TERMO DE REFERÊNCIA

COMPRAS - CONTRATAÇÃO DIRETA

Processo n.27732/2023

1. DAS CONDIÇÕES GERAIS DA CONTRATAÇÃO (art. 6º, XXIII, "a" e "i" da Lei nº 14.133/2021).

1.1. Aquisição de licenças de uso de software Antivírus, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

ITEM	ESPECIFICAÇÃO	VALOR UNITÁRIO ESTIMADO	VALOR TOTAL CONTRATO ESTIMADO
1	• 25 (vinte e cinco) ***Licenças de uso do software Antívirus 36 meses.*** **1.** Especificações mínimas do Objeto Item 01 - Software antivírus **corporativo individual** Com solução gerenciada de antivírus, a qual deverá atender esta Contratante, no sentido de garantir a funcionalidades e operacionalidades de seus arquivos e serviços. **2.** Requisitos Técnicos **2.1.** Prover segurança para estações de trabalho sejam físicas ou em ambiente virtualizados em seus equipamentos e servidores; **2.2.** Possuir console central única de gerenciamento. As configurações do antivírus, AntiSpyware, Firewall, detecção de intrusão, controle de dispositivos e controle de aplicações deverão ser realizadas através da mesma console; O produto deverá ter a capacidade de remoção do software de antivírus já instalado de forma remota pela console de gerenciamento; **2.3.** O produto deverá possuir no mínimo os seguintes módulos: • Console de gerenciamento, fornecendo funcionalidades de gestão; •Módulos para estações físicas, laptops e servidores; • Módulo para ambientes virtualizados, sendo criado especialmente para ambientes virtuais.	R$ 139,48	R$ 3.487,00

1.2. O antivírus deverá ter compatibilidade para os seguintes sistemas operacionais:
1. Microsoft Windows Server 2008 x64 e R2;
2. Microsoft Windows Small Business Server 2008 (Todas edições);
3. Microsoft Windows Server 2012 e R2 (Todas edições);
4. Microsoft Windows Server 2016 (Todas edições);
5. Microsoft Windows Server 2019 (Todas edições);
6. Microsoft Windows Vista Business / Enterprise / Ultimate SP1 ou posterior;
7. Microsoft Windows Vista Business / Enterprise / Ultimate SP1 x64 ou posterior;
8. Microsoft Windows 7 Starter/ Home Basic/Home Premium/Professional/Enterprise e Ultimate;
9. Microsoft Windows 7, x64, Starter/ Home Basic/Home Premium/Professional/Enterprise e Ultimate;
10. Microsoft Windows 8 Professional / Enterprise;
11. Microsoft Windows 8 Professional / Enterprise x64;
12. Microsoft Windows 8.1 Professional / Enterprise;
13. Microsoft Windows 8.1 Professional / Enterprise x64.
14. Microsoft Windows 10 Professional / Enterprise x64
15. Suportar as seguintes plataformas virtuais: VMware: Workstation 9.x, Workstation 10.x, ESXi 5.5, ESXi 6.0 e superior;
16. Microsoft Hyper-V: 2008, 2008 R2, 2
012, 2012 R2 e 2016;
17. Oracle VM VirtualBox 4.0.4 e Superior (Somente logon como convidado);
18. Citrix XenServer 6.0 e
19. Acropolishypervisor.

2. Características:
2.1. A console deve ser acessada via WEB (HTTPS) ou MMC;
2.2. Console deve ser baseada no modelo cliente/servidor;
2.3. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
2.4. 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;
2.5. 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;
2.6. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
2.7. 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;
2.8. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
2.9. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
2.10. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
2.11. Deve integrar com Active Directory e ler acessos específicos de usuários por permissões em grupos de gerenciamento;
2.12. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
2.13. 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;

