CONTRATO DE FORNECIMENTO FIRMADO ENTRE A CEASAMINAS E A TEC HOUSE INFORMÁTICA LTDA

Por este instrumento, em decorrência do Procedimento Interno 27/2021, a CENTRAIS DE ABASTECIMENTO DE MINAS GERAIS S/A – CEASAMINAS, sob controle acionário da União, sediada às margens da BR 040, km 688, s/nº., em Contagem/MG, CEP: 32145-900, Fone: 3399-2122, Fax: 3394-2709, CNPJ - 17.504.325/0001-04, representada pelos Diretores, infra-assinados, ora denominada **CEASAMINAS**, e a empresa TEC HOUSE INFORMÁTICA LTDA, com endereço na Rua Itaquera, 811, Jardim Stella, Santo André/SP, CEP 09.185-690, CNPJ 06.699.202/0001.50, na sequência denominada **CONTRATADA**, representada na sua forma contratual, resolvem, para aquisição parcelada dos serviços constantes neste contrato e nos termos do Procedimento Interno nº 27/2021, com base na Lei n.º 13.303/2016, no Decreto n.º 10.024/2019 e nas cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1 – Fornecimento de licenciamento de software antivírus e suporte técnico pelo período de 2 (dois) anos para um total de 250 usuários, conforme as especificações do Anexo I (Termo de Referência) e das Cláusulas deste contrato.

1.2 – Integram o presente contrato, como se nele transcritos, toda a documentação referente ao procedimento interno nº 27/2021, a proposta da Contratada e a documentação exibida.

CLÁUSULA SEGUNDA - REQUISITOS MÍNIMOS PARA A SOLUÇÃO DE ANTIVÍRUS

2.1 – Possuir uma única console de gerenciamento para gestão e configurações do antivírus, antispyware, firewall, detecção de intrusão, controle de dispositivos, controle de aplicações e criptografia de discos.

2.2 – A solução deverá ter a capacidade de remoção do atual antivírus instalado e ser capaz de instalar de forma remota o agente do antivírus pela console de gerenciamento e, caso não tenha a capacidade de realização da remoção completa, a contratada deverá remover a atual solução utilizando scripts, softwares de terceiros, ou mesmo de forma manual;

2.3 – O produto deverá possuir no mínimo os seguintes módulos e funcionalidades:

2.3.1 – Console de gerenciamento fornecendo funcionalidades de gestão e configurações de políticas;

2.3.2 – Módulos para estações físicas, notebooks e servidores;

2.3.3 – Módulo para ambientes virtualizados, sendo criado especialmente para ambientes virtuais;

2.3.4 – Módulo para dispositivos móveis no mínimo para tablets e smartphones com sistema operacional iOS e Android;

2.3.5 – Utilizar o conceito de heurística para combate e ações contra possíveis malwares;

2.3.6 – Oferecer tecnologia onde a solução explore vulnerabilidades de softwares instalados no intuito de reduzir o risco de infecções (anti-exploit);

2.3.7 – Oferecer tecnologia nativa no intuito de eliminar ameaças que sequestram dados, do tipo ransomware;

2.3.8 – Oferecer inventário de softwares;

2.3.9 – Oferecer tecnologia onde a solução teste arquivos potencialmente perigosos em ambiente isolado antes da execução do mesmo no ambiente de produção;

2.3.10 – Oferecer proteção por base de assinaturas (vacinas).

2.4 – Console de gerenciamento:

2.4.1 – Instalação e configuração

2.4.2 – Permitir instalação de console local (on-premise) com banco de dados local ou instalação em nuvem (cloud) com banco de dados também em nuvem;

2.4.3 – Para a opção de console local de ser fornecido como um appliance virtual ou executável para instalação em servidores Windows. Deverá suportar no mínimo as seguintes plataformas de virtualização:

2.4.3.1 – VMWare vSphere;

2.4.3.2 – Citrix XenServer; XenDesktop, VDI-in-a-Box;

2.4.3.3 – Microsoft Hyper-V;

2.4.3.4 – Red hat Enterprise Virtualization;

2.4.3.5 – Kernel-based Virtual Machine ou KVM;

2.4.3.6 – Oracle VM;

2.4.4 – Deverá ser fornecido com base de dados embutida e proprietária ou com possibilidade de utilização de banco de dados externo SQL ou Oracle;

2.4.5 – Para instalação da console em nuvem (cloud), a nuvem deve ser privada e do mesmo fabricante;

2.4.6 – Permitir instalação remota via console WEB de gerenciamento para ambientes virtuais VMWare ou Citrix;

2.4.7 – O mecanismo de varredura deverá estar disponível para download separadamente;

2.4.8 – A solução deverá permitir a inclusão de um modulo de balanceamento para casos em que vários servidores tenham a mesma função (para alta disponibilidade, recuperação de desastres, performance, dentre outras necessidades);

2.4.9 – Deve ser totalmente em português.

