UFG

UNIVERSIDADE FEDERAL DE GOIÁS
DIRETORIA DE COMPRAS

TERMO DE REFERÊNCIA

Processo nº 23070.054244/2022-06

PREGÃO ELETRÔNICO SRP Nº 070/2022

ANEXO I - TERMO DE REFERÊNCIA

1. DO OBJETO

1.1. **Registro de Preços para aquisição com fornecimento parcelado de SOFTWARE, APLICAÇÃO INFORMÁTICA, TIPO ANTIVÍRUS, SOLUÇÃO PARA PROTEÇÃO DE ESTAÇÕES DE TRABALHO**, conforme condições e exigências estabelecidas neste instrumento e respectivo edital.

1.1.1. A descrição detalhada dos itens da solução de TIC que integram o objeto desta licitação, o código do CATMAT, e as respectivas quantidades, seguem na Tabela abaixo:

Tabela 1 - Itens da Licitação

ITEM	CATSER	UN	ESPECIFICAÇÕES	QT. UFG	QT. IFMT CAMPO NOVO DO PARECIS	QT. IF Goiano	QT. IFMT BARRA DO GARÇAS	QT. IFMT CAMPUS CUIABÁ	QT. IFG	QT. IFMS	QT. IFMT CAMPUS TANGARÁ DA SERRA
1	27456	UN	SOFTWARE, APLICAÇÃO INFORMÁTICA, TIPO ANTIVÍRUS, SOLUÇÃO PARA PROTEÇÃO DE ESTAÇÕES DE TRABALHO E DISPOSITIVOS MÓVEIS CONTEM PLANDO 36 MESES DE SUPORTE E GARANTIA, ACOMPANHADA DE TREINAMENTO ON LINE DA EQUIPE DA CONTRATANTE	1000	70	800	60	950	2000	3900	120
2	27472	UN	SOFTWARE, APLICAÇÃO INFORMÁTICA, TIPO ANTIVÍRUS, SOLUÇÃO PARA PROTEÇÃO DE SERVIDORES (WINDOWS E LINUX) CONTEMPLANDO 36 MESES DE SUPORTE E GARANTIA, ACOMPANHADA DE TREINAMENTO ON LINE DA EQUIPE DA CONTRATANTE	30	02	150	1	10	100	100	01
TOTAL PREVISTO UNIVERSIDADE FEDERAL DE GOIÁS - GOIÂNIA-GO											**R$ 388.000,00**
TOTAL PREVISTO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MATO GROSSO - CAMPUS CAMPO NOVO DO PARECIS											**R$ 26.810,00**
TOTAL PREVISTO INSTITUTO FEDERAL GOIANO - GOIÂNIA-GO											**R$ 751.400,00**
TOTAL PREVISTO INSTITUTO FEDERAL DE MATO GROSSO - CAMPUS BARRA DO GARÇAS											**R$ 20.480,00**
TOTAL PREVISTO INSTITUTO FEDERAL DE MATO GROSSO - CAMPUS CUIABÁ											**R$ 303.850,00**
TOTAL PREVISTO INSTITUTO FEDERAL DE EDUCAÇÃO E CIÊNCIA E TECNOLOGIA DE GOIÁS											**R$ 916.000,00**
TOTAL PREVISTO INSTITUTO FEDERAL DE EDUCAÇÃO E CIÊNCIA E TECNOLOGIA DO MATO GROSSO DO SUL											**R$ 1.453.700,00**
TOTAL PREVISTO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MATO GROSSO - CAMPUS TANGARÁ DA SERRA											**R$ 37.460,00**
TOTAL GLOBAL PREVISTO PARA O GRUPO											**R$ 3.897.700,00**

Tabela 2 - Macro Requisitos Tecnológicos e Demais Requisitos

Item 01 - SOFTWARE, APLICAÇÃO INFORMÁTICA, TIPO ANTIVÍRUS, SOLUÇÃO PARA PROTEÇÃO DE ESTAÇÕES DE TRABALHO E DISPOSITIVOS MÓVEIS CONTEMPLANDO 36 MESES DE SUPORTE E GARANTIA, ACOMPANHADA DE TREINAMENTO ON LINE DA EQUIPE DA CONTRATANTE.

Funcionalidades:

1.1.1. Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;

1.1.2. Deve ser integrada ao Windows Security center, quando utilizado plataforma Microsoft;

1.1.3. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, ransomware e fileless;

1.1.4. A solução de antivírus deverá possuir funcionalidades específicas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos com a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

1.1.5. A solução de antivírus deverá detectar e informar as fontes de infecção de ameaças.

1.1.6. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em: processos em execução em memória principal (RAM), arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou PowerShell) e arquivos compactados automaticamente, em pelo menos os seguintes formatos: zip, exe, arj, mime/uu, Microsoft cab;

1.1.7. Deve permitir configurar o consumo de cpu que será utilizada para uma varredura manual ou agendada;

1.1.8. Deve possuir mecanismo de cache de informações dos arquivos já escaneados;

1.1.9. Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;

1.1.10. Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento;

1.1.11. Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL's maliciosas;

1.1.12. Deve ser capaz de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks;

1.1.13. Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentenar a ameaça;

1.1.14. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;

