TERMO DE REFERÊNCIA

COMPRAS - CONTRATAÇÃO DIRETA
Processo nº 35737/2026

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

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

Item	Especificação	Qt.	Valor Unitário	Valor Total
01	**1. Do módulo de proteção de endpoint** **1.1.** A solução proposta deverá proteger os sistemas operacionais abaixo: **1.1.1.** Windows 7 **1.1.2.** Windows 8 **1.1.3.** Windows 8.1 **1.1.4.** Windows 10 **1.1.5.** Windows 11 **1.2.** Servidores **1.2.1.** Windows Small Business Server 2011 **1.2.2.** Windows MultiPoint Server 2011 **1.2.3.** Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022 **1.3.** Servidores de terminal Microsoft **1.3.1.** Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022 **1.4.** Sistemas operacionais Linux de 32 bits: **1.4.1.** CentOS 6.7 e posterior **1.4.2.** Debian GNU/Linux 11.0 e posterior **1.4.3.** Debian GNU/Linux 12.0 e posterior **1.4.4.** Red Hat Enterprise Linux 6.7 e posterior **1.5.** Sistemas operacionais Linux de 64 bits: **1.5.1.** Amazon Linux 2. **1.5.2.** CentOS 6.7 e mais tarde **1.5.3.** CentOS 7.2 e posterior. **1.5.4.** CentOS Stream 8. **1.5.5.** CentOS Stream 9. **1.5.6.** Debian GNU/Linux 11.0 e posterior. **1.5.7.** Debian GNU/Linux 12.0 e posterior. **1.5.8.** Linux Mint 20.3 e superior. **1.5.9.** Linux Mint 21.1 e posterior. **1.5.10.** openSUSE Leap 15.0 e posterior. **1.5.11.** Oracle Linux 7.3 e posterior. **1.5.12.** Oracle Linux 8.0 e posterior. **1.5.13.** Oracle Linux 9.0 e posterior. **1.5.14.** Red Hat Enterprise Linux 6.7 e posterior **1.5.15.** Red Hat Enterprise Linux 7.2 e posterior. **1.5.16.** Red Hat Enterprise Linux 8.0 e posterior. **1.5.17.** Red Hat Enterprise Linux 9.0 e posterior. **1.5.18.** Rocky Linux 8.5 e posterior. **1.5.19.** Rocky Linux 9.1. **1.5.20.** SUSE Linux Enterprise Server 12.5 ou posterior. **1.5.21.** SUSE Linux Enterprise Server 15 ou posterior. **1.5.22.** Ubuntu 20.04 LTS. **1.5.23.** Ubuntu 22.04 LTS. **1.5.24.** Sistemas operacionais Arm de 64 bits: **1.5.25.** CentOS Stream 9. **1.5.26.** SUSE Linux Enterprise Server 15. **1.5.27.** Ubuntu 22.04 LTS. **1.6.** Sistemas operacionais MAC OS: **1.6.1.** macOS 12 – 14 **1.7.** Ferramentas de virtualização MAC OS:	**25**	**R$ 283,60**	**R$ 7.090,00**

	1.7.1. Parallels Desktop 16 para Mac Business Edition ou superior **1.7.2.** VMware Fusion 11.5 Profissional ou superior **1.8.** A solução proposta deverá suportar as seguintes plataformas virtuais: **1.8.1.** VMware Workstation **1.8.2.** VMware ESXi **1.8.3.** Microsoft Hyper-V Server **1.8.4.** Citrix Virtual Apps e Desktop **1.8.5.** Citrix Provisioning **2. Do módulo de gerenciamento avançado** **2.1.** A solução proposta deve suportar arquitetura cloud-native e on-premisse; **2.2.** A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de: **2.2.1.** Amazon Web Services **2.2.2.** Microsoft Azure **2.3.** A solução proposta deve incluir as seguintes opções de integração SIEM: **2.3.1.** HP (Microfoco) ArcSight **2.3.2.** IBM QRadar **2.3.3.** Splunk **2.4.** A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes. **2.5.** A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas; **2.6.** A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos. **2.7.** O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede. **2.8.** A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros. **2.9.** A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador. **2.10.** A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento. **2.11.** A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização. **2.12.** A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis. **2.13.** O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem. **2.14.** O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em uns único/múltiplos dispositivos com base nas seguintes regras de ativação: **2.14.1.** Status do dispositivo **2.14.2.** Tag **2.14.3.** Diretório ativo **2.14.4.** Proprietários de dispositivos **2.14.5.** Hardware **2.15.** A solução proposta deve suportar os seguintes canais de entrega de notificação: **2.15.1.** E-mail **2.15.2.** Registro de sistema **2.15.3.** SMS **2.16.** A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em: **2.16.1.** Atributos de rede **2.16.2.** Nome **2.16.3.** Domínio e/ou Sufixo de Domínio			