2.5 – Funcionalidades Gerais:

2.5.1 – Licenciamento flexível;

2.5.2 – A console de gerenciamento deve incluir informações detalhadas sobre as estações e servidores com no mínimo as seguintes informações:

2.5.2.1 – Nome;

2.5.2.2 – IP;

2.5.2.3 – Sistema Operacional;

2.5.2.4 – Política Aplicada;

2.5.3 – A console de gerenciamento deverá incluir sessão de log com as seguintes informações:

2.5.3.1 – Login;

2.5.3.2 – Edição;

2.5.3.3 – Criação;

2.5.3.4 – Log-out;

2.5.4 – Arquitetura simples de atualização, com um simples clique deve ser possível atualizar todas funções e serviços da solução;

2.5.5 – Permitir que o administrador escolha qual o pacote será atualizado;

2.5.6 – As notificações devem ser destacadas como item não lido e notificar o administrador por e-mail;

2.5.7 – No mínimo enviar notificações para as seguintes ocorrências:

2.5.7.1 – Problemas com licenças;

2.5.7.2 – Alertas de surto de vírus;

2.5.7.3 – Máquinas desatualizadas;

2.5.7.4 – Eventos de antimalware.

2.5.8 – Deverá prover o acesso via HTTPS;

2.5.9 – Deverá permitir a importação de certificados digitais;

2.5.10 – O gerenciamento e a comunicação com dispositivos móveis deve ser feito de forma segura utilizando certificados digitais.

2.6 – Monitoramento:

2.6.1 – Baseado em "portlets" configuráveis com no mínimo as seguintes especificações:

2.6.1.1 – Nome;

2.6.1.2 – Tipo de relatório;

2.6.1.3 – Alvo do relatório;

2.6.2 – Deverá disponibilizar "portlets" para gerência e monitoramento de qualquer tipo de endpoint, máquinas físicas, virtuais e dispositivos móveis.

2.7 – Inventário da Rede:

2.7.1 – Possuir no mínimo as integrações abaixo:

2.7.1.1 – Múltiplos domínios do Active Directory;

2.7.1.2 – Múltiplos VMWare vCenters;

2.7.1.3 – Múltiplos Citrix Xen Servers;

2.7.2 – Possuir a possibilidade de definição de sincronização com o Active Directory em horas;

2.7.3 – Descoberta de rede para máquinas em grupo de trabalho;

2.7.4 – Possuir busca em tempo real pelo menos com os seguintes filtros:

2.7.4.1 – Nome;

2.7.4.2 – Sistema Operacional;

2.7.4.3 – Endereço IP;

2.7.5 – Possibilitar a instalação remota e desinstalação remota do antivírus;

2.7.6 – Possibilitar a configuração de pacotes de instalação do produto de antivírus;

2.7.7 – Possuir tarefas remotas e configuráveis de scan;

2.7.8 – Possuir tarefa de reinicialização remota de estação ou servidor;

2.7.9 – Assinar políticas para no mínimo os níveis:

2.7.9.1 – Computador;

2.7.9.2 – Máquina Virtual;

2.7.9.3 – Grupo de Endpoints;

2.7.9.4 – Usuário do AD;

2.7.9.5 – Grupo do AD.

2.7.10 – Possuir a propriedade detalhada de objetos gerenciados para:

2.7.10.1 – Nome;

2.7.10.2 – IP;

2.7.10.3 – Sistema Operacional;

2.7.10.4 – Grupo;

2.7.10.5 – Política Assinada;

2.7.10.6 – Ultimo status de malware.

2.8 – Políticas:

2.8.1 – Modelo único para todos os equipamentos, sejam físicos ou virtuais;

2.8.2 – Cada serviço de segurança deve ter seu modelo configurável de política com opções específicas de ativar/desativar;

2.8.3 – Através da console de gerenciamento o administrador poderá ser capaz de enviar uma política única para configurar o antivírus;

2.8.4 – Deverá configurar as funcionalidades como escaneamento do antivírus, firewall de duas vias de detecção de intrusão, controle de acesso a rede, controle de aplicação, controle de acesso web, criptografia (Windows, Mac e Android), localização de dispositivo (Mobile), autenticação e ações para serem aplicadas em caso de vírus e dispositivos em não conformidade.

2.9 – Relatórios:

2.9.1 – Deverão apresentar as seguintes funcionalidades:

2.9.1.1 – Relatório para cada serviço de segurança;

2.9.1.2 – Facilidade de usar e visualização simplificada;

2.9.1.3 – Agendamento, com opção de envio por e-mail para qualquer destinatário conforme escolha do administrador;

2.9.1.4 – Filtros de agendamento de relatórios;

2.9.1.5 – Arquivo com todas as instâncias de relatório agendados;

2.9.1.6 – Exportar o relatório nos formatos .pdf e/ou .csv;

2.9.1.7 – Oferecer possibilidade de criar relatórios de maneira dinâmica no dashboard da da console de gerenciamento.

