INSTITUTO DE GEO-CIENCIAS/UFMG

Termo de Referência 4/2026

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
4/2026	153293-INSTITUTO DE GEO-CIENCIAS/UFMG	GABRIEL AMARAL DE PINHO	24/06/2026 11:27 (v 0.5)

Status

ASSINADO

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Serviços de TIC		23072.225993/2026-20

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de empresa para Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software - ESET PROTECT (Licença de software Antivírus) - para proteção e segurança dos computadores do Instituto de Geociências/UFMG, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

Item	Especificação	CATSER	Métrica ou Unidade de Medida	CÓD. PMC-TIC	Quantidade	Valor Unitário	Valor Total
1	Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software - ESET PROTECT - Renovação da Licença por 60 meses.	27502	UN.		100	R$299,60	R$29.960,00

Classificação do objeto quanto à heterogeneidade ou complexidade

1.2. O(s) serviço(s) objeto desta contratação são caracterizados como **comum(ns),** conforme justificativa constante do Estudo Técnico Preliminar.

Classificação do objeto quanto ao modelo de execução

1.3. O serviço é enquadrado como continuado tendo em vista a contratação para o período de cinco anos, sendo a vigência plurianual mais vantajosa considerando os apontamentos do Estudo Técnico Preliminar.

Prazo de vigência

1.4. O prazo de vigência da contratação é de **5 (cinco) anos** contados a partir do dia 01/07/2026, na forma do artigo 105 da Lei n° 14.133, de 2021.

1.5. O contrato ou outro instrumento hábil que o substitua oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A presente contratação objetiva-se assegurar a continuidade e atualização da infraestrutura de segurança da informação da unidade, garantindo proteção contra ameaças cibernéticas, gestão centralizada de dispositivos, criptografia de dados e conformidade com normas técnicas aplicáveis, como a ISO 27001.

No momento, faz-se necessária a aquisição de 100 licenças, destinadas tanto às máquinas dos setores administrativos (incluindo a Casa da Glória, em Diamantina) quanto aos laboratórios utilizados pelos discentes.

A renovação do Software Eset Protect Entry, justifica-se pela necessidade contínua de manutenção da segurança cibernética, bem como pelo fato de o referido software já ter sido contratado em períodos anteriores, encontrando-se instalado e em uso para proteção dos equipamentos do Instituto de Geociências/UFMG.

2.2. O objeto da contratação está previsto no Plano de Contratações Anual 2026, conforme detalhamento a seguir:

I) ID PCA no PNCP: 17217985000104-0-000027/2026;

II) Data de publicação no PNCP: 14/05/2025;

III) Id do item no PCA: 186;

IV) Classe/Grupo: 182 - SERVIÇOS DE LICENCIAMENTO E CONTRATOS DE TRANSFERÊNCIA DE TECNOLOGIA;

V) Identificador da Futura Contratação: 153293-48/2026;

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO

3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

3.2. A solução de TIC consiste em:

Possuir suporte nativo às arquiteturas 64-bits (x64) e ARM64, sendo o suporte a 32-bits desejável apenas para ambientes legados estritamente justificados; Deve possuir capacidade de instalação e pleno funcionamento dos módulos solicitados em estações de trabalho com no mínimo 4GB de memória RAM; Deve suportar as seguintes plataformas Microsoft (clientes/desktops):Windows 10 (versões com suporte ativo/LTSC), Windows 11 e superiores. Deve suportar as seguintes plataformas Microsoft (servidores): Windows Server 2022 e superiores; Windows Server 2019 e superiores; Desejável suporte ao Windows Server 2016 para ambientes legados justificados; Deve inclusive suportar a instalação e operação em modo Server Core; Deve suportar, pelo menos a função de proteção de endpoint (EPP/EDR), nas seguintes distribuições Linux com kernel moderno (Série 5.x ou superior): Red Hat Enterprise Linux 8 e superiores, arquitetura 64-bits; SUSE Linux Enterprise Server/Desktop 15 e superiores, arquitetura 64-bits; Ubuntu Server/Desktop 20.04 LTS, 22.04 LTS, 24.04 LTS e superiores, arquitetura 64-bits; Debian 11 e superiores, arquitetura 64-bits; Deve suportar a instalação de agente e endpoint nos sistemas operacionais acima virtualizados nas seguintes plataformas de nuvem e hiper visores: AWS (Amazon Web Services); Microsoft Azure; GCP (Google Cloud Platform); Citrix Virtual Apps (XenApp); Citrix Virtual Desktops (XenDesktop); Citrix Hyper visor (XenServer); Microsoft Hyper-V 2019 e superiores; VMware ESXi (Versões 7.0, 8.0 e superiores); VMware Player; VMware vSphere; VMware Workstation; OpenStack. Toda a proteção deverá ser realizada através de um único agente de proteção (Single Agent) com as funcionalidades descritas neste termo, não sendo aceitos plugins ou softwares adicionais na estação para a composição do pacote de segurança; O agente único deve compreender, no mínimo, as seguintes funcionalidades: Módulo antimalware de próxima geração (EPP); Módulo de proteção contra ameaças avançadas (EDR/XDR); Desejável módulo de proteção de dados (DLP Endpoint); Desejável módulo para

resposta a incidentes (isolamento de rede e remediação); Desejável módulo de inteligência integrada contra ameaças (Threat Intelligence); Módulo para controle de dispositivos removíveis (Device Control); Todas as funcionalidades deverão ser geridas por uma console única com as capacidades mínimas de: Relatórios dinâmicos; Dashboards interativos; Gestão de Políticas; Configuração global;. Instalação e Desinstalação remota; Integração com produtos de terceiros via API (ex.: SIEM/SOAR); O cliente (agente) deve ser capaz de operar em modo autônomo (self-managed), aplicando políticas de contingência em caso de perda de comunicação com o servidor; O cliente deve ser capaz de atualizar a telemetria para detecção de ameaças, seus patches e hot fixes a partir de um servidor definido pelo administrador ou diretamente na nuvem do fabricante; A solução de prevenção deve ser colaborativa, ou seja, os módulos exigidos devem ser capazes de trocarem informações para uma análise contextual mais inteligente (XDR); A solução deve possuir múltiplas camadas de proteção (Machine Learning, Análise Comportamental, Inteligência Artificial e Heurística Avançada), não sendo aceitas soluções baseadas apenas em assinaturas estáticas; A solução deve conter módulo capaz de proteger contra botnets, ataques de negação de serviço (DoS/DDoS), executáveis não confiáveis econexões web maliciosas (Firewall local/NIDS); A solução deve conter módulo web integrado capaz de garantir uma navegação segura, prevenindo contra sites de phishing, downloads de malwares e garantindo a aplicação de políticas de acesso (Permitir/Negar); A plataforma deverá permitir automação de tarefas como: agendar varreduras (scans), envio de relatórios, atualizações, atribuição dinâmica de política por grupo e iniciar uma ativação de um agente; É desejável que a solução de segurança para desktops e servidores possa se conectar a módulos de correlação e investigação reversa de incidentesna nuvem (Threat Hunting/Data Lake do fabricante).