1.1.15. Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de apresentarem risco de segurança;

1.1.16. Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;

1.1.17. Deve ter funcionalidade de Machine Learn para detectar e tomar ações sobre ameaças desconhecidas e suspeitas;

1.1.18. A Machine Learn deverá funcionar em modo on-line consultando informações em nuvem e off-line;

1.1.19. Deve fornecer um informativo compreensivo de cada simulação que descreva as ações e respectivos metadados, bem como, o porquê do veredicto emitido pela Machine Learn;

1.1.20. Deve bloquear processos comuns associados a ransomware;

1.1.21. Os módulos de segurança para enpoints, como antimalware, controle de aplicação, controle de dispositivos, firewall (host), reputação de URL's, machine learning e proteção a vulnerabilidades devem ser geridos por um único agente a ser instalado na estação de trabalho.

Funcionalidade de administração e gerência:

1.2.1. A console de gerenciamento central deve permitir a integração e correlação de eventos entre todos os componentes da solução ofertada;

1.2.2. A console de gerenciamento deve monitorar e exibir as ações a serem tomadas para os objetos enviados pela solução de Anti Malware;

1.2.3. A solução de gerenciamento deve permitir que o administrador adicione de forma manual arquivos, ips, urls, domínios e defina ação para cada tipo detecção;

1.2.4. Deve gerenciar logs das atividades e eventos gerados pela solução;

1.2.5. Nas informações da política deve conter informações como nome, status, dono da política, horário e data da última alteração;

1.2.6. A gerência central deverá mostrar quais estações estão sem políticas;

1.2.7. Deve gerar relatório de compliance com informações de máquinas que nunca realizaram scan, políticas inconsistentes entre servidor/agente e componentes desatualizados;

1.2.8. Deve possuir integração com Microsoft Active Directory;

1.2.9. Deve permitir níveis de administração da console por usuários ou grupos de usuários;

1.2.10. Deve permitir a constituição de políticas genéricas aplicáveis a máquinas, grupos de usuários ou maquinas;

1.2.11. Deve disponibilizar sua interface através dos protocolos https;

1.2.12. Deve permitir diferentes níveis de administração, de maneira independente do login da rede;

1.2.13. Geração de relatórios e gráficos e parametrizáveis nos formatos html, pdf, xml e csv;

1.2.14. Deve gerar relatórios e gráficos pré-definidos em pelo menos dois dos seguintes formatos: pdf, docx e xlsx;

1.2.15. Os relatórios devem conter informações de efetividade, ransomware, canais de infecção, principais usuários que receberam ameaças, vírus e spyware;

1.2.16. Deve permitir criação de modelos de relatórios customizados;

1.2.17. Deve permitir a criação de planos de entrega das atualizações, com hora de início ou postergação da entrega após o download dos componentes;

1.2.18. Deve permitir o controle individual de cada componente a ser atualizado;

1.2.19. Deve permitir a definição de exceções por dias e horas para não realização de atualizações;

1.2.20. Deve permitir ter como fonte de atualização um compartilhamento de rede no formato UNC;

1.2.21. Deve gerar relatórios e gráficos com o detalhamento das versões dos produtos instalados;

1.2.22. Deve possuir o acompanhamento dos comandos administrativos em execução, tal como seu status de conclusão, alvo e usuário;

1.2.23. Deve permitir a configuração dos eventos administrativos ou de segurança que geram notificações, tal como o método de envio e o destinatário;

1.2.24. Os métodos de envio suportados devem incluir: e-mail, gravação de registros de eventos do Windows, SNMP e SYSlog;

1.2.25. Deve permitir a configuração do intervalo de comunicação entre a console e os agentes;

1.2.26. Deve permitir a escolha do intervalo de tempo necessário para que um agente seja considerado off-line;

1.2.27. Deve permitir a configuração do número de tentativas inválidas de login para o bloqueio de usuários;

1.2.28. Deve permitir a configuração da duração do bloqueio;

1.2.29. Deve permitir pesquisas personalizadas para a consulta de eventos (logs) através de categorias;

1.2.30. Deve permitir pesquisas personalizadas para a consulta de eventos (logs), através de critérios lógicos, com base em todos os campos pertencentes aos eventos consultados;

1.2.31. Deve permitir a configuração da manutenção dos registros de eventos (logs), com base no intervalo de tempo que devem ser mantidos e no número máximo de registros, por tipo de evento;

1.2.32. Deve de permitir a criação de políticas de segurança personalizadas;

1.2.33. As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios: Nome parcial ou completo das estações de trabalho, range de endereços IPS e Sistema operacional;

1.2.34. Deve permitir visualização de eventos de violação de segurança de todos os módulos gerenciados, agrupado por usuário numa linha de tempo configurável;

1.2.35. Deve permitir a gerência dos módulos baseados no modelo de nuvem (cloud), quando existentes;

1.2.36. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

1.2.37. A solução deverá possuir um dashboard pré-configurado com informações sobre estações desatualizadas, usuários afetados, estações sem o antimalware instalado, estações afetadas e ameaças críticas tipo Ransomware, ameaças desconhecidas e vulnerabilidades;

1.2.38. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamento;

1.2.39. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

1.2.40. Deve permitir o upload de IoCs (Indicators of Compromise) para realização de uma análise de impacto na rede utilizando o módulo de Investigação de Endpoint;