2.10 – Administração de Usuários

2.10.1 – Deverá apresentar no mínimo as seguintes funcionalidades:

2.10.1.1 – Administração baseada em regras;

2.10.1.2 – Disponibilizar tipos de usuários pré-definidos como no mínimo:

2.10.1.2.1 – Administrador – Gerente dos componentes da solução;

2.10.1.2.2 – Administrador de rede - Gerente dos serviços de segurança;

2.10.1.2.3 – Relatório – Monitora e cria relatórios;

2.10.1.3 – Deverá ser possível customizar um tipo de usuário:

2.10.1.3.1 – Deverá permitir a integração de usuários com o Active Directory para autenticação da console de gerenciamento;

2.10.1.3.2 – Registrar as ações do usuário na console de gerenciamento;

2.10.1.3.3 – Detalhar cada ação do usuário;

2.10.1.3.4 – Permitir busca complexa baseada em ações do usuário, intervalos de tempo.

2.11 – Segurança para estações e servidores

2.11.1 – Proteção para ambientes físicos.

2.11.2 – Deverá proteger em tempo real e agendado as máquinas físicas em qualquer plataforma de sistema operacional, seja Windows, Linux ou Mac, tanto na console local (on-premises) como na console em nuvem (cloud);

2.11.3 – Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho:

2.11.3.1 – Windows 10 64Bits;

2.11.3.2 – Windows 8.1 64Bits;

2.11.3.3 – Windows 8 64Bits;

2.11.3.4 – Windows 7 64Bits;

2.11.4 – Deverá suportar no mínimo os seguintes sistemas operacionais para servidores:

2.11.4.1 – Windows Server 2012R2;

2.11.4.2 – Windows Server 2012;

2.11.4.3 – Windows Server 2008 R2;

2.11.4.4 – Windows Server 2008 apenas os módulos de antivírus e Active Virus Control;

2.11.5 – Deverá suportar no mínimo os seguintes sistemas operacionais para distribuição Linux:

2.11.5.1 – Ubuntu 14.04 LTS ou superior;

2.11.5.2 – Red Hat Enterprise Linux / CentOS 6 ou superior;

2.11.5.3 – SUSE Linux Enterprise Server 11 SP4 ou superior;

2.11.5.4 – OpenSUSE Leap 42.x;

2.11.5.5 – Fedora 25 ou superior;

2.11.5.6 – Debian 8.0 ou superior;

2.11.5.7 – Oracle Linux 6.3 ou superior;

2.11.5.8 – Amazon Linux AMI 2016.09 ou superior;

2.11.5.9 – Proteção para ambientes virtuais;

2.11.6 – Para plataforma de virtualização com VMWare, deverá:

2.11.6.1 – Ter a disponibilidade de ser integrado e oferecer a escaneamento sem instalar o agente nas máquinas virtuais;

2.11.6.2 – A console de gerenciamento central da solução deverá ter a possibilidade de integrar com múltiplos vCenters da VMWare;

2.11.6.3 – Deverá proteger em tempo real e agendado as máquinas virtuais em qualquer plataforma de sistema operacional, seja Windows, Linux ou Mac, tanto na console local (on-premises) como na console em nuvem (cloud);

2.11.7 – O produto deverá oferecer agente para virtualização dos seguintes produtos:

2.11.7.1 – Citrix Xen Server;

2.11.7.2 – Microsoft Hyper-V;

2.11.7.3 – VMware ESXi;

2.11.7.4 – Red Hat Virtualization;

2.11.7.5 – Oracle KVM;

2.11.7.6 – KVM;

2.11.7.7 – Instalação e Configuração Remota;

2.11.8 – Deverá permitir ao administrador customizar a instalação;

2.11.9 – Deverá permitir a instalação customizada do antivírus com no mínimo:

2.11.9.1 – Instalar o antivírus sem o controle de acesso a internet; (Windows Desktop)

2.11.9.2 – Instalar o antivírus sem o módulo de firewall; (Windows Desktop)

2.11.10 – A instalação deverá ser possível de executar no mínimo das seguintes maneiras:

2.11.10.1 – Executar o pacote de antivírus diretamente na estação de trabalho;

2.11.10.2 – Instalar remotamente, distribuído via console de gerencia web;

2.11.11 – Deverá ser possível ter um relatório com as estações instaladas e as faltantes da instalação;

2.11.12 – Ter a capacidade de criar um único pacote independente ser for para 32 bits ou 64 bits;

2.11.13 – Deverá permitir ao administrador criar grupos e subgrupos para mover as estações de trabalho;

2.11.14 – O agente utilizado na sincronização deve ser incluído no cliente do antivírus e não ser necessário a distribuição em um agente separado.