2.14. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux) protegidos pela solução antivírus;
2.15. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
2.16. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
2.17. 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;
2.18. A comunicação entre o cliente e o servidor de administração deve ser criptografada;
2.19. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes; 2.20. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:
2.20.1. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas (varredura);
2.20.2. Nome do computador;
2.20.3. Nome do domínio;
2.20.4. Range de IP;
2.20.5. Sistema Operacional;
2.20.6. Máquina virtual.
2.20.7. 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;
2.20.8. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;
2.20.9. 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; 4.20.10. 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;
2.20.11. 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.;
2.20.12. 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;
2.21. Deve fornecer as seguintes informações dos computadores:
2.21.1. Se o antivírus está instalado;
2.21.2. Se o antivírus está iniciado;
2.21.3. Se o antivírus está atualizado;
2.21.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;
2.21.5. Minutos/horas desde a última atualização de vacinas;
2.21.6. Data e horário da última verificação executada na máquina;
2.21.7. Versão do antivírus instalado na máquina;
2.21.8. Se é necessário reiniciar o computador para aplicar mudanças;
2.21.9. Data e horário de quando a máquina foi ligada;
2.21.10. Quantidade de vírus encontrados (contador) na máquina;
2.21.11. Nome do computador;
2.21.12. Domínio ou grupo de trabalho do computador;
2.21.13. Data e horário da última atualização de vacinas;
2.21.14. Sistema operacional com Service Pack.
2.22. Quantidade de processadores;
2.23. Quantidade de memória RAM;

2.24. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponível no Active Directory);
2.25. Endereço IP;
2.26. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
2.27. Atualizações do Windows Update instaladas;
2.28. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
2.29. Vulnerabilidades de aplicativos instalados na máquina;
2.30. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
2.31. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
2.31.1. Alteração de Gateway Padrão;
2.31.2. Alteração de subrede;
2.31.3. Alteração de domínio;
2.31.4. Alteração de servidor DHCP;
2.31.5. Alteração de servidor DNS;
2.31.6. Alteração de servidor WINS;
2.31.7. Alteração de subrede;
2.31.8. Resolução de Nome;
2.31.9. Disponibilidade de endereço de conexão SSL;
2.32. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
2.33. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
2.34. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
2.35. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
2.36. 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;
2.37. 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;
2.38. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML; 4.39. Capacidade de gerar traps SNMP para monitoramento de eventos;
2.40. Capacidade de enviar emails para contas específicas em caso de algum evento;
2.41. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
2.42. Deve possuir compatibilidade com Cisco Prime Infrastructure - Version: 3.1 ou superior; 2.43. Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo);
2.44. 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; 4.45. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
2.46. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

2.47. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:
2.47.1. Nome do vírus;
2.47.2. Nome do arquivo infectado;
2.47.3. Data e hora da detecção;
2.47.4. Nome da máquina ou endereço IP;
2.47.5. Ação realizada.
2.48. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
2.49. Capacidade de realizar inventário de hardware de todas as máquinas clientes;
2.50. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
2.51. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

3. Estações Windows
3.1. Compatibilidade:
3.1.1. Microsoft Windows Embedded 8.0 Standard x64;
3.1.2. Microsoft Windows Embedded 8.1 Industry Pro x64;
3.1.3. Microsoft Windows Embedded Standard 7 x86 / x64 SP1;
3.1.4. Microsoft Windows XP Professional x86 SP3 e superior;
3.1.5. Microsoft Windows Vista x86 / x64SP2 e posterior;
3.1.6. Microsoft Windows 7 Starter/ Home Basic/Home Premium/Professional/Enterprise e Ultimate x86 / x64 e posterior;
3.1.7. Microsoft Windows 8 Professional/Enterprise x86 / x64;
3.1.8. Microsoft Windows 8.1 Pro / Enterprise x86 / x64 (Todas as Versões);
3.1.5.1.9. Microsoft Windows 10 Pro / Enterprise x86 / x64 (Todas as Versões).
3.2. Características: 5.2.1. Deve prover as seguintes proteções:
3.2.1.1. 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);
3.2.1.2. Antivírus de Email (módulo para verificação de emails recebidos e enviados, assim como seus anexos);
3.2.1.3. 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;
3.2.1.5. Autoproteção (contra-ataques aos serviços/processos do antivírus);
3.2.1.6. Controle de dispositivos externos (cartões de memória, pen drive, etc);
3.2.1.7. Controle de acesso a sites por categoria; 5.2.1.8. Controle de acesso a sites por horário; 3.2.1.9. Controle de acesso a sites por usuários; 5.2.1.10. Controle de execução de aplicativos; 3.2.1.11. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
3.2.1.12. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
3.2.1.13. 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 Contratante;
3.2.1.14. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
3.2.1.15. 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);
3.2.1.16. 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; 3.2.1.17. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