1.2.41. Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;

1.2.42. Deve possibilitar instalação "silenciosa";

1.2.43. Deve permitir o bloqueio por nome de arquivo;

1.2.44. Deve permitir o travamento de arquivos e pastas compartilhadas;

1.2.45. Deve permitir o travamento de portas;

1.2.46. Deve permitir o rastreamento e bloqueio de infecções;

1.2.47. Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;

1.2.48. Deve efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional previamente instalado;

1.2.49. Deve desinstalar automática e remotamente o cliente de antivírus, sem requerer outro software ou agente;

1.2.50. Deve permitir a desinstalação através da console de gerenciamento da solução;

1.2.51. Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;

1.2.52. Deve ter a possibilidade de determinar a capacidade de armazenamento da área de quarentena;

1.2.53. Deve permitir a deleção dos arquivos quarentenados;

1.2.54. Deve permitir remoção automática da exibição na console de clientes inativos por determinado período de tempo;

1.2.55. Deve permitir integração com Active Directory para acesso a console de administração;

1.2.56. Identificar através da integração com o Active Directory, quais máquinas estão sem a solução de antimalware instalada;

1.2.57. Deve permitir criação de diversos perfis e usuários para acesso a console de administração;

1.2.58. Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de antimalware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

1.2.59. Deve permitir agrupamento automático de estações de trabalho e notebooks da console de gerenciamento baseando-se no escopo do Active Directory ou IP;

1.2.60. Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;

1.2.61. Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

1.2.62. Deve registrar no sistema de monitoração de eventos da console de antimalware informações relativas ao usuário logado no sistema operacional;

1.2.63. Deve prover ao administrador informações sobre quais estações de trabalho e notebooks fazem parte do escopo de gerenciamento da console de antimalware e não realizaram o escaneamento agendado ou o escaneamento demandado pelo administrador no período determinado de dias;

1.2.64. Deve prover segurança através de SSL para as comunicações entre o servidor e a console de gerenciamento web;

1.2.65. Deve prover segurança através de SSL para as comunicações entre o servidor e os agentes;

1.2.66. Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;

1.2.67. Deve permitir a criação de usuários locais de administração da console de antimalware;

1.2.68. Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;

1.2.69. Deve bloquear acessos indevidos a área de administração do agente que não estejam na tabela de políticas definidas pelo administrador;

1.2.70. Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido na console de administração;

1.2.71. Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto;

1.2.72. Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;

1.2.73. Deve permitir atualização incremental da lista de definições de vírus;

1.2.74. Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;

1.2.75. Deve permitir o rollback das atualizações das listas de definições de vírus e engines;

1.2.76. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utilizá-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de antimalware para estas tarefas;

1.2.77. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hot fixes e configurações específicas de domínios da árvore de gerenciamento;

1.2.78. O servidor da solução de antimalware, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os agentes replicadores de atualizações e configurações, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

1.2.79. O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

Funcionalidade de controle de dispositivos:

1.3.1. Deve possuir o controle de acesso a drives de mídias de armazenamento como cdrom, dvd, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

1.3.2. Deve ser capaz de liberar ou bloquear os seguintes dispositivos Bluetooth, portas COM/LPT, IEEE 1394, infravermelho, modems, cartões PCMCIA, tecla print-screen e placas de rede wireless;

1.3.3. Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, modificar, leitura e execução, apenas leitura e listar somente o conteúdo;

1.3.4. Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, cdrom);

1.3.5. Possibilidade de adicionar novos dispositivos na lista de dispositivos utilizando “Class ID”, “Device ID” ou “Serial ID” do dispositivo;

1.3.6. A solução deverá possuir recursos de prevenção contra vazamentos de dados podendo criar regras baseadas em tipo de arquivo, extensão e expressão regular;

1.3.7. O recurso de prevenção contra vazamento de dados deve possuir integração com o módulo de criptografia;

1.3.8. A proteção contra vazamento de dados deverá verificar o tipo de arquivo pelo conteúdo;

1.3.9. Deve permitir a criação de modelos personalizados (templates) para identificação de informações;

1.3.10. Deve permitir mais de uma ação para cada política, como: Apenas registrar o evento da violação, bloquear a transmissão, gerar alertas para o usuário e gerar alertas na central de gerenciamento;

1.3.11. Na ação de bloqueio de transmissão de dados o usuário deverá colocar uma justificativa da ação que está realizando;

1.3.11. A proteção contra vazamento de dados deve monitorar a transmissão de dados através dos seguintes canais de rede: Email, FTP, HTTP e HTTPS, aplicações de mensagens instantâneas, SMB e Webmail.

1.3.12. A proteção contra vazamento de dados deve aplicar-se a serviços de armazenamento em nuvem, gravadores de dados em mídia (DVD,CD), HD externo, pendrive, Impressora e área de transferência do Windows.