2.12 – Funções Gerais

2.12.1 – Deverá ter métodos de detecção de vírus, spyware, rootkits e outros mecanismos de segurança;

2.12.2 – Deverá permitir a configuração do scan do antivírus do cliente como:

2.12.2.1 – Scan local;

2.12.2.2 – Scan hibrido (local\remoto);

2.12.2.3 – Scan remoto;

2.12.3 – Deverá reportar o estado atual das máquinas virtuais no mínimo, protegida/desprotegida;

2.12.4 – Deverá fazer scan em tempo real e automático;

2.12.5 – Deverá ser configurável para não escanear arquivos conforme necessidade do administrador, ou seja, por tamanho ou por tipo de extensão;

2.12.6 – Deverá possuir escaneamento baseado em análise heurística;

2.12.7 – Deverá permitir a escolha e configuração de pastas a serem scaneadas;

2.12.8 – Para melhor proteção, o antivírus deverá ter no mínimo 3 tipos de detecção:

2.12.8.1 – Baseada em assinaturas;

2.12.8.2 –Baseada em heurística;

2.12.8.3 –Baseada em monitoramento contínuo de processos;

2.12.9 – Deverá ter a capacidade de escaneamento nos protocolos HTTP e SSL nas estações de trabalho;

2.12.10 – O cliente do antivírus deverá ter o módulo de Antiphishing que deverá ter a opção de verificar links pesquisados com os sites de pesquisas Search Advisor nas estações de trabalho;

2.12.11 – Deverá possuir módulo de firewall que de acordo com o administrador poderá ou não ser instalado/desinstalado nas estações de trabalho;

2.12.12 – No módulo de firewall deverá ser possível configurar o modo invisível tanto a nível de rede local ou Internet nas estações de trabalho;

2.12.13 – Deverá ter os seguintes requisitos mínimos de sistema:

2.12.13.1 – Plataformas de Virtualização

2.12.13.2 – VMware vSphere ESX 5.0 ou superior;

2.12.13.3 – VMware vCenter Server 4.1 ou superior;

2.12.13.4 – Citrix XenDesktop 5.0 ou superior;

2.12.13.5 – Xen Server 5.5 ou superior;

2.12.13.6 – Citrix VDI-in-a-Box 5;

2.12.13.7 – Microsoft Hyper-V Server 2008 R2, 2012

2.12.13.8 – Oracle VM 3.0;

2.12.13.9 – Red Hat Enterprise Virtualization 3.0.

2.12.13.10 – Sistemas Operacionais para Desktops

2.12.13.11 – Windows 10 64Bits;

2.12.13.12 – Windows 8.1 64Bits;

2.12.13.13 – Windows 8 64Bits;

2.12.13.14 – Windows 7 64Bits;

2.12.13.15 – Sistemas Operacionais para Servidores;

2.12.13.16 – Windows Server 2012R2;

2.12.13.17 – Windows Server 2012;

2.12.13.18 – Windows Server 2008 R2;

2.12.13.19 – Windows Server 2008 apenas os módulos de antivírus e Active Virus Control;

2.12.13.20 – L inux Red Hat Enterprise;

2.12.13.21 – CentOS 5.6 ou superior;

2.12.13.22 – Ubuntu 10.04 LTS ou superior;

2.12.13.23 – SUSE Linux Enterprise Server 11 ou superior;

2.12.13.24 – OpenSUSE 11 ou superior;

2.12.13.25 – Fedora 15 ou superior;

2.12.13.26 – Debian 5.0 ou superior.

2.13 – Quarentena

2.13.1 – Deverá permitir restauração remota, com configuração de localidade e deleção;

2.13.2 – Criação e exclusão para arquivos restaurados;

2.13.3 – Deverá permitir o envio automático de arquivos da quarentena para o laboratório de vírus;

2.13.4 – Deverá fazer a remoção automática de arquivos antigos, pré-definidos pelo administrador;

2.13.5 – Deverá permitir a movimentação do arquivo da quarentena para seu local original ou outro destino que o administrador definir;

2.13.6 – Deverá de forma automática criar exclusão para arquivos restaurados da quarentena;

2.13.7 – Deverá permitir escanear a quarentena após a atualização de assinaturas.

2.14 – Controle de Usuário

2.14.1 – Deverá ter módulo de controle de usuário integrando com as seguintes características:

2.14.1.1 – Bloqueio de acesso a internet;

2.14.1.2 – Bloqueio de acesso a aplicações definidas pelo administrador.