3.2.1.18. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
3.2.1.19. 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;
3.2.1.20. Capacidade de verificar somente arquivos novos e alterados;
3.2.1.21. Capacidade de verificar objetos usando heurística; 5.2.1.22. Capacidade de agendar uma pausa na verificação;
3.2.1.23. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
3.2.1.24. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
3.2.1.25. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
3.2.1.25.1. Perguntar o que fazer, ou;
3.2.1.25.2. Bloquear acesso ao objeto;
3.2.1.25.3. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
3.2.1.25.4. Caso positivo de desinfecção: Restaurar o objeto para uso;
3.2.1.25.5. Caso negativo de desinfecção: Mover para quarentena ou apagar (de acordo com a configuração préestabelecida pelo administrador).
3.2.1.26. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
3.2.1.27. 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);
3.2.1.27.1. Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;
3.2.1.27.2. Capacidade de verificar links inseridos em emails contra phishings;
3.2.1.28. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Google Chrome, Opera, etc.;
3.2.1.29. Capacidade de verificação de corpo e anexos de emails usando heurística;
3.2.1.30. O antivírus de email, ao encontrar um objeto potencialmente perigoso, deve:
3.2.1.30.1. Perguntar o que fazer, ou;
3.2.1.30.2. Bloquear o email;
3.2.1.30.3. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
3.2.1.30.4. Caso positivo de desinfecção: Restaurar o email para o usuário;
3.2.1.30.5. Caso negativo de desinfecção: Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);
3.2.1.31. 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;
3.2.1.32. Capacidade de filtrar anexos de email, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
3.2.1.33. Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas;
3.2.1.34. Deve ter suporte total ao protocolo IPv6;
3.2.1.35. Capacidade de alterar as portas monitoradas pelos módulos de Web e Email.
3.2.1.36. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
3.2.1.36.1. Perguntar o que fazer, ou;
3.2.1.36.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
3.2.1.36.3. Permitir acesso ao objeto;

3.2.1.37. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
3.2.1.37.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo real, ou
3.2.1.37.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação.
3.2.1.38. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
3.2.1.39. 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;
3.2.1.40. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;
3.2.1.41. 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;
3.2.1.42. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo AntiPhishingWorkingGroup (http://www.antiphishing.org/);
3.2.1.43. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
3.2.1.44. 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;
3.2.1.45. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
3.2.1.45.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
3.2.1.45.2. 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.
3.2.1.46. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
3.2.1.46.1. Discos de armazenamento locais;
3.2.1.46.2. Armazenamento removível;
3.2.1.46.3. Impressoras;
3.2.1.46.4. CD/DVD;
3.2.1.46.5. Drives de disquete;
3.2.1.46.6. Modems;
3.2.1.46.7. Dispositivos de fita;
3.2.1.46.8. Dispositivos multifuncionais;
3.2.1.46.9. Leitores de smartcard;
3.2.1.46.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc); 5.2.1.46.11. Wi-Fi;
3.2.1.46.12. Adaptadores de rede externos;
3.2.1.46.13. Dispositivos MP3 ou smartphones;
3.2.1.46.14. Dispositivos Bluetooth;
3.2.1.46.15. Câmeras e Scanners.
3.2.1.47. 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;
3.2.1.48. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;

3.2.1.49. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
3.2.1.50. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
3.2.1.51. 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;
3.2.1.52. 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.);
3.2.1.53. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
3.2.1.54. 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;
3.2.1.55. 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;
3.2.1.56. 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.

