da parcela em atraso.

I = Índice de compensação financeira = 0,00016438, assim apurado:

$I = \frac{i}{365}$ $I = \frac{6/100}{365}$ ***I = 0,00016438***

Onde i = taxa percentual anual no valor de 6%.

8.9. Será retido o Imposto de Renda (IR), com base na Instrução Normativa RFB n.º 1.234, de 11 de janeiro de 2012, e alterações posteriores.

8.10. Uma vez apurado, no curso da contratação, que a CONTRATADA acresceu, indevidamente, a seus preços, valores correspondentes a tributos, contribuições fiscais e/ou parafiscais e emolumentos de qualquer natureza, não incidentes sobre a execução do objeto, tais valores serão imediatamente excluídos, com a consequente redução dos preços praticados e o reembolso dos valores porventura pagos à mesma.

8.11. Durante a vigência do contrato, os preços registrados poderão ser reajustáveis, nas hipóteses, devidamente comprovadas na ocorrência de situação previstas no art. 124, inciso II, alínea “d” da Lei nº 14.133/2021, ou de redução dos preços praticados no mercado.

8.12. Durante a vigência do Contrato, o preço inicialmente contratado poderá ser reajustado, devendo-se observar a periodicidade mínima de 12 (doze) meses, com data-base vinculada à data do orçamento estimado, tendo como limite máximo a variação do Índice de Preços ao Consumidor Amplo – IPCA.

9. ADEQUAÇÃO ORÇAMENTÁRIA

9.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados em dotação orçamentária própria do Consórcio Intermunicipal de Saúde do Vale do Ivaí e Região, conforme documento anexo.

9.1.1. A contratação será atendida pela seguinte dotação:

RE	FUNCIONAL PROGRAMÁTICA	DESPESA	FONTE	OBJETIVO
11	01.001.000460122.0001.2001	333.90.40.57	000	Serviço de processamento de dados.

9.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação do orçamento da respectiva e liberação dos da respectiva e liberação dos créditos correspondentes, mediante apostilamento.

9.3. As dotações indicadas estão sujeitas a alterações conforme as necessidades da Administração Pública.

Apucarana, PR – 11 de julho de 2024

Assinado eletronicamente por:
DANIEL FELIPE REIS
085.779.509-05
11/07/2024 14:21:31
Assinatura digital avançada com certificado digital não ICP-Brasil.

Daniel Felipe Reis
Tecnologia da Informação/Fiscal do Contrato