O módulo HIPS deve permitir controle granular e monitoramento sobre as seguintes ações: Acesso remoto a pastas locais e compartilhamentos de rede; Alteração de políticas de direitos das contas de usuários (UAC/IAM); Alteração dos registros de extensão dos arquivos e associações de software; Criação de novos arquivos em diretórios nativos do sistema, como Arquivos de Programas e App Data; Criação de novos executáveis ou injeção de binários na pasta Windows (ex.: System32); Criar ou modificar remotamente arquivos do tipo Portable Executable (PE), scripts, variáveis de ambiente e localizações do sistema; Criar ou modificar remotamente arquivos ou pastas sensíveis; Tentativas de desativação ou by pass do editor de registro, gerenciador de tarefas e PowerShell; Execução de arquivos a partir das pastas do usuário (ex.: Downloads, Temp); Execução de scripts pelo Windows Script Host, PowerShell, Python ou interpretadores similares; Instalar objetos auxiliares à navegação (BHOs), plugins ou extensões de shell; Instalar e registrar novos CLSIDs, APPIDs e TYPE LIBs (objetos COM/DCOM); Modificar configurações de rede de forma furtiva (ex.: DNS hijacking, rotas, proxy); Modificar configurações de segurança dos navegadores web modernos (Edge, Chrome, Firefox); Modificar processos principais do Windows, contemplando as seguintes ações: Navegadores iniciando processos e programas não autorizados a partir da pasta de downloads; Registrar programas para execução automática (chaves de Autostart / Run); As regras especificadas na política do HIPS devem permitir o: Bloqueio da ação, ou; Geração de Evento de Informação (Auditoria/Log), ou; Bloqueio e Geração de Evento de Informação simultaneamente; A solução deve permitir ao administrador criar regras customizadas contendo, no mínimo, os seguintes parâmetros: Processos: Nome do processo; Hash do arquivo (SHA-256 ou MD5);. Assinatura Digital/Certificado; Usuário (integrado à base de identidades, ex.: AD); Ações em Arquivos: Criação; Exclusão;. Execução; Alteração de permissão; Leitura; Renomeação; Escrita; Chave de Registro: Escrita; Criação; Exclusão; Leitura; Enumeração; Carregamento; Substituição; Restauração; Alterar permissão; Valor de Registro: Leitura; Criação; Exclusão; Ações de Processo: Qualquer acesso; Criação de thread (injeção remota); Modificação do payload; Finalização (Tampering); Execução;. A plataforma deve permitir a configuração de exclusões granulares de regras do HIPS.

A varredura residente deve ser passível de habilitação ou desativação por opção do administrador via console; Deve iniciar a proteção na camada de driver durante a inicialização do sistema operacional (tecnologia ELAM - Early Launch Anti-Malware); Deve ser capaz de realizar análise no setor de boot (incluindo UEFI e Secure Boot); O administrador da solução deve poder especificar o tempo máximo de análise (timeout) para um único arquivo, evitando travamentos; Deve analisar os processos em memória durante a inicialização do serviço e após a atualização da base de telemetria; Deve possibilitar ao administrador a criação de bypass temporário ou análise otimizada para instaladores corporativos assinados e confiáveis; Deve realizar inspeção ativa durante a cópia de arquivos entre pastas locais, unidades de rede e nuvem mapeada; A solução deve possuir conexão ativa em tempo real com a Nuvem de Inteligência de Ameaças (Threat Intelligence) do fabricante, passível de ativação ou desativação por parte do administrador; Deve permitir a configuração do nível de agressividade da análise heurística entre: Muito Baixo; Baixo; Médio; Alto; Muito Alto; Deve possibilitar aplicar as configurações de varredura a todos os processos do sistema operacional ou restringir a uma lista de grupos específica criada pelo administrador; Deve realizar varredura de inspeção quando o processo realizar as seguintes ações de I/O: Ler o disco; Gravar no disco; Deixar a solução decidir de forma automática baseada em inteligência; Deve possibilitar análise nativa nos seguintes locais e formatos:

Unidades de Rede mapeadas (SMB/NFS); Arquivos abertos para backup (suportando limites de performance para não impactar a rotina); Arquivos compactados com algoritmos modernos, por exemplo .jar, .zip e outros; Arquivos codificados e scripts embutidos (MIME, Base64); Deve detectar Aplicações Potencialmente Indesejadas (PUA/PUPs), ameaças de dia zero (Zero-Day) em programas desconhecidos e ameaças embutidas em macros desconhecidas; Deve permitir selecionar, no mínimo, uma das seguintes opções de ação automática após detectar uma ameaça confirmada (malware): Limpar o arquivo; Excluir o arquivo; Isolar ou Negar acesso ao arquivo; Deve permitir selecionar, no mínimo, uma das seguintes opções de ação automática após detectar um programa indesejado (PUA): Limpar o arquivo; Excluir o arquivo; Permitir acesso ao arquivo (via aprovação); Negar acesso ao arquivo; Deve possibilitar ao administrador a gestão centralizada de uma lista de exclusões confiáveis (por caminho, hash ou certificado); Deve possuir integração com recursos do sistema (ex.: AMSI) capazes de interceptar e analisar scripts ofuscados na memória (Javascript, VBScript, PowerShell) indicando se o comportamento é malicioso ou não; Deve permitir a criação de listas de exclusão de URLs confiáveis que não sofrerão interceptação rígida e análise de scripts; Ao detectar uma ameaça, o agente deverá emitir uma notificação nativa no sistema operacional ao usuário com uma mensagem customizável pelo administrador da solução.

Deve ser possível realizar varreduras agendadas com periodicidade diária, semanal ou customizada; Deve permitir a criação de repetição da tarefa na console; Deve permitir definir a hora exata da execução da tarefa de análise; Deve permitir a criação da tarefa de varredura com janela aleatória (randômica) para evitar sobrecarga de I/O em ambientes de virtualização simultâneos; Deve permitir a realização de varreduras agendadas apenas após o logon do usuário ou durante a inicialização do sistema operacional; Deve permitir ao administrador escolher (um ou mais) alvos granulares da varredura, dentre eles: Os locais da varredura contemplando: Memória RAM (para detecção de rootkits e malwares fileless); Processos em execução; Arquivos e chaves do Registro do sistema; "Meu Computador" ou "Este Computador"; Todas as unidades locais do disco; Todas as unidades de armazenamento fixas; Todas as unidades de armazenamento removíveis; Todas as unidades mapeadas na rede; Pasta inicial/Boot; Pastas de perfil do usuário (ex.: AppData, Downloads); Pasta base do Windows; Pasta de Arquivos de Programas; Pasta de arquivos temporários do sistema; Lixeira do sistema operacional; Qualquer arquivo ou pasta específica delimitada pelo administrador; Setor de inicialização física/lógica (boot/UEFI); Arquivos compactados em sua totalidade; Arquivos estruturados em MIME; Os tipos de arquivos específicos que serão analisados por extensão ou cabeçalho; Opções adicionais de detecção durante o scan, como detecção de programas indesejados (PUA), ameaças de dia zero e macros maliciosas; Áreas de exclusão específicas que não deverão ser varridas sob hipótese alguma para garantir compatibilidade com sistemas internos críticos; Deve permitir a integração direta com o Centro de Inteligência na Nuvem do fabricante durante a varredura agendada para validação de falsos positivos; Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça confirmada na varredura sob demanda: Limpar o arquivo infectado; Excluir o arquivo malicioso; Negar acesso/Isolar o arquivo em quarentena; Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado (PUA): Limpar o arquivo; Excluir o arquivo; Permitir acesso mediante aprovação de política; Negar acesso ao arquivo; Para minimizar o impacto sistêmico e no trabalho do usuário final, a solução deve permitir tecnologias de otimização contendo: Utilização de cache inteligente (Smart Cache), ou seja, arquivos já analisados que não tiveram seu conteúdo e hash alterados não serão reprocessados; Capacidade de iniciar a varredura apenas e tão somente quando o sistema operacional estiver em estado de ociosidade (idle); Permitir ao usuário ou administrador pausar e retomar varreduras manualmente; Deve permitir ao administrador inserir uma conta de serviço de domínio via console para realizar a análise em dispositivos de armazenamento de rede (NAS/Storages) de forma autenticada.