4. Estações Linux
4.1. Compatibilidade (Plataforma 32 e 64 bits):
4.1.1. RedHat Enterprise Linux
4.2 Desktop e Superiores;
4.1.2. Fedora 16 e Superiores;
4.1.3. CentOS-6.2 e Superiores;
4.1.4. SUSE Linux Enterprise Desktop 10 SP4 e Superiores;
4.1.5. OpenSUSE Linux 12.2 e Superiores;
4.1.6. Debian GNU/Linux 6.0.5 e Superiores;
4.1.7. Mandriva Linux 2011 e Superiores;
4.1.8. Ubuntu10.04 LTS e Superiores.
4.2. Características:
4.2.1. Deve prover as seguintes proteções:
4.2.1.1. Antivírus de Arquivos Residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
4.2.1.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
4.2.1.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
4.2.1.3.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
4.2.1.3.2. 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;
4.2.1.3.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.
4.2.1.4. Verificação por agendamento:
4.2.1.4.1. Procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados);
4.2.1.4.2. Análise de arquivos; desinfecção ou remoção de objetos infectados.
4.2.1.5. Em caso de erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

4.2.1.6. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
4.2.1.7. 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;
4.2.1.8. Capacidade de verificar objetos usando heurística;
4.2.1.9. Possibilidade de escolha da pasta onde serão guardados os backups e arquivo em quarentena;
4.2.1.10. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
4.2.1.11. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNULinux).

5. Servidores Windows
5.1. Compatibilidade com Plataforma 32-bits:
5.1.1. Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);
5.1.2. Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior).
5.2. Compatibilidade com Plataforma 64-bits:
5.2.1. Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);
5.2.2. Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior);
5.2.3. Microsoft Windows Server 2008 R2 Standard / Enterprise / DataCenter (SP1 ou posterior);
5.2.4. Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter (SP1 ou posterior);
5.2.5. Microsoft Windows Storage Server 2008 R2;
5.2.6. Microsoft Windows Hyper-V Server 2008 R2 (SP1 ou posterior);
5.2.7. Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;
5.2.8. Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;
5.2.9. Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;
5.2.10. Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;
5.2.11. Microsoft Windows Storage Server 2012 (Todas edições);
5.2.12. Microsoft Windows Storage Server 2012 R2 (Todas edições);
5.2.13. Microsoft Windows Hyper-V Server 2012;
5.2.14. Microsoft Windows Hyper-V Server 2012 R2.
5.2.15. Microsoft Windows Hyper-V Server 2016.
5.2.16. Microsoft Windows Hyper-V Server 2019.
5.3. Características:
5.3.1. Deve prover as seguintes proteções:
5.3.2. Antivírus de Arquivos Residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
5.3.3. Auto-proteção contra-ataques aos serviços/processos do antivírus;
5.3.4. Firewall com IDS;
5.3.5. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
5.3.6. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
5.3.7. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
5.3.8. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

5.3.8.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
5.3.8.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
5.3.8.3. Leitura de configurações;
5.3.8.4. Modificação de configurações;
5.3.8.5. Gerenciamento de Backup e Quarentena;
5.3.8.6. Visualização de relatórios;
5.3.8.7. Gerenciamento de relatórios;
5.3.8.8. Gerenciamento de chaves de licença;
5.3.8.9. Gerenciamento de permissões (adicionar/excluir permissões acima).
5.3.9. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
5.3.9.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
5.3.9.2. 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;
5.3.9.3. 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;
5.3.9.4. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc.);
5.3.9.5. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS);
5.3.9.6. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
5.3.9.7. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
5.3.9.8. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
5.3.9.9. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;
5.3.9.10. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
5.3.9.11. 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;
5.3.9.12. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
5.3.9.13. 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;
5.3.9.14. Capacidade de verificar somente arquivos novos e alterados;
5.3.9.15. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);
5.3.9.16. Capacidade de verificar objetos usando heurística;
5.3.9.17. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
5.3.9.18. Capacidade de agendar uma pausa na verificação;
5.3.9.19. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado.
5.3.10. O Antivírus de Arquivos, ao encontrar um objeto potencialmente perigoso, deve:
5.3.10.1. Perguntar o que fazer, ou;

5.3.10.2. Bloquear acesso ao objeto;
5.3.10.3. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
5.3.10.4. Caso positivo de desinfecção: Restaurar o objeto para uso;
5.3.10.5. Caso negativo de desinfecção: Mover para quarentena ou apagar (de acordo com a configuração préestabelecida pelo administrador);
5.3.10.6. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
5.3.10.7. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
5.3.10.8. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
5.3.10.9. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