	2.16.4. Endereço de IP **2.16.5.** Endereço IP para servidor de gerenciamento **2.16.6.** Localização no Active Directory **2.16.7.** Unidade organizacional **2.16.8.** Grupo **2.16.9.** Sistema operacional **2.16.10.** Número do pacote de serviço **2.16.11.** Arquitetura Virtual **2.16.12.** Registro de aplicativos **2.16.13.** Nome da Aplicação **2.16.14.** Versão do aplicativo **2.16.15.** Fabricante **2.16.16.** Tipo e versão **2.16.17.** Arquitetura **2.17.** A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão. **2.18.** A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública. **2.19.** As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte: **2.19.1.** Dispositivos Desktop/Servidores **2.19.2.** Dispositivos móveis **2.19.3.** Dispositivos de rede **2.19.4.** Dispositivos virtuais **2.19.5.** Componentes OEM **2.19.6.** Periféricos de computador **2.19.7.** Dispositivos IoT conectados **2.19.8.** Telefones VoIP **2.19.9.** Repositórios de rede **2.20.** A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em: **2.20.1.** Nome da Aplicação **2.20.2.** Caminho do aplicativo **2.20.3.** Metadados do aplicativo **2.20.4.** Aplicativo Certificado digital **2.20.5.** Categorias de aplicativos predefinidas pelo fornecedor **2.20.6.** SHA256 e MD5 **2.21.** A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos: **2.21.1.** Bluetooth **2.21.2.** Dispositivos móveis **2.21.3.** Modems externos **2.21.4.** CD/DVD **2.21.5.** Câmeras e scanners **2.21.6.** MTPs **2.21.7.** E a transferência de dados para dispositivos móveis **2.22.** A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização. **2.23.** A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados: **2.23.1.** Estruturas de domínios e grupos de trabalho do Windows **2.23.2.** Estruturas de grupos do Active Directory **2.23.3.** Conteúdo de um arquivo de texto criado manualmente pelo administrador **2.24.** A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização. **2.25.** A solução proposta deve permitir realizar as seguintes ações para endpoints:			

	2.25.1. Verificação manual; **2.25.2.** Verificação no acesso; **2.25.3.** Verificação por demanda; **2.25.4.** Verificação de arquivos compactados **2.25.5.** Verificação de arquivos individuais, pastas e unidades; **2.25.6.** Bloqueio e verificação de scripts **2.25.7.** Proteção contra alteração de registros; **2.25.8.** Proteção contra estouro de buffer; **2.25.9.** Verificação em segundo plano/inativa **2.26.** Verificação de unidade removível na conexão com o sistema; **2.27.** A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware. **2.28.** O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas. **2.29.** A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade. **2.30.** A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc. **2.31.** A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração. **2.32.** A solução proposta deve suportar Windows Failover Cluster. **2.33.** A solução proposta deve ter um recurso de clustering integrado. **2.34.** A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus. **2.35.** A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia. **2.36.** O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança. **2.37.** A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo. **2.38.** A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux. **2.39.** A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB. **2.40.** A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB. **2.41.** A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes. **2.42.** A solução proposta deverá possuir controles para download de DLL e drivers. **2.43.** A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo especifico de prevenção de intrusão. **2.44.** A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável. **2.45.** A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log). **2.46.** A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server. **2.47.** A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço			

	IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory. **2.48.** A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las. **2.49.** A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior. **2.50.** A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários. **2.51.** A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança antimalware através do servidor de administração. **2.52.** A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários. **2.53.** A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações antimalware instalados, e para distribuir notificações sobre eventos por e-mail. **2.54.** A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração. **2.55.** A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal. **2.56.** A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc. **2.57.** A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis. **2.58.** A solução proposta deve permitir ao administrador personalizar relatórios. **2.59.** A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado. **2.60.** A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor. **2.61.** A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento. **2.62.** A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico. **2.63.** A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos. **2.64.** O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos; **2.65.** O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários. **2.66.** A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais: **2.67.** Windows **2.68.** Linux			

	3. A solução proposta deverá suportar os seguintes servidores de banco de dados: **3.1.** Windows: **3.1.1.** Microsoft SQL Server **3.1.2.** Microsoft Banco de dados SQL do Azure **3.1.3.** MySQL Standard e Enterprise **3.1.4.** MariaDB **3.1.5.** PostgreSQL **3.2.** Linux: **3.2.1.** MySQL **3.2.2.** MariaDB **3.2.3.** PostgreSQL **4.** A solução proposta deverá suportar as seguintes plataformas virtuais: **4.1.** Windows: **4.1.1.** VMware vSphere 6.7 e 7.0 **4.1.2.** Estação de trabalho VMware 16 Pro **4.1.3.** Servidor Microsoft Hyper-V 2012 de 64 bits **4.1.4.** Servidor Microsoft Hyper-V 2012 R2 de 64 bits **4.1.5.** Microsoft Servidor Hyper -V 2016 de 64 bits **4.1.6.** Servidor Microsoft Hyper-V 2019 de 64 bits **4.1.7.** Servidor Microsoft Hyper-V 2022 de 64 bits **4.1.8.** Citrix XenServer 7.1 LTSR **4.1.9.** Citrix XenServer 8.x **4.1.10.** Oracle VM VirtualBox 6.x **4.2.** Linux: **4.2.1.** VMware vSphere 6.7 e 7.0 **4.2.2.** VMware Desktop 16 Pro e 17 Pro **4.2.3.** Servidor Microsoft Hyper-V 2012 de 64 bits **4.2.4.** Servidor Microsoft Hyper-V 2012 R2 de 64 bits **4.2.5.** Microsoft Servidor Hyper -V 2016 de 64 bits **4.2.6.** Servidor Microsoft Hyper-V 2019 de 64 bits **4.2.7.** Servidor Microsoft Hyper-V 2022 de 64 bits **4.2.8.** Citrix XenServer 7.1 e 8.x **4.2.9.** Oracle VM VirtualBox 6.x e7.x **5. Do módulo de gerenciamento simplificado** **5.1.** A solução proposta deve suportar arquitetura cloud; **5.2.** A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional. **5.3.** O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque. **5.4.** A solução proposta deve permitir ao administrador gerar relatórios pré-definidos. **5.5.** A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint. **5.6.** A solução proposta deve atender as condições apontadas no item e subitens 6. **5.7.** A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS. **5.8.** A solução proposta deve incluir informações do endpoint: **5.8.1.** IP público de internet; **5.8.2.** IP interno do dispositivo; **5.8.3.** Versão do agente de proteção; **5.8.4.** Ultima comunicação com a console, contendo data e hora; **5.8.5.** Informações do sistemas operacional; **6. Requisitos gerais** **6.1.** A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças: **6.1.1.** Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados. **6.2.** A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência. **6.3.** A solução proposta deve suportar integração com Anti-malware Scan Interface			

	(AMSI). **6.4.** A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender. **6.5.** A solução proposta deve suportar o subsistema Linux no Windows. **6.6.** A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo: **6.6.1.** Proteção contra ameaças sem arquivos (Fileless); **6.6.2.** Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque; **6.7.** A solução proposta deve fornecer varredura de memória para estações de trabalho Windows; **6.8.** A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux. **6.9.** A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados. **6.10.** A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia. **6.11.** A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows. **6.12.** A solução proposta deve fornecer análise comportamental baseada em machine learning. **6.13.** A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento. **6.14.** A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint: **6.14.1.** Controles de aplicativos, **6.14.2.** Controle web e dispositivos **6.14.3.** HIPS e Firewall **6.14.4.** Descoberta de patches e vulnerabilidades de sistemas operacionais Windows; **6.15.** A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor. **6.16.** A solução proposta deve ser protegida por senha para evitar que o processo do anti-malware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema. **6.17.** A solução proposta deve ter bancos de dados de reputação locais e globais. **6.18.** A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares. **6.19.** A solução proposta deve incluir um módulo capaz, no mínimo, de: **6.19.1.** Bloqueio de aplicativos com base em sua categorização. **6.19.2.** Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos. **6.19.3.** A adição de sub-redes e a modificação de permissões de atividade. **6.20.** A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização. **6.21.** A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção. **6.22.** A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça. **6.23.** A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho. **6.24.** A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected			