Funcionalidade de Host Firewall e HIPS:

1.4.1. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host ips e host firewall;

1.4.2. As regras de vulnerabilidades deverão possuir a opção de desativar a regra de forma individual;

1.4.3. Todas as regras das funcionalidades de firewall e ips de host devem permitir apenas detecção (log) ou prevenção (bloqueio);

1.4.4. Deve permitir ativar e desativar o produto sem a necessidade de remoção;

1.4.5. Deve permitir que o administrador altere as configurações de níveis de segurança e exceções;

1.4.6. Deverá possuir a possibilidade de configurar níveis diferentes de segurança podendo ser eles Alto, médio e baixo;

1.4.7. Deverá prevenir contra os seguintes tipos de ataque: Too Big Fragment, Ping da morte, Conflito de ARP, SYN Flood, Overlapping Fragment, Teardrop, Tiny Fragment Attack, Fragmented IGMP e Land Attack;

1.4.8. O módulo de HIPS deverá possuir perfis pré-determinados baseados em performance e segurança;

1.4.9. O módulo de HIPS deverá possuir regras para proteger contra ameaças do tipo Ransomware;

1.4.10. O módulo de HIPS deverá conter regras contra exploit, vulnerabilidades e genéricas protegendo contra ameaças conhecidas ou desconhecidas;

Módulo para controle de aplicações:

1.5.1. As regras de controle de aplicação devem permitir as seguintes ações:

- Permissão de execução;
- Bloqueio de execução;
- Bloqueio de novas instalações;

1.5.2. As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação configurada na regra;

1.5.3. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações: assinatura sha-1 e sha-256 do executável; atributos do certificado utilizado para assinatura digital do executável, caminho lógico do executável, base de assinaturas de certificados digitais válidos e seguros;

1.5.4. As regras de controle de aplicação devem possuir categorias pré-determinadas de aplicações;

1.5.5. As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações;

1.5.6. O módulo de controle de aplicativos deve possuir uma lista de aplicações mal-intencionadas para bloqueio e monitoramento;

Módulo de criptografia:

1.6.1. Deve possuir módulo de criptografia para as estações de trabalho (desktops e notebooks), com as seguintes funcionalidades de criptografia para: Disco completo (fde – full disk encryption);

1.6.2. Deve possuir autenticação durante a inicialização (boot) da estação de trabalho, antes do carregamento do sistema operacional, para a funcionalidade de criptografia do disco completo;

1.6.3. A autenticação durante a inicialização (boot) deve ser a partir das credenciais sincronizadas com o Active Directory;

1.6.4. Deve possuir suporte ao algoritmo de criptografia aes-256;

1.6.5. Deve possuir criptografia no canal de comunicação entre as estações de trabalho e o servidor de políticas;

1.6.6. Deve possuir certificação FIPS 140-2;

1.6.7. Deve ser compaovel com os padrões SED ('self-encrypting drive), opal e opal2

1.6.8. Deve possuir compatibilidade de autenticação por múltiplos fatores;

1.6.9. Deve permitir atualizações do sistema operacional mesmo quando o disco está criptografado;

1.6.10. Deve permitir configurar senha de administração local na estação de trabalho para desinstalação do módulo;

1.6.11. Deve possuir políticas por usuários, grupos e dispositivos;

1.6.12. Deve possuir autoajuda para usuários que esqueceram a senha com a combinação de perguntas e respostas;

1.6.13. Deve possuir mecanismos para wipe (limpeza) remoto;

1.6.14. Deve possuir mecanismo para desativar temporariamente a autenticação de pré-inicialização (boot);

1.6.15. Deve prover ferramenta presente na estação de trabalho que possibilite migrá-la para um servidor de gerenciamento diferente;

1.6.16. Deve permitir a gerência das seguintes soluções terceiras de criptografia: Microsoft bitlocker e Apple filevault;

1.6.17. Deve permitir a exibição de aviso legal quando o agente de criptografia é instalado na estação de trabalho;

1.6.18. Deve possibilitar que cada política tenha uma chave de criptografia única;

1.6.19. Deve permitir, em nível de política, a escolha da chave de criptografia a ser utilizada, entre as seguintes opções: Chave do usuário: somente o usuário tem acesso aos arquivos; Chave da empresa: qualquer usuário da empresa tem acesso aos arquivos e Chave da política: qualquer estação de trabalho que tenha aplicada a mesma política tem acesso aos arquivos;

Módulo de proteção para smartphones e tablets:

1.7.1. As funcionalidades estarão disponíveis de acordo com cada plataforma;

1.7.2. O módulo de proteção de dispositivos móveis deve possuir aplicativo para os sistemas operacionais iOS e Android;

1.7.3. Deve possuir proteção de antimalware utilizando assinaturas e machine learning;

1.7.4. Deve ser capaz de realizar escaneamento de malwares em tempo real, do cartão sd e após atualização de vacinas;

1.7.5. Deve possuir engine para detecção e bloqueio de ransomware;

1.7.6. Deve realizar scan de aplicações vulneráveis no smartphone;

1.7.7. Deve possuir capacidade de detecção de spam proveniente de SMS;

1.7.8. Deve monitorar a conexão wi-fi e notificar o usuário caso a conexão não seja segura;

1.7.9. Deve permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URL's acessadas;

1.7.10. Deve permitir o controle de acesso a websites por meio de listas de bloqueio e aprovação;

1.7.11. Deve permitir o bloqueio de aplicativos;

1.7.12. Controle da política de segurança de senhas, com critérios mínimos de:

1.7.a. Padrão de senha;