A solução deve possuir tecnologia de isolamento ou confinamento dinâmico (Sandboxing local ou em nuvem) de aplicativos e arquivos executáveis com comportamentos suspeitos, como tentativas de criptografia (ransomware); A solução deve ser capaz de avaliar aplicações desconhecidas e potencialmente maliciosas executando-as em ambiente micro-virtualizado ou emulado controlado antes de permitir a execução real no sistema; Deve permitir a indicação de aplicações confiáveis em lista de permissões para que sistemas internos não caiam no filtro de confinamento dinâmico(falsos positivos); A proteção anti-ransomware de análise comportamental não deve requerer obrigatoriamente conexão com a internet ou centro de inteligência para que a contenção da ameaça seja ativada; A solução deve manter um cache de reputação local com informações de aplicações dinamicamente categorizadas (conhecidas, desconhecidas e maliciosas); Dentre os Comportamentos Indicadores de Ataque (IoAs) monitorados e passíveis de prevenção, a solução deve ser capaz de: Bloquear acesso local a partir de cookies maliciosos; Bloquear a criação massiva de arquivos a partir de extensões de risco automatizado como .bat, .exe, .html, .hpg, .jpg, .bmp, .job e scripts .vbs / .ps1; Bloquear a criação não autorizada de arquivos executáveis em qualquer local mapeado na rede; Bloquear a criação ou manipulação de CLSIDs, APPIDs e TYPELIBs usados em ataques fileless; Bloquear injeções e criação de threads remotas em outros processos legítimos do sistema (ex.: Process Hollowing); Bloquear a

tentativa de desativação de executáveis ou serviços críticos do sistema operacional ou da própria solução antivírus (Tamper Protection); Bloquear a leitura, exclusão ou gravação atípica em lote de arquivos estruturados frequentemente visados por ransomwares (documentos, planilhas, bancos de dados); Bloquear a gravação clandestina ou extração de leitura na memória de processos críticos alheios (ex.: proteção ao LSASS para evitar roubo de credenciais); Bloqueio de modificação indevida das políticas do Firewall nativo do Windows; Bloqueio de modificação anômala ou adição de malwares na pasta de tarefas agendadas do Windows; Bloqueio de modificação de arquivos vitais de inicialização do Windows e locais críticos do Registro do sistema; Bloqueio de modificação parasitária em arquivos executáveis portáteis (PE) já compilados; Bloqueio de manipulação do bit de atributo oculto (hidden) em diretórios de sistema; Bloqueio de manipulação forçada do bit de atributo somente leitura em arquivos de proteção; Bloqueio de modificação de entradas de registro sensíveis como DLL AppInit; Bloqueio de modificação de chaves e locais do Registro responsáveis pela inicialização do SO; Bloqueio de modificação em lote ou exclusão de pastas de dados nativas de usuários; Bloqueio de modificação ou sequestro do local do Registro de Serviços do sistema; Bloqueio de suspensão indevida ou travamento de processos cruciais; Bloqueio de término ou finalização violenta de processos críticos do sistema; A partir dos comportamentos maliciosos observados, deve ser possível à solução aplicar ação de bloqueio automático da ameaça ou gerar apenas evento de informação (modo de auditoria), conforme política configurada; Deve ser capaz de informar ao usuário final, caso configurado, os comportamentos de risco e ameaças bloqueadas através de notificação pop-up com mensagem customizada; Deve possuir o modo de ativação de bloqueio proativo para o confinamento de quaisquer arquivos desconhecidos (Zero-Day) acessados pelo sistema operacional e não possuidores de reputação global; O administrador deve poder atribuir perfis de regras baseados no equilíbrio estratégico da política, visando aplicar maior rigidez de segurança ou maior flexibilidade para a produtividade do usuário final; Toda a proteção de detecção avançada (EDR) deve estar nativamente embutida no mesmo agente de proteção (Single Agent), não requerendo download secundário, sensor separado ou aplicação adicional na estação de trabalho para a execução e ativação do monitoramento; Deve possuir capacidade de inspecionar arquivos suspeitos, correlacionar eventos e detectar anomalias comportamentais utilizando técnicas nativas de Inteligência Artificial e "Machine-Learning" sem depender primariamente de vacinas/assinaturas legadas.

Deve controlar ativamente o modo como os usuários copiam ou acessam dados em drives USB, cartões de memória, mídias óticas e magnéticas, dispositivos Bluetooth e IrDA, dispositivos de leitura de imagem (MTP), smartphones, portas legadas (COM/LPT) ou interfaces modernas (Thunderbolt/USB-C); Deve permitir que o administrador especifique granuralmente quais dispositivos podem ou não ser usados utilizando parâmetros de hardware, incluindo: códigos do produto (PID), códigos de fornecedor (VID), números de série exclusivos do pendrive/disco, classes de dispositivos ou identificadores de nome; O módulo deve ser capaz de coletar dados contextuais de incidentes tais como identificação do dispositivo, data/hora da inserção, usuário logado e evidências das ações de leitura/gravação, exportando as métricas para reação, investigação e auditoria na console central; Deve permitir a aplicação de regras de reação específicas para unidades de mídia removível (ex.: pendrive) com opções mandatórias de: bloqueio total de acesso, acesso em modo somente leitura (read-only) ou acesso total com monitoramento e gravação de logs (auditoria); Deve ser capaz de monitorar automaticamente o uso das interfaces listadas e aplicar o bloqueio de todas as tentativas de uso e evasão de política em tempo real; Deve possuir integração nativa com a ferramenta de gerenciamento centralizado para o envio e coleta de logs essenciais para o cumprimento de normativas de privacidade (ex.: LGPD), contendo device, times tamp e metadados da transação; Deve suportar integração direta com a estrutura de identidades corporativas (Active Directory / Entra ID) para a criação e amarração de regras de acesso a dispositivos baseadas em usuários, grupos de domínio ou Unidades Organizacionais (OUs); Deve bloquear de forma nativa a tentativa do usuário de desabilitar o serviço, modificar os processos ou desinstalar o agente de proteção da estação de trabalho (Tamper Protection), permitindo a remoção apenas mediante inserção de senha de desinstalação configurada e fornecida pelo administrador central.