	Process Light) para proteção contra ações maliciosas. **6.25.** A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo. **6.26.** A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem. **6.27.** A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas. **6.28.** A solução proposta deve ser capaz de decriptografar e verificar o tráfego de rede transmitido por conexões criptografadas. **6.29.** A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint; **6.30.** A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho; **6.31.** A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint. **6.32.** A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem. **6.33.** A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada. **6.34.** A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior. **6.35.** A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda. **6.36.** A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint. **6.37.** A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos. **6.38.** A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos. **6.39.** A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo. **6.40.** A solução proposta deve ter categoria de detecção para bloquear banners de sites. **6.41.** A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis; **6.42.** A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos. **6.43.** A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais. **6.44.** A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP. **6.45.** A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo; **6.46.** A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões. **6.47.** A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos. **6.48.** A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem. **6.49.** O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.			

	6.50. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões. **6.51.** A solução proposta deve suportar o controle de scripts executados em PowerShell. **6.52.** A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados. **6.53.** A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo. **6.54.** A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem. **6.55.** A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor. **6.56.** A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas. **6.57.** A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint. **6.58.** A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com: **6.58.1.** Filtro de anexos. **6.58.2.** Verificação de mensagens de email ao receber, ler e enviar. **6.59.** A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo. **6.60.** A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo; **6.61.** A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.); **6.62.** A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware. **6.63.** A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio. **6.64.** A solução proposta deve incluir suporte ao protocolo IPv6. **6.65.** A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente. **6.66.** A solução proposta deve incorporar a tecnologia de autoproteção de aplicação: **6.67.** Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo. **6.68.** Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários. **6.69.** A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar. **6.70.** A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha. **6.71.** A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística. **6.72.** A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail. **6.73.** A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária. **6.74.** A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows. **6.75.** A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.			

	6.76. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia , bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça. **6.77.** A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft. **6.78.** A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização. **6.79.** A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição. **6.80.** A solução proposta deve suportar endereços IPv6. **6.81.** A solução proposta deve suportar verificação em duas etapas (autenticação). **6.82.** A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento. **6.83.** A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração. **6.84.** A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente. **6.85.** A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes. **6.86.** A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware. **6.87.** A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas. **6.88.** A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas. **6.89.** A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos. **6.90.** A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet. **6.91.** A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi , Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor. **6.92.** A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes. **6.93.** A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS. **6.94.** A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de endpoint está instalado. **6.95.** A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração. **6.96.** A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos. **6.97.** A solução proposta deve ter a capacidade de excluir atualizações baixadas. **6.98.** A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados. **6.99.** A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português. **6.100.** A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints. **6.101.** A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos. **6.102.** Os relatórios da solução proposta devem incluir informações sobre cada ameaça			

	e a tecnologia que a detectou. **6.103.** A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor. **6.104.** A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional. **6.105.** A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor. **6.106.** A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo: **6.106.1.** Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível. **6.106.2.** Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica. **6.107.** A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados. **6.108.** A solução proposta deve gerar relatorios de vulnerabilidades encontradas nos dispositivos com sensor de endpoint instalado. **7. Do modulo de gerenciamento de dispositivos móveis** **7.1.** O modulo deve ser integrado a console de gerenciamento; **7.2.** A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android: **7.2.1.** Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition) **7.3.** A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS: **7.3.1.** iOS 10–17 ou iPadOS 13–17 **7.4.** A solução proposta deve oferecer suporte a dispositivos Android Device Owner. **7.5.** A solução proposta deve suportar dispositivos iOS supervisionados. **7.6.** A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador. **7.7.** A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras. **7.8.** A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões. **7.9.** A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais). **7.10.** A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário. **7.11.** A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps. **7.12.** A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado. **7.13.** A solução proposta deve ter recursos de conteinerização para dispositivos Android. **7.14.** A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android: **7.14.1.** Dados em contêineres **7.14.2.** Contas de e-mail corporativo **7.14.3.** Configurações para conexão à rede Wi-Fi corporativa e VPN **7.14.4.** Nome do ponto de acesso (APN) **7.14.5.** Perfil do Android for Work **7.14.6.** Recipiente KNOX			