6. Servidores Linux
6.1. Compatibilidade com Plataforma 64-bits:
6.1.1. RedHat Enterprise Linux Server 7 e Superiores;
6.1.2. CentOS-7.0 e Superiores;
6.1.3. SUSE Linux Enterprise Server 12 e Superiores;
6.1.4. Novell Open Enterprise Server 11 SP2 e Superiores;
6.1.5. Ubuntu Server 14.04 LTS e Superiores;
6.1.6. Ubuntu Server 14.10 e Superiores;
6.1.7. Oracle Linux 6.5 e Superiores;
6.1.8. Debian GNU/Linux 7.5, 7.6, 7.7 e Superiores;
6.1.9. 5.6.1.9. openSUSE® 13.1 e Superiores.
6.2. Características – Deve prover as seguintes proteções:
6.2.1. Antivírus de Arquivos Residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
6.2.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
6.2.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
6.2.3.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
6.2.3.2. 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;
6.2.3.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
6.2.3.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;
6.2.3.5. Em caso de erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
6.2.3.6. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
6.2.3.7. 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;
6.2.3.8. Capacidade de verificar objetos usando heurística;
6.2.3.9. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
6.2.3.10. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

6.2.3.11. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

7. Criptografia
7.1. Compatibilidade:
7.1.1. Microsoft Windows XP Professional sp3 ou superior;
7.1.2. Microsoft Windows Vista Business/Enterprise/ultimate sp2;
7.1.3. Microsoft Windows Vista Business/Enterprise/ultimate x64 sp2;
7.1.4. Microsoft Windows 7 Starter/ Home Basic/Home Premium/Professional/Enterprise e Ultimate;
7.1.5. Microsoft Windows 7 Starter/ Home Basic/Home Premium/Professional/Enterprise e Ultimate x64;
7.1.6. Microsoft Windows 8 Professional/Enterprise;
7.1.7. Microsoft Windows 8 Professional/Enterprise x64;
7.1.8. Microsoft Windows 8.1 Professional / Enterprise;
7.1.9. Microsoft Windows 8.1 Professional / Enterprise x64;
7.1.10. Microsoft Windows 10 Pro x86 / x64; Microsoft Windows 10 Enterprise x86 /x64.
7.11. Qualificação Técnica:
7.11.1. Comprovação de aptidão para o fornecimento de bens em características, quantidades e prazos compatíveis com o objeto desta licitação, por meio da apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.
7.11.2. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:
7.11.2.1. Atestado(s) de Capacidade Técnica emitido (s) por pessoa jurídica de direito público ou privado, que comprovem aptidão da proponente para desempenho de atividades em características e quantidades semelhantes às descritas no termo de Referencia, sendo permitida a apresentação de quantos atestados forem necessários para atingir o quantitativo exigido;
7.11.2.2. O (s) atestado (s) deverá (ão) estar em nome da empresa licitante, indicar a vigência contratual, as especificações dos produtos entregues, o nome da contratante, o período e o local do fornecimento, a identificação do contrato (tipo ou natureza), quantidade de mercadorias;
7.2. Características:
7.2.1. 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;
7.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
7.2.3. Deve ter a capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
7.2.4. Deve ter a capacidade de utilizar single sign-on para a autenticação de pré-boot;
7.2.5. Permitir criar vários usuários de autenticação pré-boot;
7.2.6. 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;
7.2.7. Deve ter a capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
7.2.7.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
7.2.7.2. Criptografar todos os arquivos individualmente;
7.2.7.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
7.2.7.4. Criptografar o dispositivo removível, em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

7.2.8. 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
7.2.9. Deve ter a capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
7.2.10. Deve ter a capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
7.2.11. Verificar compatibilidade de hardware antes de aplicar a criptografia;
7.2.12. Deve ter a capacidade de estabelecer parâmetros para a senha de criptografia;
7.2.13. Bloquear o reuso de senhas;
7.2.14. Bloquear a senha após um número de tentativas pré-estabelecidas;
7.2.15. Deve ter a capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
7.2.16. Permitir criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo;
7.2.17. Permitir criptografar as seguintes pastas pré-definidas: “meus documentos”, “favoritos”, “desktop”, “arquivos temporários” e “arquivos do outlook”;
7.2.18. Permitir utilizar variáveis de ambiente para criptografar pastas customizadas;
7.2.19. Deve ter a capacidade de criptografar arquivos por grupos de extensão, tais como: documentos do office, documentos .txt, arquivos de áudio, etc.;
7.2.20. Permitir criar um grupo de extensões de arquivos a serem criptografados;
7.2.21. Deve ter a capacidade de criar regra de criptografia para arquivos gerados por aplicações;
7.2.22. Permitir criptografia de dispositivos móveis mesmo quando o Endpoint não possuir comunicação com a console de gerenciamento.