2.15 – Controle do Dispositivo

2.15.1 – Deverá ser possível a instalação do módulo de controle de dispositivos através da console de gerenciamento;

2.15.2 – Através do módulo de controle de dispositivo deverá ser possível controlar:

2.15.2.1 – Bluetooth;

2.15.2.2 – CDROM/DVDROM;

2.15.2.3 – IEEE 1284.4;

2.15.2.4 – IEEE 1394;

2.15.2.5 – Windows Portable;

2.15.2.6 – Adaptadores de Rede;

2.15.2.7 – Adaptadores de rede Wireless;

2.15.2.8 – Discos Externos;

2.15.3 – Deverá escanear em tempo real qualquer informação localizada em mídias de armazenamento como:

2.15.3.1 – CD/DVD;

2.15.3.2 – Discos Externos;

2.15.3.3 – Pen-Drivers;

2.15.4 – Deverá permitir regras de definição de bloqueio/desbloqueio;

2.15.5 – Deverá permitir regras de exclusão.

2.16 – Criptografia

2.16.1 – Deverá oferecer a possibilidade de criptografia de disco através da mesma console de gerenciamento do antivírus, seja em nuvem (cloud) ou local (on-premise);

2.16.2 – Deverá utilizar quando necessário serviços de criptografia com agentes nativos da estação de trabalho seja baseada em Windows ou Mac;

2.16.3 – Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento;

2.16.4 – Deverá ser compatível com Mac OS X Moutain, Mavericks, Yosemite, Sierra.

2.17 – Atualização

2.17.1 – Após a atualização o administrador deverá ter a capacidade de configurar uma reinicialização;

2.17.2 – Possibilidade de utilizar um servidor local para efetuar as atualizações das estações de trabalho;

2.17.3 – Permitir atualizações de assinatura de hora em hora;

2.17.4 – Permitir motor de varredura local, no servidor de rede ou em nuvem afim de aumentar o desempenho da estação de trabalho quando a mesma estiver sendo escaneada.

2.18 – Segurança para dispositivos móveis

2.18.1 – Requisitos mínimos do Sistema Operacional:

2.18.1.1 – Android 2.2 ou superior.

2.18.2 – Recursos:

2.18.2.1 – Permitir atribuir dispositivo com usuário do Active Directory;

2.18.2.2 – A ativação do dispositivo da console de gerenciamento deverá ser através de um QR code;

2.18.2.3 – Os pacotes de instalação devem estar disponíveis nas lojas dos Sistemas Operacionais;

2.18.3 – Deverá permitir no mínimo as seguintes ações:

2.18.3.1 – Impor bloqueio de tela e autenticação;

2.18.3.2 – Desbloquear o dispositivo;

2.18.3.3 – Restaurar as configurações de fábrica;

2.18.3.4 – Localizar o Dispositivo;

2.18.3.5 – Análise de dispositivos para o Sistema Operacional Android;

2.18.3.6 – Criptografia de memória do dispositivo para o Sistema Operacional Android.

2.19 – Configurações de Segurança

2.19.1 – Caso o dispositivo não esteja em conformidade com as políticas estabelecidas deverá ser possível as ações abaixo:

2.19.1.1 – Ignorar;

2.19.1.2 – Bloquear acesso;

2.19.1.3 – Bloquear o dispositivo;

2.19.1.4 – Restaurar as configurações de fábrica;

2.19.1.5 – Remover o dispositivo da console de gerenciamento;

2.19.2 – Deverá permitir o uso de senha. A senha pode ser configurada conforme necessidade do administrador com no mínimo os seguintes recursos:

2.19.2.1 – Senha simples ou complexa;

2.19.2.2 – Números e caracteres;

2.19.2.3 – Comprimento mínimo;

2.19.2.4 – Caracteres especiais mínimos;

2.19.2.5 – Período de expiração da senha;

2.19.2.6 – Definir restrição de reutilização de senha;

2.19.2.7 – Definir o número de tentativas de entradas de senha incorretas;

2.19.2.8 – Período de bloqueio do dispositivo.

2.20 – Segurança de e-mails

2.20.1 – Fornecer proteção de antispam para ambiente com instalação local (on-premise) do MS Exchange;

2.20.2 – Oferecer análise comportamental e proteção para zero-day;

2.20.3 – Oferecer proteção contra vírus e tentativas de phishing.

2.20.4 – Deverá oferecer a possibilidade de criptografia de disco através da console de gerenciamento seja em nuvem ou on-premise com módulo de Criptografia presente na mesma Console do Antivirus.

2.20.5 – Deverá utilizar quando necessários serviços de criptografia através agentes nativos da estação de trabalho baseada em Windows (BitLocker) ou Mac (FileVault);

2.20.6 – Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento;

2.20.7 – Deverá ser compatível com Mac OS X Moutain, Mavericks, Yosemite, Sierra.

2.21 – Na hipótese de não haver vencedor para a cota reservada, esta poderá ser adjudicada ao vencedor da cota principal ou, diante de sua recusa, aos demais fornecedores remanescentes, desde que pratiquem o preço do primeiro colocado da cota principal.