	7.14.7. Chave do gerenciador de licença KNOX **7.15.** A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS: **7.15.1.** Todos os perfis de configuração instalados **7.15.2.** Todos os perfis de provisionamento **7.15.3.** O perfil iOS MDM **7.16.** Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas **7.17.** A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo . **7.18.** A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controlo de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes: **7.18.1.** Critérios de verificação do dispositivo; **7.18.2.** Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido; **7.19.** A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc. **7.20.** A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo: **7.20.1.** Cartões de memória e outras unidades removíveis **7.20.2.** Câmera do dispositivo **7.20.3.** Conexões Wi-Fi **7.20.4.** Conexões Bluetooth **7.20.5.** Porta de conexão infravermelha **7.20.6.** Ativação do ponto de acesso Wi-Fi **7.20.7.** Conexão de área de trabalho remota **7.20.8.** Sincronização de área de trabalho **7.20.9.** Definir configurações da caixa de correio do Exchange **7.20.10.** Configurar caixa de e-mail em dispositivos iOS MDM **7.20.11.** Configure contêineres Samsung KNOX. **7.20.12.** Definir as configurações do perfil do Android for Work **7.20.13.** Configurar e-mail/calendário/contatos **7.20.14.** Defina as configurações de restrição de conteúdo de mídia. **7.20.15.** Definir configurações de proxy no dispositivo móvel **7.20.16.** Configurar certificados e SCEP **7.21.** A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay . **7.22.** A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel: **7.22.1.** Portal de inscrição móvel KNOX **7.22.2.** Pacotes de instalação pré-configurados independentes **7.23.** A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel. **7.24.** A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente. **7.25.** A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros: **7.25.1.** VMware AirWatch 9.3 ou posterior **7.25.2.** MobileIron 10.0 ou posterior **7.25.3.** IBM MaaS360 10.68 ou posterior **7.25.4.** Microsoft Intune 1908 ou posterior **7.25.5.** SOTI MobiControl 14.1.4 (1693) ou posterior			

	7.26. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo. **7.27.** A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo. **7.28.** A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo. **7.29.** A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento. **7.30.** A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena. **7.31.** A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos. **7.32.** A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente. **7.33.** A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores. **7.34.** A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente. **7.35.** A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel. **7.36.** A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis. **7.37.** A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel. **7.38.** A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido. **7.39.** A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes; **7.40.** A solução proposta deve proteger contra ameaças online em dispositivos iOS. **8. Do módulo de EDR** **8.1.** Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta. **8.2.** Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados. **8.3.** A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças; **8.4.** Deve apresentar as seguintes informações: **8.4.1.** Processo; **8.4.2.** Arquivos; **8.4.3.** Chaves de registros; **8.4.4.** Conexões de rede; **8.4.5.** SHA256 e MD5; **8.5.** Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise; **8.6.** Deve apresentar informações detalhadas contendo: **8.6.1.** Usuário que executou a ação; **8.6.2.** Informações acesso privilegiado; **9. Requisitos para documentação da solução.** **9.1.** A documentação da solução do anti-malware incluindo ferramentas de administração, deve incluir os seguintes documentos: **9.2.** Ajuda on-line para administradores **9.3.** Ajuda on-line para melhores práticas de implementação **9.4.** Ajuda on-line para proteção de servidores de administração **9.5.** A documentação do software anti-malware fornecida deve descrever			

	detalhadamente os processos de instalação, configuração e uso do software anti-malware. **9.6.** Deve estar disponível página com informações de ciclo de vida das soluções e módulos.			
			TOTAL	**R$ 7.090,00**

1.2. DA GARANTIA E SUPORTE

1.2.1. O objeto deverá possuir garantia técnica mínima de 36 (trinta e seis) meses, sob a responsabilidade da CONTRATADA. O fornecedor deverá disponibilizar assistência técnica durante todo o período da garantia;

1.2.2. 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;

1.2.3. Todas as licenças de software utilizadas para atender o objeto deverão possuir garantia de 36 (trinta e seis) meses;

1.2.4. A Licitante vencedora deverá prestar suporte técnico e operacional durante o período de vigência da licença, com atendimento através do serviço telefônico, 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);

1.2.5. 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.