8. Gerenciamento de Sistemas
8.1.1. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
8.1.2. 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;
8.1.3. Capacidade de gerenciar licenças de softwares de terceiros;
8.1.4. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
8.1.5. 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;
8.1.6. Possibilitar fazer distribuição de software de forma manual e agendada;
8.1.7. Suportar modo de instalação silenciosa;
8.1.8. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
8.1.9. Possibilitar fazer a distribuição através de agentes de atualização;
8.1.10. Utilizar tecnologia multicast para evitar tráfego na rede;
8.1.11. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
8.1.12. Suportar modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
8.1.13. Capacidade de gerar relatórios de vulnerabilidades e patches;
8.1.14. Possibilitar criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
8.1.15. Permitir iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
8.1.16. Permitir baixar atualizações para o computador sem efetuar a instalação;

8.1.17. Permitir o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
8.1.18. Ter capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
8.1.19. Permitir selecionar produtos a serem atualizados pela console de gerenciamento;
8.1.20. Permitir selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc.

2.3. DA GARANTIA E SUPORTE

2.3.1. Os objetos deverão possuir garantia técnica mínima de 36 (trinta e seis) meses, sob a responsabilidade da CONTRATADA. A CONTRATADA deverá disponibilizar assistência técnica no período da garantia técnica;
2.3.2. No período de vigência, a Contratante 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;
2.3.3. Todas as licenças de software utilizadas para atender o objeto deverão possuir garantia de 36 (trinta e seis) meses;
2.3.4. 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);
2.3.5. O serviço de Suporte Técnico garante:
a) Reinstalação, reconfiguração e auxilio na utilização de recursos ou solução de problemas relacionados aos sistemas ofertados;
b) 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.
2.3.6. A CONTRATADA deverá prestar atendimento técnico em regime de garantia.

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO (art. 6º, inciso XXIII, alínea ‘b’ da Lei n. 14.133/2021).

3.1. Trata-se de processo para aquisição de licenças de uso de software Antivírus, fundamentados no art. 75, II, da Lei 14.133/2021.
3.2. Busca-se com a referida aquisição: Dar maior proteção contra invasores de rede; Realizar os requisitos mínimos de proteção contra criptografia ou perda de dados; Adequar os processos de contingência.
Isso tudo tendo em vista que foi constatado pela equipe técnica que a Colombo Previdência atualmente não possui nenhum tipo de programa de computador projetado para detectar, prevenir e remover eventuais softwares maliciosos.
Por essa razão, foi recomendado que, para implantar melhorias e possibilitar a prática da Política de Segurança da Informação, é necessário, dentre outras medidas, a contratação de um serviço de antivírus corporativo que possua os requisitos de proteção e gerenciamento necessários voltados à empresa.
3.3. A partir disso, prezando pela segurança da informação, com a preocupação da vulnerabilidade dos dados do RPPS e ao atendimento dos regramentos vigentes, bem como à renovação da certificação, justifica-se a aquisição deste item.

4. DO ESTUDO TÉCNICO PRELIMINAR

3.1. Por tratar-se de contratação enquadrada no art. 75, II da Lei 14.133/2021 utilizar-se-á da prerrogativa disposta na IN 58/2022 art.14, I, facultando assim a realização do Estudo Técnico Preliminar e analise de risco.

5. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERANDO O CICLO DE VIDA DO OBJETO (art. 6º, inciso XXIII, alínea 'c')

5.1. Em se tratando da necessidade de garantir segurança e proteção de dados no setor tecnológico da autarquia visando o cumprimento das obrigações, se faz indispensável aquisição das licenças de uso de software Antivírus com capacidades mínimas, prezando pela segurança da informação e com a preocupação da vulnerabilidade dos dados armazenados pelo RPPS, e visando ainda o atendimento dos regramentos vigentes e o atendimento dos critérios mínimos para renovação da certificação.
5.2. A contratação poderá ser formalizada mediante a emissão de Nota de Empenho, conforme o art. 95 da Lei n° 14.133/21.
5.3. No caso concreto, não é possível a aferição de elementos de sustentabilidade.

6. REQUISITOS DA CONTRATAÇÃO (art. 6º, XXIII, alínea 'd' da Lei nº 14.133/21)

6.1. Trata-se de aquisição de bem, a ser contratado mediante dispensa de licitação nos termos do art. 75, inciso II, da Lei nº 14.133/2021.
6.2. Não será admitida a subcontratação do objeto contratual.
6.3. É imprescindível que a contratada esteja em dia com suas obrigações tributárias, nos termos dos incisos I e III do art. 62 da Lei nº 14.133/2021.

7. VISTORIA

7.1. O objeto em tela será vistoriado pela equipe técnica de tecnologia da informação que presta serviços à Contratante, sujeito ao crivo de sua expertise.

8. MODELO DE EXECUÇÃO CONTRATUAL (arts. 6º, XXIII, alínea "e" da Lei n. 14.133/2021).

8.1. O prazo de entrega do bem será no máximo de 10 (dez) dias úteis, contados do envio da Nota de Empenho, o qual deverá ser entregue em remessa única.
8.2. O bem deverá ser entregue no endereço da seda da Contratante.
8.3. O bem será recebido provisoriamente, de forma sumária, no prazo de 05 (cinco) dias, pelo (a) responsável pelo acompanhamento e fiscalização do contrato e pela equipe técnica do TI, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta
8.4. O bem poderá ser rejeitado, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituído no prazo de 10 (dez) dias, a contar da notificação da Contratada, às suas custas, sem prejuízo da aplicação das penalidades.
8.5. Os bens serão recebidos definitivamente no prazo de 15 (quinze) dias, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.
8.6. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.
8.7. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do bem nem a responsabilidade ético-profissional pela perfeita execução do contrato.

9. MATERIAIS A SEREM DISPONIBILIZADOS

9.1. Para a perfeita execução deste contrato, a Contratada deverá disponibilizar os materiais e equipamentos que forem necessários à entrega do bem.

10. INFORMAÇÕES RELEVANTES PARA O DIMENSIONAMENTO DA PROPOSTA

A descrição técnica do bem está informada no item 1.1 deste documento.

11. DA GESTÃO DO CONTRATO (art. 6º, XXIII, alínea "f" da Lei nº 14.133/21)

11.1. ROTINAS DE FISCALIZAÇÃO CONTRATUAL

11.1.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial (Lei nº 14.133/2021, art. 115, *caput*).

11.1.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila (Lei nº 14.133/2021, art. 115, §5º).

11.1.3. O contratado será responsável pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato, e não excluirá nem reduzirá essa responsabilidade a fiscalização ou o acompanhamento pelo contratante (Lei nº 14.133/2021, art. 120).

11.1.4. Somente o contratado será responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato (Lei nº 14.133/2021, art. 121, *caput*).

11.1.4.1. A inadimplência do contratado em relação aos encargos trabalhistas, fiscais e comerciais não transferirá à Administração a responsabilidade pelo seu pagamento e não poderá onerar o objeto do contrato (Lei nº 14.133/2021, art. 121, §1º).

11.1.5. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se, excepcionalmente, o uso de mensagem eletrônica para esse fim (IN 5/2017, art. 44, §2º).

11.1.6. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato (IN 5/2017, art. 44, §3º).

11.1.7. Antes do pagamento da nota fiscal ou da fatura, deverá ser consultada a regularidade fiscal da empresa.

11.1.8. Serão exigidos a Certidão Negativa de Débito (CND) relativa a Créditos Tributários Federais e à Dívida Ativa da União, o Certificado de Regularidade do FGTS (CRF) e a Certidão Negativa de Débitos Trabalhistas (CNDT).