2.22 – Se a mesma empresa vencer a cota reservada e a cota principal, a contratação das cotas deverá ocorrer pelo menor preço.

2.23 – Será dada a prioridade de aquisição aos produtos das cotas reservadas quando forem adjudicados aos compradores qualificados como microempresas ou empresas de pequeno porte, ressalvados os casos em que a cota reservada for inadequada para atender as quantidades ou as condições do pedido, conforme vier a ser decidido pela Administração, nos termos do art. 8º, §4º do Decreto n.º 8.538, de 2015.

CLÁUSULA TERCEIRA – DO PRAZO DE VIGÊNCIA DO CONTRATO

3.1 – O prazo de vigência da contratação é de **2 (dois) anos**, contados a partir da publicação no Diário Oficial da União – DOU, vedada a possibilidade de renovação.

CLÁUSULA QUARTA – DA CLASSIFICAÇÃO DE BENS/SERVIÇOS COMUNS

4.1 – O objeto da contratação enquadra-se na classificação de materiais/serviços comuns, nos termos do art. 1º, § único, da Lei n.º 10.520/2002 e do art. 32, inciso IV, da Lei nº 13.303/2016.

CLÁUSULA QUINTA – DA ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO

5.1 – O prazo de entrega dos bens/serviços é de 10 (dez) dias, contados da publicação no Diário Oficial da União – DOU em sua totalidade e em endereço eletrônico registrado.

5.2 – Os bens/serviços serão recebidos provisoriamente no prazo de 10 (dez) dias, pelo (a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste contrato e na proposta.

5.3 – Os bens/serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste contrato e na proposta, devendo ser substituídos no prazo de 05 (cinco) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

5.4 – Os bens/serviços serão recebidos definitivamente no prazo de 16 (dezesseis) dias, contados do recebimento provisório, após a verificação da qualidade e quantidade do material/serviço e consequente aceitação mediante termo circunstanciado.

5.4.1 – Na hipótese da 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.

5.5 – O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do contrato.

CLÁUSULA SEXTA – DAS OBRIGAÇÕES DA CONTRATANTE

6.1 – São obrigações da Contratante:

6.1.1 – Receber o objeto no prazo e condições estabelecidas no Processo de compra e seus anexos;

6.1.2 – Verificar minuciosamente, no prazo fixado, a conformidade dos bens/serviços recebidos provisoriamente com as especificações constantes do Processo de compra e da proposta, para fins de aceitação e recebimento definitivo;

6.1.3 – Comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto do processo de compra fornecido, para que seja substituído, reparado ou corrigido;

6.1.4 – Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de fiscal do contrato, devidamente designado pela autoridade superior;

6.1.5 – Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Processo de compra e seus anexos;

6.1.6 – Aplicar as penalidades quando cabíveis, nos termos do processo de compra, deste contrato e da lei.

6.2 – A Administração não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

6.3 – Prestar quaisquer esclarecimentos que venham a ser formalmente solicitados pela CONTRATADA, pertinentes ao objeto do presente pacto;

6.4 – Observar para que, durante a vigência do presente contrato, sejam mantidas todas as condições de habilitação e qualificação exigidas no processo de compra, bem como a compatibilidade com as obrigações assumidas, nos termos do art. 69, inciso IX, da Lei 13.303/2016;

6.5 – Aplicar as penalidades, quando cabíveis, conforme determinam os artigos 82 a 84 da Lei nº 13.303/2016 e os artigos 136 a 138 do Manual de Procedimentos e Regulamento de Licitações e Contratos da CEASAMINAS.

CLÁUSULA SÉTIMA - DAS OBRIGAÇÕES DA CONTRATADA

7.1 – A Contratada deve cumprir todas as obrigações constantes no Processo de compra, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

7.1.1 – Efetuar a entrega do objeto do processo de compra em perfeitas condições, conforme especificações, prazo e local constantes neste contrato e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade;

7.1.2 – Responsabilizar-se pelos vícios e danos decorrentes do objeto do processo de compra, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei n.º 8.078, de 1990);

7.1.3 – Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste contrato, o objeto do processo de compra com avarias ou defeitos;

7.1.4 – Comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

7.1.5 – Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas no processo de compra, nos termos do art. 69, inciso IX, da Lei 13.303/2016;

7.1.6 – Indicar preposto para representá-la durante a execução do contrato.

7.1.7 – Comparecer, sempre que solicitada, à sede da Fiscalização da CONTRATANTE, em horário por esta estabelecida, a fim de receber instruções e acertar providências;

7.1.7.1 – No intuito de atender às medidas de distanciamento social impostas pela pandemia do COVID-19, bem como em razão da CONTRATADA estar situada no Estado de São Paulo, este comparecimento poderá ser substituído por reuniões remotas, na forma de videoconferência ou outro meio similar.