1.2.6. A CONTRATADA deverá prestar atendimento técnico em regime de garantia.

1.3. O prazo de vigência da contratação é de 36 (trinta e seis) meses contados da emissão da Nota de Empenho, na forma do artigo 105 da Lei n° 14.133, de 2021.

1.3.1. O prazo de vigência desta Dispensa Eletrônica poderá ser prorrogado, por igual período, desde que comprovado o preço vantajoso para a administração, nos termos do Art. 107 da lei 14.133/21.

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

2.1. Trata-se de processo para aquisição de licenças de uso de software Antivírus, fundamentados no art. 75, II, da Lei 14.133/2021.

2.2. Busca-se, por meio da referida aquisição, garantir a devida proteção dos arquivos virtuais contra acessos não autorizados e possíveis invasões à rede, bem como atender aos requisitos mínimos de segurança relacionados à prevenção de criptografia indevida e à perda de dados, além de adequar e fortalecer os processos de contingência.

Considerando que a licença anteriormente adquirida pela Colombo Previdência encontra-se próxima do vencimento, e tendo em vista que o serviço é essencial para assegurar a proteção, a segurança e a privacidade dos dados armazenados, faz-se necessária a continuidade da contratação, de modo a evitar a interrupção da proteção e garantir a integridade, a disponibilidade e a confidencialidade das informações institucionais.

3. 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 análise de risco.

4. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO (art. 6º, inciso XXIII, alínea 'c' da Lei nº 14.133/21)

4.1. Considerando a necessidade de garantir a segurança e a proteção dos dados no ambiente tecnológico da autarquia, bem como o cumprimento das obrigações institucionais e dos regramentos vigentes, torna-se indispensável a aquisição de licenças de uso de software antivírus, com capacidades e recursos mínimos adequados às necessidades do órgão. A contratação visa fortalecer a segurança da informação, reduzir os riscos relacionados a vulnerabilidades e ameaças cibernéticas e proteger os dados armazenados e processados pelo Regime Próprio de Previdência Social. Além disso, busca-se assegurar a continuidade e a confiabilidade dos serviços tecnológicos, bem como atender aos critérios e requisitos mínimos necessários à manutenção e à renovação da certificação institucional.

4.2. A contratação poderá ser formalizada mediante a emissão de Nota de Empenho, conforme o art. 95 da Lei nº 14.133/2021.

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

5.1. A contratação será realizada por meio de processo de Dispensa Eletrônica, nos termos previstos no art. 75 II da Lei 14.133/2021.

5.2. A Dispensa terá vigência de 36 (trinta e seis) meses.

5.3. Não será admitida a subcontratação do objeto contratual.

5.4. 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.

6. VISTORIA

6.1. O objeto em tela dispensa a avaliação prévia deste contrato.

7. MODELO DE EXECUÇÃO CONTRATUAL (art. 6º, inciso XXIII, alínea 'e' da Lei n. 14.133/2021).

7.1. 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.

7.2. O produto deverá ser entregue na sede da Contratante.

7.3. O material será recebido e conferido no ato da entrega por servidor responsável sendo verificado a qualidade e a quantidade em conformidade com as especificações constantes neste Termo de Referência e na proposta.

7.4. O material 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 05 (cinco) dias, a contar da notificação da Contratada, às suas custas, sem prejuízo da aplicação das penalidades.

8. MATERIAIS A SEREM DISPONIBILIZADOS

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

9. INFORMAÇÕES RELEVANTES PARA O DIMENSIONAMENTO DA PROPOSTA

9.1. A descrição técnica do produto está devidamente informada entre os itens 1.1 e 1.9 deste documento.

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

10.1. 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.

10.2. 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.

10.3. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

10.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

10.5. Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

10.6. A execução do contrato deverá ser acompanhada e fiscalizada pelo fiscal do contrato, ou pelo respectivo substituto (Lei nº 14.133, de 2021, art. 117, caput).