A ferramenta de console de gerenciamento local (se instalada On-Premise) deve suportar a instalação em ambientes virtualizados contendo os seguintes sistemas operacionais base: Windows Server 2025 e Windows Server 2022; Windows Server 2019; Desejável suporte de estabilidade ao Windows Server 2016 caso exigido por restrições de arquitetura de legado interno;(Itens antigos referentes a Windows 2008 R2 e 2012 foram descontinuados no escopo de instalação segura de consoles de segurança, devendo a numeração ser atendida pelo fornecimento das instâncias atualizadas); É desejável e plenamente aceito o fornecimento opcional de um Virtual Appliance (Appliance virtual no formato OVA/OVF) por parte da contratada, contendo uma distribuição Linux embarcada e segura para implantação rápida (Plug-and-Play) da console em hypervisors compatíveis com os requisitos deste ETP; A arquitetura exigida para a instalação da console de gerenciamento ou servidor de aplicação deve ser exclusivamente de 64-bits; O módulo de banco de dados e gerenciamento deve suportar ser implantado de forma redundante em cluster Microsoft (High Availability); Toda a camada de comunicação do gerenciamento deve possuir suporte nativo e pleno aos

protocolos de rede IPv4 e IPv6 (Dual-Stack); Deve suportar implantação e operação 100% suportada em sistemas operacionais devidamente virtualizados ou hospedados na nuvem (IaaS); Para o armazenamento da inteligência e telemetria, deve possuir suporte a bases de dados estruturadas: Microsoft SQL Server 2019 ou edições superiores; Desejável suporte a instâncias modernas de MySQL (versões 8.0 ou superiores, 64 bits); Desejável suporte a PostgreSQL e MariaDB modernos em arquitetura 64 bits para maior flexibilidade arquitetural; Toda a interface de administração da console de gerência deve possuir acesso exclusivamente via WEB, unificando a experiência no modelo "Single Pane of Glass"; A interface web gerencial deve ser nativamente compatível com os seguintes navegadores corporativos padrão: Google Chrome e navegadores baseados no motor Chromium; Mozilla Firefox; Apple Safari nas suas edições com suporte ativo; Microsoft Edge; Em implantações On-Premise de larga escala, deve ser possível segregar a arquitetura de instalação dos componentes da solução de gerência em servidores distintos: Servidor responsável pela interface da Console Web; Servidor de hospedagem da Base de Dados; Servidor de comunicação, telemetria e gerenciamento de endpoints (Proxy/Relay de interação); Agentes na rede configurados como distribuidores de atualizações locais de vacina/cache para economia de link de internet; O banco de dados da aplicação deve suportar o uso nativo de instâncias SQL Server rodando sob volumes lógicos em Storage Area Networks(SAN); Deve permitir a configuração e a geração automatizada dos instaladores (agentes) para todos os módulos da solução a partir de um único console; Deve permitir a propagação e a alteração instantânea das configurações dos módulos nos clientes (endpoints) de maneira remota, silenciosa e sem exigir reinicialização massiva; Deve possuir a capacidade de integração do gerenciamento de estações de trabalho e de servidores deste mesmo fabricante, a fim de prover uma única e universal console de gerenciamento centralizado de todas as soluções de segurança de endpoint (single agent/single console); O sistema de distribuição deve permitir a atualização de forma estritamente incremental das bases de inteligência e vacinas nos clientes finais, a partir de um único servidor ou proxy local, reduzindo drasticamente o consumo de banda WAN corporativa; A console deve extrair e permitir a visualização em formato de inventário básico das características de hardware (CPU, RAM, Disco) e software dos endpoints gerenciados; Deve permitir integração, leitura e sincronização bidirecional automática com a árvore hierárquica e grupos de segurança de domínios Microsoft Active Directory (AD) ou Microsoft Entra ID existentes na rede local; Deve permitir a criação centralizada de tarefas em lote (Deployment Tasks) para atualização de versão de motor de agentes, varreduras programadas e upgrades de inteligência programados para execução imediata, periódica, ou ativada no momento da inicialização / logon da estação na rede; Deve reter e permitir a auditoria das informações coletadas dos endpoints armazenando logs, eventos e políticas de bloqueio de maneira durável no banco de dados centralizado; Deve garantir governança administrativa suportando controle de acesso baseado em funções (RBAC), permitindo a criação de diferentes níveis de administração da console, com perfis customizáveis de maneira independente ou associados ao login da rede do administrador (SSO);. O sistema de gestão de privilégios deve contemplar múltiplos administradores com acesso restrito focado a grupos operacionais distintos (ex.: administrador com visão de filiais, operador somente leitura) a fim de respeitar as permissões de acesso aos produtos gerenciados;. Deve permitir a construção e gestão de agrupamentos dinâmicos de endpoints com base em regras estáticas como faixas e blocos de número IP/Sub-redes associadas ao cliente; Deve permitir a classificação avançada na rede através da criação de grupos virtuais baseados em "Marcadores" dinâmicos (Tags); O sistema de regras lógicas deve permitir que a console posicione o endpoint automaticamente dentro de grupos hierárquicos ao ler os seguintes critérios dinâmicos da máquina: tipo de sistema operacional, módulos instalados, tempo da última conexão, risco e vulnerabilidade detectada, dentre outros; A comunicação arquitetural deve forçar proativamente (modo de enforcement) que as políticas e senhas parametrizadas no servidor cheguem e sejam acatadas imperativamente pelos endpoints conectados; Como mecanismo de resiliência, caso um usuário local altere a configuração por vias excepcionais, a mesma deverá ser sobrescrita automaticamente, retornando ao padrão estabelecido na política oficial do servidor de gerência assim que o agente se comunicar; Para a garantia do sigilo, a comunicação de dados, de comandos executivos e as atualizações de inteligência trocadas entre os agentes na ponta e o servidor de gerenciamento deve transitar de forma segura e criptografada (ponta-a-ponta) utilizando protocolos TLS modernos via HTTPS (mínimo exigido TLS 1.2); Deve fornecer suporte a tarefas mandatórias para forçar a remediação e a instalação faltante dos módulos requeridos nos clientes não conformes; O serviço no agente deve ser autorreparável. Caso ocorra uma desinstalação acidental ou maliciosa, o processo guardião ou as tarefas da gerência devem prover o reparo automático e reinstalação imediata; O instalador gerado pela plataforma de gerenciamento deverá possuir tecnologia embarcada capaz de forçar de forma desassistida (silenciosa) a desinstalação e a remoção de chaves de registro residuais de produtos de antivírus concorrentes, EDRs, agentes desatualizados ou soluções legadas que já operem nas estações para evitar conflitos de software na implantação; A central administrativa do módulo de gestão deverá consolidar, relatar e orquestrar nativamente, no mínimo, as seguintes soluções do escopo: O módulo gerencial da solução voltada para proteção antimalware e heurística em estações de trabalho e sistemas de servidores (EPP); O módulo gerencial da funcionalidade avançada responsável pela correlação e resposta a incidentes