1.7.b. Uso obrigatório de senha; tamanho mínimo;

1.7.c. Tempo de expiração;

1.7.d. Bloqueio automático da tela;

1.7.e. Bloqueio por tentativas inválidas;

1.7.13. Deve verificar se o smartphone está em modo root (Android);

1.7.14. Deve verificar se o smartphone está com jailbreak (iOS);

1.7.15. A proteção para smartphones e tablets deverá identificar aplicativos maliciosos oferecendo sugestões de ações;

1.7.16. A proteção para smartphones e tablets deverá possuir integração nativa com Samsung KNOX;

1.7.17. A proteção para smartphones e tablets deverá possuir integração com VMware WorkSpace One (AirWatch);

Resposta a incidentes de Endpoints

1.8.1. Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos endpoints para a console de correlação centralizada;

1.8.2. Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

1.8.3. A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;

1.8.4. Capacidade de construir sequências de buscas poderosas para localizar os dados ou objetos em seu ambiente que você deseja examinar;

1.8.5. A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;

1.8.6. Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;

1.8.7. Deve ser possível configurar playbooks para resposta automatizada à incidentes;

1.8.8. Deve possuir dahsboard com resumo de incidentes, escopo afetado e severidade do evento;

1.8.9 Deve analisar o ambiente da organização e atribuir sua pontuação de risco;

1.8.10. Deve prover relatórios de inteligência de ameaças avançadas mais recentes e indicadores de comprometimento para ajudar sua organização a se defender proativamente contra ameaças;

1.8.11. Deve integrar relatórios de inteligência criados por especialistas em ameaças do fabricante e terceiros para ajudar na identificação de ameaças;

1.8.12. Deve permitir adicionar no mínimo os seguintes indicativos de comprometimento (IOCs) à base de inteligência:

- Arquivos SHA-1;
- URLs;
- IPs;
- Domínios;

1.8.13. Deve permitir configurar as ações dos indicativos de comprometimento (IOCs) adicionados à console em pelo menos:

- Log;
- Bloquear/Enviar à quarentena;

1.8.14. Deve permitir realizar buscas de objetos para pelo menos os seguintes critérios:

- Comandos CLI executados nas estações de trabalho;
- Nome da estação de trabalho;
- IP;
- Endpoint ID;
- Nome do arquivo;
- Porta;
- URL;
- Arquivo SHA-1;
- Arquivo SHA-2;
- Caminho do arquivo;
- Arquivo MD5;
- Chave de registro do Windows;
- Valor da chave de registro do Windows;
- Técnicas do MITRE;
- Táticas do MITRE;

1.8.15. Deve permitir adicionar arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores;

1.8.16. Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores;

1.8.17. Deve realizar integração com MISP;

1.8.18. Deve suportar TAXII para integração com terceiros;

1.8.19. Deve ter a capacidade de enviar os eventos e detecções para aplicações de SIEM e Syslog terceiros;

1.8.20. A solução deve ser capaz de associar diferentes modelos de ameaças e associá-los a um único incidente/evento;

1.8.21. Deve ter capacidade de apresentar informações relacionadas ao MITRE ATT&CK para cada um dos eventos detectados no ambiente, caso possuam;

1.8.22. A solução deve apresentar uma lista com todos os modelos de detecção pré-definidos que a solução possui;

1.8.23. Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;

1.8.24. Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;

1.8.25. Permitir tomar diferentes ações de resposta no ambiente e monitorar cada ação tomada, com opção de desfazê-la;

1.8.26. A solução deve apresentar uma lista com todos os modelos de detecção pré-definidos que possui;

1.8.27. Cada modelo deve possuir uma descrição e um score para auxiliar na identificação do risco e impacto de cada modelo;

1.8.28. Deve permitir ativar ou desativar qualquer modelo de detecção caso necessário;

1.8.29. Permitir criação de listas de exceção de objetos para redução de falso-positivo.

1.8.30. Os modelos de detecção deverão possuir níveis de severidade (score) individuais para cada modelo em pelo menos os seguintes níveis:

- Crítico;
- Alto;
- Médio;
- Baixo;

1.8.31. Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;

1.8.32. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;

1.8.33. Deve somar as pontuações de cada modelo durante a correlação das atividades para melhor categorização do incidente;

1.8.34. Deve exibir todos os detalhes do incidente em uma única página, contendo no mínimo:

- Status do incidente;
- Score;
- Escopo impactado:
- Quantidade de contas de e-mail impactadas;
- Data e hora da detecção;
- Técnica do MITRE utilizada;
- Modelo(s) de detecção acionado(s);
- Objetos detectados dentro de cada modelo;
- Deve permitir alterar o status de cada evento, para no mínimo:
- Novo;
- Em progresso/análise;
- Fechado;
- Fechado – falso positivo;

ITEM 2 - SOFTWARE, APLICAÇÃO INFORMÁTICA, TIPO ANTIVÍRUS, SOLUÇÃO PARA PROTEÇÃO DE SERVIDORES CONTEMPLANDO 36 MESES DE SUPORTE E GARANTIA, ACOMPANHADA DE TREINAMENTO ON LINE DA EQUIPE DA CONTRATANTE.