10.7. Identificada qualquer inexatidão ou irregularidade, o fiscal do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

10.7.1. O fiscal do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

10.7.2. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal do contrato comunicará o fato imediatamente ao gestor do contrato.

10.7.3. O fiscal do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.

10.7.4. O fiscal do contrato verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

10.7.5. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência.
10.8. O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.
10.8.1. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.
10.8.2. O gestor do contrato acompanhará os registros realizados pelo fiscal do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência..
10.8.3. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelo fiscal quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.
10.8.4. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 151.10 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso.
10.9. O gestor do contrato deverá elaborará relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.

11. DOS CRITÉRIOS DE AFERIÇÃO E MEDIÇÃO PARA FATURAMENTO

11.1. Neste caso concreto, o fiscal do contrato e o ordenador da despesa farão a conferência da nota fiscal recebida, para aferição dos valores acordados.
11.2. 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 serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

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

12.1. O fornecedor será selecionado por meio da realização de procedimento de dispensa eletrônica de licitação, com fundamento na hipótese do art. 75, II, da Lei n.º 14.133/2021.
12.2. 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)
12.3. 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.
12.4. 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.
12.5. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.
12.6. O fornecedor será convocado para manifestação previamente a uma eventual negativa de contratação.

12.7. Caso atendidas as condições para contratação, a habilitação do fornecedor será verificada por meio do SICAF, nos documentos por ele abrangidos.
12.8. É dever do fornecedor manter atualizada a respectiva documentação constante do SICAF, ou encaminhar, quando solicitado pela Administração, a respectiva documentação atualizada.
12.9. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.
12.10. 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.
12.11. 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.
12.12. Para fins de contratação, deverá o fornecedor comprovar os requisitos de habilitação dos itens 12.12.1 e 12.12.2
12.12.1. Habilitação Jurídica:
12.12.1.1. 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;
12.12.1.2. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;
12.12.1.3. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;
12.12.1.4. 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.
12.12.2. Habilitações fiscal, social e trabalhista:
12.12.2.1. Prova de inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ);
12.12.2.2. 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.
12.12.2.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);
12.12.2.4. 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;
12.12.2.5. 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.
12.12.2.6. 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;
12.12.2.6.1. 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.
12.12.2.7. Prova de regularidade com a Fazenda Municipal ou Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;
12.12.2.7.1. 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.

13. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

13.1. O parâmetro para obter a estimativa do valor da aquisição foi aferido por meio da utilização da composição do valor da mediana, nos termos do art. 23 § 1º da Lei nº 14.133/2021.

13.2. A tabela demonstrativa do cálculo da mediana segue anexo ao presente processo, juntamente com os documentos que lhe dão suporte, sendo, no caso, consultas no banco de dados junto ao PNCP e em painéis de Portal de Transparência de outras entidades.
13.3. O custo estimado total da contratação é de R$ 7.090,00 (sete mil e noventa reais), conforme custos unitários apostos na tabela no tópico 1.1.

14. ADEQUAÇÃO ORÇAMENTÁRIA:
14.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no orçamento da autarquia.
14.2. A contratação será atendida pela seguinte dotação:
Órgão: 02;
Unidade: 03;
Ação: 2025;
Elemento de Despesa: 33903047000000 - Aquisição de software de base.
14.3. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

Colombo, 19 de agosto de 2026.

gov.br Documento assinado digitalmente
WILTON LUIZ CARRAO
Data: 25/08/2026 08:39:00-0300
Verifique em https://validar.iti.gov.br

Wilton Luiz Carrão
Diretor Superintendente

gov.br Documento assinado digitalmente
JOICE LAGOS MARONE
Data: 20/08/2026 11:24:04-0300
Verifique em https://validar.iti.gov.br

Joice Lagos Marone
Gestor do Contrato

gov.br Documento assinado digitalmente
ALINE PESSINI DE ALMEIDA
Data: 24/08/2026 13:32:05-0300
Verifique em https://validar.iti.gov.br

Aline Pessini de Almeida
Fiscal de Contrato

gov.br Documento assinado digitalmente
LUIZ VANDERLEY DALLASUANNA
Data: 20/08/2026 10:31:22-0300
Verifique em https://validar.iti.gov.br

Luiz Vanderley Dallasuanna
Elaborador do Termo de Referência