11.2. DOS CRITÉRIOS DE AFERIÇÃO E MEDIÇÃO PARA FATURAMENTO

11.2.1. Neste caso concreto, o fiscal do contrato e o ordenador da despesa farão a conferencia de cada nota fiscal recebida, para aferição dos valores acordados.

11.2.2. A avaliação da execução do objeto utilizará o disposto neste item, devendo haver o redimensionamento no pagamento com base nos indicadores estabelecidos, sempre que a CONTRATADA:

a) não produzir os resultados, deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

b) deixar de utilizar materiais e recursos humanos exigidos para a execução do contrato, ou utilizá-los com qualidade ou quantidade inferior à demandada.

10.3. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR (art. 6º, inciso XXIII, alínea 'h', da Lei n. 14.133/2021)

10.3.1. O fornecedor será selecionado por meio da realização de procedimento de dispensa de licitação, com fundamento na hipótese do art. 75, II, da Lei n.º 14.133/2021.

10.3.2. .Previamente à celebração do contrato, a Administração verificará o eventual descumprimento das condições para contratação, especialmente quanto à existência de sanção que a impeça mediante a consulta a cadastros informativos oficiais, tais como:
a) SICAF;
b) Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (www.portaldatransparencia.gov.br/ceis);
c) Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep)
10.3.3. A consulta aos cadastros será realizada em nome da empresa fornecedora e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.
10.3.4. Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.
10.3.5. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.
10.3.6. O fornecedor será convocado para manifestação previamente a uma eventual negativa de contratação.
10.3.7. Caso atendidas as condições para contratação, a habilitação do fornecedor será verificada por meio do SICAF, nos documentos por ele abrangidos.
10.3.8. É dever do fornecedor manter atualizada a respectiva documentação constante do SICAF, ou encaminhar, quando solicitado pela Administração, a respectiva documentação atualizada. Termo de Referência – Compras – Lei nº 14.133/21 – Contratação Direta Atualização: Junho/2022
10.3.9. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.
10.3.10. Se o fornecedor for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, caso exigidos, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.
10.3.11. Serão aceitos registros de CNPJ de fornecedor matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.
10.3.12. Para fins de contratação, deverá o fornecedor comprovar os requisitos de habilitação dos itens 10.4 e 10.5

10.4. Habilitação Jurídica:
10.4.1. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;
10.4.2. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;
10.4.3. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;
10.4.4. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

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

11.5. **Habilitações fiscal, social e trabalhista:**

11.5.1. prova de inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ);

11.5.2. prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

11.5.3. prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

11.5.4. declaração de que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

11.5.5. prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943.

11.5.6. prova de inscrição no cadastro de contribuintes municipal, se houver, relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

11.5.6.1. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

11.5.7. prova de regularidade com a Fazenda Municipal ou Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

11.5.7.1. caso o fornecedor seja considerado isento dos tributos municipais ou distritais relacionados ao objeto, deverá comprovar tal condição mediante a apresentação de certidão ou declaração da Fazenda respectiva do seu domicílio ou sede, ou por meio de outro documento equivalente, na forma da respectiva legislação de regência.

12. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

11.1. O parâmetro para obter a estimativa do valor da contratação foi aferido por meio da utilização da composição do valor da média, nos termos do art. 23 § 1º da Lei nº 14.133/2021 e art. 324 § 3º do Decreto Municipal nº 133/2021.

11.2. A tabela demonstrativa do cálculo da média segue anexo ao presente processo, juntamente com os documentos que lhe dão suporte, sendo, no caso, consultas no banco de dados junto ao PNCP, à painéis de Portal de Transparência de outras entidades, e em dados de pesquisas publicadas em mídia especializada de domínio amplo.

13. ADEQUAÇÃO ORÇAMENTÁRIA

13.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento da Autarquia.

13.1.1. A contratação será atendida pela seguinte dotação:

Órgão: 23;
Unidade: 003;
Ação: 2025;
Elemento de Despesa: 44905235 – Equipamento de processamento de dados.

13.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

Colombo, 03 de agosto de 2023.

_____

WILTON LUIZ CARRÃO
Diretor Superintendente
Ordenador da Despesa