sofisticados, como análise forense comportamental e detecção contínua na estação (EDR/XDR); O módulo de regras estritas exigidas para proteção nativa do workload de servidores críticos de rede; A plataforma deve dispor de um motor de relatórios em formato gráfico, possibilitando a criação de templates, consultas customizáveis e personalização visual detalhada na geração de reportes estatísticos e executivos; Os relatórios analíticos extraídos a partir da plataforma deverão possuir funcionalidade para exportação ou agendamento de envio automático via e-mail utilizando obrigatoriamente os padrões de arquivo do mercado, incluindo: HTML, CSV, PDF e XML; O motor de governança e compliance do gerenciador deverá fornecer consultas e relatórios imediatos contendo um detalhamento minucioso do status do ambiente, informando: O levantamento estatístico integral evidenciando os endpoints (máquinas) cuja lista de definições locais da vacina/agente encontre-se em estado de atraso ou defasagem perante o servidor central; O catálogo detalhado com controle de conformidade, extraindo a build de versão de software ou agente, incluindo as telemetrias com apoio na nuvem do fabricante ativas naquele exato momento em cada endpoint pesquisado; A catalogação gráfica e de volumetria informando, por assinatura ou categoria (MITRE ATT&CK), os vetores de vírus, malwares e PUPs/PUAs identificados com maior reincidência global de tentativas de ataque à infraestrutura da rede; Os relatórios investigativos evidenciando de forma nominal (nome de host ou IP) as estações de trabalho mapeadas como alvo preferencial e que mais registraram interações de logs focados em mitigação de infecção em um escopo ou janela de dias previamente definida na busca; Os relatórios extraídos correlacionando identidades e destacando com ênfase as contas de perfis de usuário logadas nos instantes críticos onde o agente mais detectou comportamentos suspeitos e evitou comprometimentos ativos contra a rede corporativa, suportando filtro por um período parametrizado; Possibilidade unificada de licenciamento, ativação, delegação e administração tática para que a equipe técnica utilize todos os módulos integrantes da suíte a partir desta tela mestre (master pane); O servidor e seus componentes web front-end não deverão depender apenas de linhas de base textual, provendo uma visualização moderna orientada a módulos gráficos ou mini painéis conhecidos como Dashboards na página inicial de acompanhamento (Home Screen); Os módulos e visões gráficas presentes nos referidos Dashboards devem apresentar nativamente recursos interativos (clicáveis com técnica Drill-Down) de leitura prática, devendo o fornecedor assegurar a abrangência visual para todos os relatórios estratégicos mapeados anteriormente; Possuir regras lógicas automáticas embutidas ou perfis móveis flexíveis na gerência central aptos a orientarem e manterem a atualização fluida para a proteção completa dos agentes de antivírus hospedados em equipamentos móveis e computadores em constante viagem, conhecidos como endpoints portáteis (como notebooks da força de vendas corporativa ou regime home office), realizando os devidos downloads em plano de fundo quer se encontrem acoplados presencialmente através de comunicação LAN via rede interna ou operando remotamente ancorados por túnel VPN; Os fluxos lógicos voltados à redução de contenção de roteamento na distribuição na rede matriz ou filiais devem englobar a arquitetura provendo permissão ao uso orquestrado e simultâneo de inúmeros espelhos, também conhecidos com a denominação técnica de múltiplos repositórios internos locais, aptos a hospedarem fisicamente o volume de instalação matriz para as builds de novos produtos requisitadas via rede local, e a prover o espelhamento diário contendo os fragmentos de arquivo referenciando a vacina e assinaturas via mecanismo seletivo de sincronização diferencial entre tais servidores locais; Para suprir de forma robusta e rastreável eventuais necessidades periciais da própria gerência de redes (certificações SOX e afins), de terno motor de registros uma base relacional sólida dispondo de capacidade técnica autônoma com retenção configurável para processar e exportar ininterruptamente históricos estruturados, registrando de forma inalterável a tabela de alterações nas normas de sistema bem como na atribuição de privilégios entre técnicos da empresa, popularmente chamada de registros/logs transacionais voltados à rotina de auditoria sistêmica e investigativa; Na gestão macro dos milhares de endpoints operacionais mapeados na rede ou isolados via política autônoma, permitir dentro de sua base estrutural do gerenciamento a criação e associação múltipla atribuindo etiquetas lógicas personalizáveis ou tags predefinidas diretamente associadas ao inventário das máquinas virtuais ou computadores físicos registrados no banco, de modo a instrumentalizar este recurso permitindo ao próprio administrador usar estas tags como balizadores lógicos aptos a promover o cálculo do filtro condicional de movimentação e a distribuição autônoma de nós (equipamentos) reajustando-os e arrastando suas permissões por dentro dos subgrupos lógicos hierárquicos vigentes no coração da arquitetura desenhada em sua estrutura matricial de gerenciamento corporativo diário; Conforme já estipulado no quesito central em itens supramencionados de especificação técnica e de comunicação de infraestrutura e serviços , ser capaz de suportar por via nativa do fornecedor oficial a disponibilidade absoluta aos perfis sistêmicos exigindo que todo seu leque interativo para configuração de chaves gerenciais seja suportado universalmente fornecendo amplo acesso interativo em sua interface ou à sua tela primária de console mestre conectando-se sob rigorosa exigência exclusivamente a interações web a partir de qualquer segmento validado e seguro (interface web-based SaaS e navegação).

4. REQUISITOS DA CONTRATAÇÃO

Requisitos de Negócio:

4.1. A presente contratação orienta-se pelos seguintes requisitos de negócio:

4.1.1. As soluções de proteção do Antivírus modelo ESET aproveitam as tecnologias multicamadas em equilíbrio dinâmico para constantemente balancear performance, detecção e falsos positivos. Fornece proteção avançada para todo o armazenamento de arquivo de rede, servidores gerais e servidores multiuso. Asseguram que os servidores fiquem estáveis e livres de conflito. Limita reinicializações e janelas de manutenção a um mínimo para garantir a continuidade das atividades. Fornece Proteção contra ataques direcionados, contra ransomware, contra ataques sem arquivo e também oferece gerenciamento remoto e unificado, permitindo ao Gestor de TI local verificar o status da proteção de todas as máquinas onde o software está instalado.

Requisitos de Capacitação

4.2. Não faz parte do escopo da contratação a realização de capacitação técnica na utilização dos recursos relacionados ao objeto da presente contratação;

Requisitos Legais

4.3. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133, de 2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis;

Requisitos de Manutenção

4.4. Devido às características da solução, há necessidade de realização de manutenções adaptativas e evolutivas (toda vez que houver atualizações e inovações do software) pela Contratada, visando à manutenção da disponibilidade da solução e ao aperfeiçoamento de suas funcionalidades;

Requisitos Temporais

4.5. Os serviços devem ser prestados no prazo máximo de 24 horas, a contar do recebimento da abertura da Ordem de Serviço (OS), emitida pela Contratante, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante;

4.6. Na contagem dos prazos estabelecidos neste Termo de Referência, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento.

4.7. Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias corridos. Ressaltando que serão contados os dias a partir da hora em que ocorrer o incidente até a mesma hora do último dia, conforme os prazos.

4.9. Na execução dos serviços, deverá ser observado o seguintes prazo:

4.9.1. Inicio do fornecimento das 100 licenças, impreterivelmente no dia 01/07/2026.

Requisitos de Segurança e Privacidade

4.10. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação do Contratante, e alinhados à legislação vigente e aos padrões estabelecidos pelo Governo Digital:

4.10.1. **Conformidade com Normativos**:

- Observância da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) para tratamento de dados pessoais.
- Cumprimento da Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, que dispõe sobre requisitos mínimos de segurança da informação para soluções de computação em nuvem.

- Alinhamento aos guias e modelos de privacidade e segurança disponibilizados pela Secretaria de Governo Digital (SGD) e pela Advocacia-Geral da União (AGU).

Requisitos Técnicos:

- Implementação de controles criptográficos, registros de logs e políticas de segurança da informação e privacidade.
- Garantia de disponibilidade, integridade e confidencialidade dos dados, incluindo mecanismos de rastreabilidade e trilha de auditoria.
- Gestão de riscos de segurança da informação, com processos definidos para identificação, avaliação e mitigação de vulnerabilidades.
- Realização de auditorias periódicas de conformidade com os requisitos de segurança e privacidade estabelecidos no contrato.

Tratamento de Incidentes:

- Implementação de um plano de resposta a incidentes de segurança, com procedimentos claros para notificação, investigação e remediação de incidentes.
- Sistematização da gestão e tratamento de incidentes, incluindo relatórios periódicos ao órgão contratante.

Computação em Nuvem (se aplicável):

- Provedores de serviços em nuvem devem possuir, no mínimo, dois data centers em território brasileiro, conforme exigência da IN GSI/PR nº 5/2021.
- Certificações de normas de segurança da informação aplicáveis ao objeto da contratação, conforme justificativa prévia.

Outros Requisitos:

- Definição de processos de gestão de mudanças e implementação de gestão de capacidade.
- Exigência de conformidade com normas técnicas e certificações emitidas por instituições credenciadas, como ABNT e INMETRO.