7.1.8 – Obedecer obrigatoriamente às normas e especificações Técnicas constantes do Processo de compra, bem como respeitar rigorosamente as recomendações Técnicas da Associação Brasileira de Normas Técnicas (ABNT);

7.1.9 – Realizar todos os testes e ensaios de materiais, em obediência às normas da ABNT e outros que forem julgados necessários pela Fiscalização;

7.1.10 – Substituir, dentro do prazo estipulado pela Fiscalização, os eventuais defeitos ou incorreções constatados pela Fiscalização;

7.1.11 – Responsabilizar-se por eventuais danos que vier a causar à CONTRATANTE ou a terceiros, decorrentes de sua culpa ou dolo na execução do contrato;

7.1.12 – Cumprir rigorosamente os prazos estabelecidos;

7.1.13 – Fornecer os materiais/serviços em até 10 (dez) dias após a emissão da Autorização de Fornecimento (AF) ou Ordem de Serviço;

7.1.14 – Assumir os valores existentes na proposta comercial e assumir total responsabilidade para eventuais erros e omissões que nela venha ser encontrada;

7.1.15 – Emissão da nota fiscal de faturamento, bem como assumir encargos e impostos.

7.1.16 – Seguir integralmente normas, procedimentos e regulamentações internas da CONTRATANTE, além das legislações pertinentes, inclusive, trabalhista.

7.1.17 – Todas as comunicações entre a Contratada e a CEASAMINAS devem ser feitas por escrito;

7.1.18 – A responsabilidade da Contratada é integral para o objeto do presente contrato, nos termos do Código Civil Brasileiro.

7.1.19 – Todos os materiais a serem empregados serão obrigatoriamente de primeira qualidade e deverão obedecer às especificações e normas da ABNT. Em nenhum caso o uso de material menos nobre poderá servir de justificativa, devendo a boa técnica fornecimento os materiais de qualidade por conta da Contratada.

7.1.20 – É vedado à CONTRATADA caucionar ou utilizar o contrato objeto da presente licitação, para qualquer operação financeira.

7.1.21 – A Contratada será obrigada a atender todas as solicitações efetuadas durante a vigência do contrato, mesmo que o fornecimento deles decorrente estiver previsto para data posterior a do seu vencimento. O pedido poderá ser feito por memorando, ofício, telex, fac-símile ou e-mail, devendo dela constar: a data, a quantidade pretendida, o local para a entrega e o nome do responsável.

7.1.22 – Os materiais/serviços deverão ser fornecidos acompanhados da Nota Fiscal/Nota Fiscal Fatura.

CLÁUSULA OITAVA – DA SUBCONTRATAÇÃO

8.1 – Não será admitida a subcontratação do objeto licitatório.

CLÁUSULA NONA – DA ALTERAÇÃO SUBJETIVA

9.1 – É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos no processo de compra original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

CLÁUSULA DÉCIMA – DO CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

10.1 – Nos termos do artigo 84, inciso II, do Manual de Procedimentos e Regulamento de Licitações e Contratos da CEASAMINAS, será designado como fiscal administrativo do Contrato e fiscal técnico, o (a) Gestor (a) do Departamento de Tecnologia da Informação; esse último para aceitar tecnicamente os materiais, anotando em registro próprio todas as ocorrências relacionadas com a execução do Contrato, reportando todas as necessidades de regularização de falhas ou defeitos observados.

10.1.1 – O Fiscal do Contrato será nomeado através de Portaria de emissão do Diretor-Presidente.

10.2 – A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, em conformidade com o art. 76, da Lei n.º 13.303/2016.

10.3 – O representante da Administração anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

CLÁUSULA DÉCIMA PRIMEIRA – DOS PREÇOS E DO PAGAMENTO

11.1 – Serão adquiridos mediante o presente contrato os seguintes itens e quantitativos constantes abaixo, derivados da Proposta Orçamentária encaminhada pela Contratada, constante no Procedimento Interno nº 27/2021:

Item	Unidade	Descrição	Quantidade	Preços (R$)	
				Unitário	Total
1	Un	Aquisição de Licenças e Atualização do Antivírus + Suporte Técnico à Ferramenta.	250	39,60	**9.900,00**
VALOR TOTAL					**9.900,00**

Obs.: 1 - Valores monetários expressos na moeda Real.
2 – No valor acima estão incluídas todas as despesas com frete.

11.2 – O pagamento será realizado em parcela única e em 30 (trinta) dias após recebimento dos materiais/serviços e da devida Nota Fiscal, mas fica condicionado ao recebimento técnico dos materiais/serviços e será realizado em até 10 (dez) dias após o recebimento e aceite da Nota Fiscal/Fatura eletrônica pelo e-mail: nfe@ceasaminas.com.br, a qual será conferida e atestada pelo Fiscal Administrativo, após aceitação do Fiscal Técnico ou com apoio técnico de seu assessor caso entenda necessário.