Funcionalidades:

2.1. Deve ser totalmente compatível e homologada para gerenciamento de máquinas virtuais nos ambientes Vmware, HyperV, Citrix XenServer, Oracle Cloud e IBM Cloud.

2.2. A solução deverá permitir gerenciar políticas de segurança em múltiplas plataformas e sistemas operacionais, para hosts Físicos, virtuais ou em nuvem (Vcloud, AWS, Microsoft Azure ou Google Cloud), todos em uma única console centralizada e do mesmo fabricante.

2.3. Para cada plataforma de virtualização poderá existir uma forma diferente de integração, com ou sem agente, preservando a capacidade de implementação das funcionalidades.

2.4. Permitir a integração com todas as versões do VMware vCenter a partir da Versão 4.0, de modo a importar e sincronizar os objetos (hosts VMware e Guests VM) para a console de gerenciamento da solução.

2.5. Permitir, no caso de versões anteriores a VMware 6.0, integração com as seguintes API's VMware: VMsafe API; Vshield Endpoint API.

2.6. Suportar a aplicação das funcionalidades de segurança descritas a seguir inclusive para ambientes com versão 6.0 ou superior do vCenter/vSphere, com integração com as novas API's da VMware (NSX).

2.7. Deverá suportar a integração com o vRealize Operations (vROps) da VMware permitindo apresentar os eventos de segurança que ocorrerem nos hosts virtuais protegidos na console do vROps.

2.8. Conter os seguintes módulos de segurança para a proteção de Servidores físicos, virtuais ou em nuvem:

- Reputação Web;
- Firewall;
- Inspeção de Pacotes com virtual Patching (IDS/IPS);
- Monitoramento de Integridade;
- Inspeção de Logs;
- Controle de Aplicações;

2.9. Para hosts gerenciados de Docker container deverá permitir a aplicação de regras de IPS/IDS e proteção contra artefatos maliciosos.

2.10 Permitir a implantação dos módulos de segurança supracitados, no mínimo para os seguintes sistemas operacionais:

1. Windows Server 2012 e Windows Server 2016, 2019 e 2022.
2. Linux, no mínimo para as distribuições: Red Hat, Suse, CentOs, Ubuntu e Debian.

2.11. A solução deverá permitir agrupar os hosts gerenciados em pastas, possibilitando a aplicação de políticas.

2.12. O agrupamento de hosts deverá ser no mínimo pelos seguintes parâmetros:

1. Hostname;
2. Sistema Operacional;
3. Docker Host;
4. Política de Configurações;
5. Active Directory Name/Folder;
6. Range de IP.

2.12. Deverá possuir gerenciamento de todos os eventos relativos aos hosts gerenciados possibilitando, além do armazenamento dos eventos na própria solução, o seu encaminhamento para uma solução de SIEM.

2.14. A solução deverá ter a capacidade de se integrar com os principais softwares de SIEMs de mercado, no mínimo com:

1. Splunk e ArcSight de modo a permitir enviar os seus logs para essas soluções.

2.16. A solução deverá ter a possibilidade de enviar logs para SYSLOG servers.

2.17. A solução deverá suportar o uso de REST API's para permitir a integração com outras aplicações.

2.18. O uso das REST API's deve suportar no mínimo as seguintes funcionalidades:

1. Autenticação – Log in e Log out;
2. Administração de Contas - Criação, edição e exclusão de contas de acesso;
3. Eventos – Acesso à lista de eventos do módulo de Reputação Web;
4. Monitoração de Status- Visualização do status dos hosts gerenciados, incluindo a realização de healthcheks.

2.19. Deverá permitir a criação de maneira personalizada de termos de compromisso para usuários de administração, via console de gerenciamento apresentando a mensagem personalizada ao usuário no momento de login.

2.20. A solução deverá permitir a entrega de agentes por pelo menos duas dentre as principais ferramentas de distribuição de software do mercado: no mínimo para Microsoft System Center Configuration Manager e Puppet.

2.21. A solução deverá efetuar a proteção contra códigos maliciosos através da instalação ou não de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça.

2.22. A solução deverá suportar a análise de comportamento (Behavior Monitoring) para a detecção avançada de ameaças.

2.23. A funcionalidade de análise de comportamento deverá permitir o bloqueio de atividades suspeita de criptografia de arquivos visando impedir a propagação de ameaças do tipo ransomware.

2.24. A funcionalidade de análise de comportamento deverá permitir o backup de arquivos que estiverem sendo criptografados, fazendo a restauração dos mesmos em caso de bloqueio do processo de criptografia.

2.25. A solução deverá incluir técnicas de Inteligência artificial baseada em algoritmos de Machine Learning para análise preditiva de ameaças.

2.26. Deve ser capaz de executar rastreamento nos hosts e fornecer lista de todas as recomendações de segurança para os softwares que estiverem instalados nesse host, bem como do sistema operacional.

2.27. Proteger de forma automática e transparente contra brechas de segurança descobertas, interrompendo somente o tráfego de rede malicioso.

2.28. Operar como firewall de host stateful bidirecional, monitorando as comunicações nos servidores protegidos.

2.29. Possuir a capacidade de controlar o tráfego baseado no endereço MAC, frame types, tipos de protocolos, endereços IP e intervalo de portas.