Requisitos Sociais, Ambientais e Culturais

4.11. Os serviços devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais alinhados à legislação vigente e aos padrões estabelecidos pelo Governo Digital.

Requisitos da Arquitetura Tecnológica

4.12. Os serviços deverão ser executados observando-se as diretrizes de arquitetura tecnológica estabelecidas pela área técnica da Contratante.

4.13. A adoção de tecnologia ou arquitetura diversa deverá ser autorizada previamente pela Contratante. Caso não seja autorizada, é vedado à Contratada adotar arquitetura, componentes ou tecnologias diferentes daquelas definidas pela Contratante.

Requisitos de Projeto e de Implementação

4.14. Os serviços deverão observar integralmente os requisitos de definição do objeto descritos no item 3 deste termo de referência.

Requisitos de Implantação

4.15. Os serviços deverão observar integralmente os requisitos de implantação, instalação e fornecimento descritos neste termo de referência e no estudo técnico preliminar anexo a este documento.

Requisitos de Garantia e Manutenção

4.16. O prazo de garantia é aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), e suas atualizações.

Requisitos de Experiência Profissional

4.17. Não serão exigidos requisitos de experiência profissional para a presente a contratação.

Requisitos de Formação da Equipe

4.18. Não serão exigidos requisitos de formação da equipe para a presente a contratação.

Requisitos de Metodologia de Trabalho

4.19. A execução dos serviços está condicionada ao recebimento pelo Contratado de Ordem de Serviço (OS) emitida pela Contratante.

4.20. A OS indicará o serviço, a quantidade e a localidade na qual os deverão ser prestados.

4.21. O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 24 horas por dia e 7 dias por semana de maneira eletrônica e 8 horas por dia e 5 dias por semana por via telefônica.

4.22. A execução do serviço dever ser acompanhada pelo Contratado, que dará ciência de eventuais acontecimentos à Contratante.

Requisitos de Segurança da Informação e Privacidade

4.23. O Contratado deverá observar integralmente os requisitos de Segurança da Informação e Privacidade descritos a seguir:

- Observância da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) para tratamento de dados pessoais.
- Cumprimento da Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, que dispõe sobre requisitos mínimos de segurança da informação para soluções de computação em nuvem.
- Alinhamento aos guias e modelos de privacidade e segurança disponibilizados pela Secretaria de Governo Digital (SGD) e pela Advocacia-Geral da União (AGU).

Vistoria

4.24. Não há necessidade de realização de avaliação prévia do local de execução dos serviços.

Sustentabilidade

4.25. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis.

Indicação de marcas ou modelos

4.26. Na presente contratação será admitida a indicação da seguinte(s) marca(s), característica(s) ou modelo(s), de acordo com as justificativas contidas nos Estudos Técnicos Preliminares: Somente será aceito o software antivírus modelo ESET PROTECT ou similar, em decorrência da necessidade de padronização do objeto, uma vez que, as 100 maquinas onde serão renovadas as licenças já fazem uso do referido software antivírus, sendo este o único capaz de atender às necessidades do contratante.

Subcontratação

4.27. Não será admitida a subcontratação do objeto contratual.

Garantia da contratação

4.28. Não haverá exigência da garantia da contratação dos art. 96 e seguintes da Lei nº 14.133, de 2021, pelas razões constantes do Estudo Técnico Preliminar.

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da CONTRATANTE:

5.1.1. nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

5.1.2. encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

5.1.3. receber o objeto fornecido pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

5.1.4. aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

5.1.5. liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

5.1.6. comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

5.1.7. definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do contratado, com base em pesquisas de mercado, quando aplicável;

5.1.8. prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer.

5.2. São obrigações do CONTRATADO:

5.2.1. indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato;

5.2.2. atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

5.2.3. reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;

5.2.4. propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

5.2.5. manter, durante toda a execução do contrato, as mesmas condições da habilitação;

5.2.6. quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

5.2.7. quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

5.2.8. ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;

5.2.9. fazer a transição contratual, quando for o caso.

5.3. São obrigações do órgão gerenciador do registro de preços:

5.3.1. efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;

5.3.2. conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;

5.3.3. definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:

5.3.4. as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e

5.3.5. definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável;

5.3.6. definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:

5.3.7. a definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;

5.3.8. as regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pelo contratado; e

5.3.9. as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a verificação de Amostra do Objeto, observado o disposto no inciso III, alínea "c", item 2 do art. 17 da Instrução Normativa SGS/ME nº 94, de 2022, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

6. MODELO DE EXECUÇÃO DO OBJETO

Condições de execução

6.1. A execução do objeto seguirá a seguinte dinâmica:

6.1.1. Início da execução do objeto: no dia 01/07/2026 após emissão da ordem de serviço.

6.1.2. A entrega das licenças de uso dos softwares dar-se-á através do fornecimento, pela contratada à contratante, de link para acesso/download às licenças que possibilitarão fazer uso do software.

6.1.3. A instalação do software fica a cargo do cliente, com total apoio da contratada.

6.1.4. A contratada deverá se comprometer a entregar modelo original do software Eset Protect e todas as atualizações automáticas do antivírus (toda vez que houver).

Local e horário da prestação dos serviços

6.2. Os serviços serão entregues através do endereço de e-mail, que serão repassado posteriormente, da área de suporte técnico do Laboratório de Informática do Instituto de Geociências/UFMG, sob os cuidados do técnico Vinicius Etrusco.

Rotinas a serem cumpridas

6.3. O e-mail para o acesso/download às licenças, deverá ser enviado pela contratada, até 03 dias após o recebimento da Nota de Empenho.

Materiais a serem disponibilizados

6.4. Para a perfeita execução dos serviços, o Contratado deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas e qualidades a seguir estabelecidas, promovendo sua substituição quando necessário:

6.4.1. Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software - antivírus ESET PROTECT, com todas as atualizações automáticas disponíveis;

6.4.2. Serão fornecidas 100 (cem) licenças do software antivírus ESET PROTECT ENTRY.

Informações relevantes para o dimensionamento da proposta

6.5. A demanda do órgão tem como base as seguinte característica:

6.5.1. Proteger o sistema contra ameaças cibernéticas. A renovação de licenças de antivírus tem como intuito dar continuidade no trabalho de prevenir a contaminação por vírus, malwares, suas variantes e demais ameaças cibernéticas, nos computadores que podem pôr em risco o sigilo, a integridade e a disponibilidade das informações, a não renovação do mesmo poderá causar problemas de segurança nos computadores, demandando mais manutenção e por consequência atrasos/interrupções nos serviços;

Formas de transferência de conhecimento

6.6. Não será necessária transferência de conhecimento devido às características do objeto.

Procedimentos de transição e finalização do contrato

6.7. Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

Quantidade mínima de serviços para comparação e controle

6.8. Serão fornecidas 100 (cem) licenças do software antivírus ESET PROTECT ENTRY.

Mecanismos formais de comunicação

6.9. São definidos como mecanismos formais de comunicação, entre a Contratante e o Contratado, os seguintes:

I) Ordem de Serviço;

II) Ata de Reunião;

III) Ofício;

IV) Sistema de abertura de chamados;

V) E-mails e telefones;

Manutenção de Sigilo e Normas de Segurança

6.10. O Contratado deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

7. MODELO DE GESTÃO DO CONTRATO

7.1. 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.

7.2. 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.

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

7.4. O órgão ou entidade poderá convocar o preposto da empresa para adoção de providências que devam ser cumpridas de imediato.