11.3 – Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o órgão contratante atestar a execução do objeto do contrato.

11.4 – A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 56, do Manual de Procedimentos e Regulamento de Licitações e Contratos da CEASAMINAS.

11.4.1 – As notas fiscais deverão ser entregues até o dia 25 de cada mês em relação a cada pedido realizado.

11.4.2 – Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no do art. 31, da Instrução Normativa n.º 3, de 26 de abril de 2018.

11.5 – Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

11.6 – Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no processo de compra.

11.7 – Constatando-se junto ao SICAF a situação de irregularidade da Contratada, será providenciada sua notificação, por escrito, para que, no prazo de 05 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da Contratante.

11.8 – Previamente à cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa n.º 3, de 26 de abril de 2018.

11.9 – Não havendo regularização ou sendo a defesa considerada improcedente, a Contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da Contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

11.10 – Persistindo a irregularidade, a CEASAMINAS deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à Contratada a ampla defesa.

11.11 – Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a Contratada não regularize sua situação junto ao SICAF.

11.12 – Será rescindido o contrato em execução com a Contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da CEASAMINAS.

11.13 – Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

11.13.1 – A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar n.º 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

11.14 – Nenhum pagamento será efetuado à Contratada enquanto pendente de liquidação qualquer obrigação financeira, sem que isso gere direito à alteração dos preços, ou de compensação financeira por atraso de pagamento.

11.15 – Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido de alguma forma para tanto, fica convencionado que a taxa de compensação financeira devida pela CEASAMINAS, entre a data acima referida e a correspondente ao efetivo adimplemento da parcela será correspondente à multa de 2% (dois por cento) e juros legais de 1% (um por cento) ao mês.

11.16 – No caso de inadimplemento por parte da Contratada, o fiscal administrativo deve solicitar à diretoria da CEASAMINAS abertura de Processo Administrativo para Apuração de Responsabilidade (PAAR), nos termos do artigo 139 do Manual de Procedimentos e Regulamento de Licitações e Contratos da CEASAMINAS.

11.17 – O valor total deste Contrato é de **R$ 9.900,00** (nove mil e novecentos reais).

CLÁUSULA DÉCIMA SEGUNDA – DOS RECURSOS ORÇAMENTÁRIOS

12.1 – As despesas decorrentes desta licitação, para o período de 2 (dois) anos, correrão à conta da dotação orçamentária n.º 2.205.050.300.

CLÁUSULA DÉCIMA TERCEIRA – DO REAJUSTE

13.1 – Os preços são fixos e irreajustáveis no prazo de vigência deste contrato.

CLÁUSULA DÉCIMA QUARTA – DA GARANTIA DE EXECUÇÃO

14.1 – Não haverá exigência de garantia contratual da execução.

CLÁUSULA DÉCIMA QUINTA – DAS SANÇÕES ADMINISTRATIVAS

15.1 – Nos artigos 136 e seguintes do Manual de Procedimentos e Regulamento de Licitações e Contratos da CEASAMINAS e nos artigos 82 e seguintes da Lei 13.303/2016 encontram-se a tipificação de todas as condutas lesivas praticadas pelo licitante/contratado, bem como as devidas sanções administrativas.

15.2 – A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada.

15.3 – As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor da CEASAMINAS, ou deduzidos da garantia, quando for o caso, e cobrados judicialmente.

15.4 – A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

15.5 – Se, durante o processo de aplicação de penalidade, houver indícios de prática de infração administrativa tipificada pela Lei n.º 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização - PAR.

15.6 – A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei n.º 12.846, de 1º de agosto de 2013, seguirão seu rito normal na CEASAMINAS.

15.7 – O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

CLÁUSULA DÉCIMA SEXTA – DA PUBLICAÇÃO

16.1 – A publicação do Contrato, sob a forma de extrato, será promovida pela CEASAMINAS.

CLÁUSULA DÉCIMA SÉTIMA – DO FORO

17.1 – Fica eleito o foro de Contagem/MG, como o único competente para a solução das dúvidas oriundas da interpretação das cláusulas deste Contrato.

17.2 – E por estarem assim ajustadas, as partes com as testemunhas assinam o presente instrumento de Contrato em 03 (três) vias de igual teor e forma, para todos os fins de direito.

Contagem/MG, terça-feira, 09 de julho de 2021.

CEASAMINAS
Diretor Presidente
Luciano José de Oliveira

CEASAMINAS
Diretor de Administração
Juliano Maquiaveli Cardoso

TEC HOUSE INFORMÁTICA LTDA.

Testemunha: Thiago Resende Machado Andrade
CPF ****.022.986.18

Testemunha: Leonardo Cabral Ferreira
CPF ***.007.376-**

Fiscal do Contrato/CeasaMinas