2.30. Possuir a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador.

2.31. Permitir que regras de Firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não).

2.32. Permitir que as regras de Firewall executem as seguintes ações, ou equivalentes: Allow, Log Only, by-pass, force allow, deny.

2.33. Permitir realizar pseudo stateful em tráfego UDP.

2.34. Permitir limitar o número de conexões entrantes e de saída de um determinado IP de origem.

2.35. Permitir a criação de novas regras utilizando templates padrão.

2.36. Permitir atuar no modo em linha para bloqueio de ataques ou modo escuta para monitoração e alertas.

2.37. Possuir a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do sistema operacional e demais aplicações.

2.38. Possuir a capacidade de varrer o servidor protegido detectando o tipo e versão do sistema operacional e as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindam vulnerabilidades existentes no sistema operacional e aplicações (patch virtual).

2.39. Permitir execução de varreduras sob demanda ou agendada.

2.40. Possuir a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão.

2.41. Permitir que a opção de detecção e bloqueio seja implementada de forma global (todas as regras) ou apenas para uma regra ou grupos de regras.

2.42. Conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem, no mínimo, os seguintes sistemas operacionais e aplicações:

- Windows Server 2012 e Windows Server 2016, 2019 e 2022.
- Linux Red Hat, Suse, CentOS e Debian;
- Aplicações padrão de mercado, tais como: Microsoft IIS, SQL Server, Microsoft Exchange, Microsoft Office, Red hat Oracle Database, PostgreSQL, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome, Edge e Web Server Apache, Jboss, Wordpress, PHP, Joomla, Jenkins.

Funcionalidades de Gerenciamento:

2.43. Permitir o envio de notificações via SMTP;

2.44 Permitir o envio de registros de logs a um servidor remoto;

2.45. Implementar gravação de eventos de auditoria envolvendo todos os eventos e ações realizadas na console de gerenciamento;

2.46. Permitir que a distribuição de atualizações e novos componentes possa ser efetuada por replicadores espalhados pelo ambiente;

2.47. Permitir a criação de múltiplos perfis de segurança, que serão vinculados aos diferentes tipos de servidores do ambiente;

2.48 Permitir a criação de relatórios, sob demanda, ou agendados, com o envio automático via e-mail, no formato PDF;

2.49 Armazenar políticas e logs em base de dados, suportando, no mínimo, bancos de dados:

- PostgreSQL, Microsoft SQL Server e Oracle Database;

2.50. Permitir a definição de permissionamento, no mínimo, para os modos de visualização e edição de políticas;

2.51. Permitir a atribuição granular de permissões para servidores gerenciados, podendo delimitar quais os servidores que podem ser visualizados e gerenciados para cada usuário ou grupo de usuários;

2.52. Possuir dashboards para facilidade de monitoração, as quais poderão ser customizados pelo usuário;

2.53. Possuir a capacidade de criar políticas de forma global para todas as máquinas virtuais, por perfis e individualmente para cada host;

2.54. Permitir a criação/utilização de tags pré-definidas para o agrupamento e aplicação de políticas aos hosts segundo características comuns;

2.55. Permitir o envio de eventos da console via SNMP;

2.56. Permitir o rollback de atualização de regras pela console de gerenciamento;

2.57. Gerar pacote de autodiagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;

2.58. Possuir a capacidade de marcar eventos (tags) de modo a facilitar o gerenciamento, relatórios e visualização;

2.59. Possuir a capacidade de classificar eventos para facilitar a identificação e a visualização de eventos críticos em servidores críticos.

Serviço de Suporte, garantia e atualização
• A Contratada deverá prover garantia, suporte técnico, e atualização de versões das licenças fornecidas, pelo prazo de trinta meses, contados da data do recebimento definitivo dessas licenças; • O serviço inclui a instalação inicial das licenças contratadas e entrega do ambiente em efetivo funcionamento, para emissão do recebimento definitivo pelo Contratante; • Inclui todas as atualizações de versões, pequenas atualizações de release e reparos de defeitos (bug fixing patches); • Os serviços de suporte técnico aos produtos deverão incluir, dentre outros: • Orientações sobre uso, configuração e instalação do software ofertado; • Questões sobre compatibilidade e interoperabilidade do produto ofertado (hardware e software); • Interpretação da documentação do software ofertado; • Orientações para identificar a causa de uma falha de software; • Orientação para solução de problemas de “performance” e “tuning” das configurações do software ofertado; • Orientação quanto às melhores práticas para implementação do software adquirido; • Apoio na recuperação de ambientes em caso de panes ou perda de dados; • Apoio para execução de procedimentos de atualização para novas versões do software instalado;

- A contratada deverá gerar relatório mensal, analítico e sintético, indicando todos os eventos relevantes ocorridos durante o período de execução do mesmo a ser entregue até o 5 (quinto) dia útil do mês subsequente.
- Durante o período de garantia, suporte técnico e manutenção, a Contratada deverá atender às solicitações do Ministério, em qualquer horário, respeitando as condições e níveis de serviços especificados a seguir:

  a) SEVERIDADE ALTA: Aplicado quando há indisponibilidade do ambiente tecnológico;

  b) SEVERIDADE MÉDIA: Aplicado quando há falha no uso dos softwares, estando ainda disponíveis, porém apresentando problemas ou instabilidade;

  c) SEVERIDADE BAIXA: Aplicado para instalação, configuração, manutenção preventivas, aplicações de atualização e esclarecimento técnico relativo ao uso das ferramentas.