Preposto

7.5. O Contratado designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto Contratado.

7.6. O Contratado não necessitará manter preposto da empresa no local da execução do objeto durante o período de vigência da contratação.

7.7. O Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que o Contratado designará outro para o exercício da atividade.

Reunião Inicial

7.8. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

7.9. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em dias úteis, podendo ser prorrogada a critério da Contratante.

7.10. A pauta desta reunião observará, pelo menos:

7.10.1. Presença do representante legal da contratada, que apresentará o seu preposto;

7.10.2. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

7.10.3. esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

7.10.4. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

7.10.5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

Rotinas de Fiscalização

7.11. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos, nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

Fiscalização Técnica

7.12. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

7.13. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados.

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

7.15. O fiscal técnico do contrato informará ao gestor do contato, 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.

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

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

7.18. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade do Contratado, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade do Contratante ou de seus agentes, gestores e fiscais, de conformidade.

Fiscalização Administrativa

7.19. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, 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.

7.20. Caso ocorra 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.

Gestor do Contrato

7.21. Cabe ao gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022:

7.21.1. coordenar 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.

7.21.2. acompanhar os registros realizados pelos fiscais 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.

7.21.3. acompanhar 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.

7.21.4. emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial 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.

7.21.5. tomar 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. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso.

7.21.6. elaborar 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.

7.21.7. enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, com a indicação expressa de que o valor da Nota Fiscal emitida pela contratada confere com o valor dimensionado pela fiscalização e gestão no recebimento definitivo do serviço.

7.21.8. receber e dar encaminhamento imediato:

7.21.8.1. às denúncias de discriminação, violência e assédio no ambiente de trabalho, conforme o art. 2º, inciso III, do Decreto n.º 12.174/2024;

7.21.8.2. à notificação formal de que a empresa contratada está descumprindo suas obrigações trabalhistas, enviada pelo trabalhador, sindicato, Ministério do Trabalho, Ministério Público, Defensoria Pública ou por qualquer outro meio idôneo.

8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

8.1. A avaliação da execução do objeto utilizará o disposto nesta seção, devendo haver o redimensionamento no pagamento caso os indicadores estabelecidos não sejam cumpridos.

8.2. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que o Contratado:

8.2.1. não produziu os resultados acordados,

8.2.2. deixou de executar, ou não executou com a qualidade mínima exigida as atividades contratadas; ou

8.2.3. deixou de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou os utilizou com qualidade ou quantidade inferior à demandada.

Recebimento

8.3. Os serviços serão recebidos provisoriamente, no prazo de até 3 (três) dias, pelo Setor de Tecnologia da Informação do Instituto de Geociências/UFMG, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo.

8.4. O prazo para recebimento provisório será contado do recebimento de comunicação de cobrança oriunda do Contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

8.5. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico.

8.6. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo.

8.7. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.

8.8. Para efeito de recebimento provisório, será considerado para fins de faturamento o período de 7 (sete) dias úteis após o recebimento e instalação da licença do software antivírus pelo setor requisitante.

8.9. Ao final de cada período/evento de faturamento:

8.9.1. o fiscal técnico do contrato deverá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos no ato convocatório, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato;

8.10. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último.

8.11. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no recebimento provisório.

8.12. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no recebimento provisório.

8.13. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

8.14. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

8.15. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

8.16. Os serviços serão recebidos definitivamente no prazo de 5 (cinco) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

8.16.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento.

8.16.2. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando ao Contratado, por escrito, as respectivas correções;

8.16.3. Emitir Termo Detalhado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

8.16.4. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

8.16.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

8.17. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal quanto à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

8.18. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo Contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

8.19. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

Procedimentos de Teste e Inspeção

8.20. Serão adotados como procedimentos de teste e inspeção, para fins de elaboração dos Termos de Recebimento Provisório e Definitivo:

8.20.1. A liberação e instalação das cem licenças do software antívirus ESET PROTECT originais;

8.20.2. disponibilização de todas as atualizações e inovações do software; e

8.20.3. suporte técnico on-line durante todo o período contratual.

Liquidação

8.21. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §3º da Instrução Normativa SEGES/ME nº 77/2022.

8.22. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, nos casos de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

8.23. Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

I) o prazo de validade;

II) a data da emissão;

III) os dados do contrato e do órgão contratante;

IV) o período respectivo de execução do contrato;

V) o valor a pagar; e

VI) eventual destaque do valor de retenções tributárias cabíveis.

8.24. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o Contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao Contratante.

8.25. 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. 68 da Lei nº 14.133/2021.

8.26. A Administração deverá realizar consulta ao SICAF para:

8.26.1. verificar a manutenção das condições de habilitação exigidas;

8.26.2. Identificar possível razão que impeça a participação em licitação/contratação no âmbito do órgão ou entidade, tais como a proibição de contratar com a Administração ou com o Poder Público, bem como ocorrências impeditivas indiretas.

8.27. Constatando-se, junto ao SICAF, a situação de irregularidade do Contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (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 do Contratante.

8.28. Não havendo regularização ou sendo a defesa considerada improcedente, o Contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do Contratado, 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.

8.29. Persistindo a irregularidade, o Contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao Contratado a ampla defesa.

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

Prazo de pagamento

8.31. O pagamento será efetuado no prazo máximo de até dez dias úteis, contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

8.32. No caso de atraso pelo Contratante, os valores devidos ao Contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IGP-M de correção monetária.

Forma de pagamento

8.33. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo Contratado.

8.34. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

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

8.35.1. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

8.36. O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 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.

Reajuste

8.37. Os preços inicialmente contratados são fixos e irreajustáveis, para todo o período da vigência, contado da data do orçamento estimado, em 26/06/2026.

Cessão de Crédito

8.38. As cessões de crédito dependerão de prévia aprovação do Contratante.

8.38.1. A eficácia da cessão de crédito, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

8.38.2. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do Contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 8.429, de 1992, nos termos do Parecer JL-01, de 18 de maio de 2020.

8.38.3. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (Contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração.

8.38.4. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do Contratado.

8.39. O disposto nesta seção não afeta as operações de crédito de que trata a Instrução Normativa SEGES/MGI nº 82, de 21 de fevereiro de 2025, as quais ficam por esta regidas.

9. SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO

9.1. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela contratante, conforme a tabela abaixo:

Id	*Ocorrência*	*Glosa / Sanção*
1	*Não prestar os esclarecimentos imediatamente, referente à execução dos serviços, salvo quando implicarem em*	*Multa de (0,2) % sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela contratante, até o limite de 5 (cinco) dias úteis.*

	indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de (4) horas úteis.	*Após o limite de 5 (cinco) dias úteis, aplicar-se-á multa de (0,5) % do valor total do Contrato.*
2	*Não cumprir qualquer outra obrigação contratual não citada nesta tabela.*	*Advertência.* *Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 2 (dois) % do valor total do Contrato.*

9.2. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que o contratado:

9.2.1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

9.2.2. deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

9.3. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:

a) der causa à inexecução parcial do contrato;

b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;

c) der causa à inexecução total do contrato;

d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

f) praticar ato fraudulento na execução do contrato;

g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

9.4. Serão aplicadas ao Contratado que incorrer nas infrações acima descritas as seguintes sanções:

9.4.1. Advertência, quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;

9.4.2. Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima, sempre que não se justificar a imposição de penalidade mais grave;

9.4.3. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave.

9.4.4. Multa:

9.4.4.1. Moratória, para as infrações descritas no item “d”, de **2**% (**dois** por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de **5** (**cinco**) dias.

9.4.4.2. Moratória de 0,07% (sete centésimos por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 2% (dois por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia;

9.4.4.2.1. O atraso superior a 25 (vinte e cinco) dias para apresentação, suplementação ou reposição da garantia autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

9.4.4.3. Compensatória, para as infrações descritas acima alíneas "**e**" a "**h**" de **1**% (**um** por cento) a **2**% (**dois** por cento) do valor da contratação.

9.4.4.4. Compensatória, para a inexecução total do contrato prevista acima na alínea "**c**", de **2**% (**dois** por cento) a **5**% (**cinco** por cento) do valor da contratação.

9.4.4.5. Compensatória, para a infração descrita acima na alínea "**b**", de **2**% (**dois** por cento) a **4**% (**quatro** por cento) do valor da contratação.

9.4.4.6. Compensatória, em substituição à multa moratória para a infração descrita acima na alínea "d", de **2**% (**dois** por cento) a **4**% (**quatro** por cento) do valor da contratação.

9.4.4.7. Compensatória, para a infração descrita acima na alínea "**a**", de **1**% (**um** por cento) a **5**% (**cinco** por cento) do valor da contratação, ressalvadas as seguintes infrações também enquadráveis nessa alínea:

9.5. A aplicação das sanções previstas neste Termo de Referência não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante.

9.6. Todas as sanções previstas neste Termo de Referência poderão ser aplicadas cumulativamente com a multa.

9.7. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

9.8. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

9.9. A multa poderá ser recolhida administrativamente no prazo máximo de 15 (quinze) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

9.10. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

9.10.1. Para a garantia da ampla defesa e contraditório, as notificações serão enviadas eletronicamente para os endereços de e-mail informados na proposta comercial, bem como os cadastrados pela empresa no SICAF.

9.10.2. Os endereços de e-mail informados na proposta comercial e/ou cadastrados no SICAF serão considerados de uso contínuo da empresa, não cabendo alegação de desconhecimento das comunicações a eles comprovadamente enviadas.

9.11. Na aplicação das sanções serão considerados:

9.11.1. a natureza e a gravidade da infração cometida;

9.11.2. as peculiaridades do caso concreto;

9.11.3. as circunstâncias agravantes ou atenuantes;

9.11.4. os danos que dela provierem para o Contratante; e

9.11.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

9.12. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei.

9.13. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Termo de Referência ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

9.14. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP), instituídos no âmbito do Poder Executivo Federal.

9.14.1. As penalidades serão obrigatoriamente registradas no SICAF.

9.15. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133, de 2021.

9.16. Os débitos do Contratado para com a Administração Contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o Contratado possua com o mesmo órgão ora Contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

Forma de seleção e critério de julgamento da proposta

10.1. O fornecedor será selecionado por meio da realização do procedimento de DISPENSA DE LICITAÇÃO COM DISPUTA, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO.

Regime de Execução

10.2. O regime de execução do contrato será por Nota de Empenho.

Exigências de habilitação

10.3. Para fins de habilitação, deverá o interessado comprovar os seguintes requisitos:

Habilitação jurídica

10.4. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

10.5. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

10.6. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

10.7. 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;

10.8. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

10.9. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

10.10. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

10.11. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

10.12. Consórcio de empresas: contrato de consórcio devidamente arquivado no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis (art. 279 da Lei nº 6.404, de 15 de dezembro de 1976) ou compromisso público ou particular de constituição, subscrito pelos consorciados, com a indicação da empresa líder, responsável por sua representação perante a Administração (art. 15, caput, I e II, da Lei nº 14.133, de 2021).

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

Habilitação fiscal, social e trabalhista

10.14. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

10.15. 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 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

10.16. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

10.17. 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;

10.18. Prova de inscrição no cadastro de contribuintes Distrital ou Municipal relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

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

10.20. Caso o fornecedor seja considerado isento dos tributos relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

10.21. 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.

Qualificação Econômico-Financeira

10.22. certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do interessado, caso se trate de pessoa física, desde que admitida a sua participação na licitação/contratação, ou de sociedade simples;

10.23. certidão negativa de falência expedida pelo distribuidor da sede do fornecedor;

10.24. balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, comprovando, índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um), obtidos por meio da aplicação das seguintes fórmulas:

$$LG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

10.25. Caso a empresa apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido, para fins de habilitação, **capital mínimo** de **10% valor total estimado da contratação.**

10.26. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos;

10.27. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

10.28. As empresas criadas no exercício financeiro da licitação/contratação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.

Disposições gerais sobre habilitação

10.29. Quando permitida a participação na licitação/contratação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

10.30. Na hipótese de o fornecedor ser empresa estrangeira que não funcione no País, para assinatura do contrato ou da ata de registro de preços ou do aceite do instrumento equivalente, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

10.31. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

10.32. 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, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

10.33. 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.

Documentação complementar para cooperativas

10.34. Caso admitida a participação de cooperativas, será exigida a seguinte documentação complementar:

10.34.1. A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971;

10.34.2. A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

10.34.3. A comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço;

10.34.4. O registro previsto na Lei n. 5.764, de 1971, art. 107;

10.34.5. A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato;

10.34.6. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa:

10.34.6.1. ata de fundação;

10.34.6.2. estatuto social com a ata da assembleia que o aprovou;

10.34.6.3. regimento dos fundos instituídos pelos cooperados, com a ata da assembleia;

10.34.6.4. editais de convocação das três últimas assembleias gerais extraordinárias;

10.34.6.5. três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais;

10.34.6.6. ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da contratação; e

10.34.6.7. última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O custo estimado total da contratação, que é o máximo aceitável, é de R$29.960,00 (vinte e nove mil, novecentos e sessenta reais), conforme custos unitários apostos na tabela contida no item 1.1 acima.

12. ADEQUAÇÃO ORÇAMENTÁRIA

12.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

12.2. A contratação será atendida pela seguinte dotação:

I) Gestão/unidade: 15229 / 153293;

II) Fonte de recursos: 3050000377;

III) Programa de trabalho: 230045;

IV) Elemento de despesa: 339040 - 06; e

V) Plano interno: MSUPEG1993N.

13. DISPOSIÇÕES FINAIS

13.1. As informações contidas neste Termo de Referência não são classificadas como sigilosas.

Cronograma Físico Financeiro

Evento	Prazo estimado	Valor
Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software - ESET PROTECT - Renovação da Licença por 60 meses	(01/07/2026) a (30/06/2031)	R$29.960,00

Integrante **Requisitante** **SETOR DE TECNOLOGIA DA INFORMAÇÃO**	**Integrante** **Técnico** **Bruno William Mendes Salustiano** **Técnico de Laboratório** ****970****	**Integrante** **Administrativo** **Gabriel Amaral de Pinho** Assistente em Administração ******87*-*

Autoridade Máxima da Área de TIC
Vinícius Etrusco Moreira, Técnico de Laboratório **915**

Belo Horizonte, 18 de junho de 2026

Aprovo,

Autoridade Competente
ÚRSULA RUCHKYS DE AZEVEDO

Diretora do Instituto de Geociências da UFMG

14. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

GABRIEL AMARAL DE PINHO

Membro da comissão de contratação

Assinou eletronicamente em 24/06/2026 às 10:32:28.

VINICIUS ETRUSCO MOREIRA

Membro da comissão de contratação

Assinou eletronicamente em 24/06/2026 às 11:27:41.

BRUNO WILLIAM MENDES SALUSTIANO

Membro da comissão de contratação

Assinou eletronicamente em 24/06/2026 às 10:35:11.