- Os prazos estabelecidos nos níveis de serviços serão contados a partir da abertura do chamado, o qual será classificado conforme as severidades especificadas no item anterior.
- Os prazos máximos para o atendimento dos chamados obedecerão ao disposto na tabela a seguir, contados a partir da data e hora de abertura do chamado:

Severidade	Atendimento	Solução definitiva
Alta	2 (duas) horas	4 (quatro) horas
Média	4 (quatro) horas	12 horas
Baixa	12 (doze) horas	24 (vinte e quatro) horas

Para os chamados de severidade ALTA (paralisação de pelo menos 1 (uma) das funcionalidades elencadas nas especificações técnicas), o início do atendimento deverá ocorrer no máximo em 2 (duas) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 4 (quatro) horas corridas a contar do início do atendimento.

Para os chamados severidade MÉDIA (degradação na performance, funcionamento ou serviço da solução), o início do atendimento deverá ocorrer no máximo em 4 (quatro) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 12 (doze) horas corridas a contar do início do atendimento.

Para os chamados severidade BAIXA (quando há comprometimento do desempenho), o início do atendimento deverá ocorrer no máximo em 12 (doze) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 24 (vinte e quatro) horas corridas a contar do início do atendimento.

Para os chamados de qualquer severidade, a critério da universidade, poderá ser agendado o melhor horário para atendimento.

O fechamento de qualquer chamado só poderá ocorrer mediante consulta prévia à universidade quanto à efetiva solução do problema.

Qualquer chamado fechado, sem anuência da universidade ou sem que o problema tenha sido resolvido, será reaberto e os prazos serão contados a partir da abertura original do chamado, inclusive para efeito de aplicação das sanções previstas.

A Contratada manterá cadastro das pessoas indicadas pela universidade que poderão efetuar abertura e autorizar o fechamento de chamados.

Ao término de atendimentos relacionados à assistência técnica da garantia, a Contratada deverá apresentar Relatório de Atendimento contendo data e hora da abertura do chamado, data e hora do início e do término do atendimento, identificação do defeito, nome do técnico responsável pela execução da garantia, providências adotadas e outras informações pertinentes. O Relatório deverá ser assinado por técnico da universidade.

O atendimento deve ser efetuado em língua portuguesa.

A Contratada deverá fornecer relatório de atendimento técnico, referente a cada chamado, contendo no mínimo as seguintes informações:

a) Data e hora da abertura do chamado;

b) Data e hora do início do atendimento;

c) Responsável pelo atendimento da solicitação;

d) Motivo da ocorrência (indicação do defeito);

e) Status do chamado (aberto, em tratamento, fechado, etc.);

f) Data e hora do fechamento do chamado;

g) Solução adotada (resolução).

O atendimento de suporte para a solução deverá ser do tipo 24 x 7 (vinte e quatro horas por dia, sete dias por semana), e deverá ser realizado por profissionais especializados.

Não haverá limite para o número de chamados de suporte técnico.

Nos casos em que as manutenções necessitarem de paradas do ambiente, a universidade deverá ser imediatamente notificada para que se proceda a aprovação da manutenção, ou para que seja agendada nova data, a ser definida pelo Contratante, para execução das atividades de manutenção.

1.1.2. À forma de cálculo do quantitativo dos itens desta licitação consta descrita no item 7 do Estudo Técnico Preliminar desta contratação.

1.1.3. **Caso ocorra alguma divergência entre as especificações técnicas constantes na tabela com aquelas lançadas no sistema eletrônico (Comprasnet), prevalecerá o constante neste instrumento.**

1.2. **O prazo de vigência da contratação é de 36 (trinta e seis) meses,** conforme vier a constar do (s) contrato (s) ou instrumento substituto (se for o caso).

1.3. **Compartilham desta licitação através da IRP 001/2023:**

1.3.1. Instituto Federal de Mato Grosso/Campus Novo do Parecis, UASG 158492.

1.3.2. Instituto Federal de Educação, Ciência e Tecnologia Goiano, UASG 158124.

1.3.3. Instituto Federal de Mato Grosso/Campus Barra do Garças, UASG 158497.

1.3.4. Instituto Federal de Mato Grosso/Campus Cuiabá Octayde Jorge da Silva, UASG 158333.

1.3.5. Instituto Federal de Educação, Ciência e Tecnologia de Goiás, UASG 158153.

1.3.6. Instituto Federal de Educação, Ciência e Tecnologia do Mato Grosso do Sul, UASG 158132.

1.3.7. Instituto Federal de Educação, Ciência e Tecnologia do Mato Grosso/Campus Tangará da Serra, UASG 158144.

2. JUSTIFICATIVA E OBJETIVO DA AQUISIÇÃO DOS ITENS DA SOLUÇÃO DE TIC

2.1. A Universidade Federal de Goiás (UFG) necessita adquirir os equipamentos constantes da **Tabela 1**, pois os mesmos são importantes para oferecer a infraestrutura necessária para que o trabalho administrativo possa ser desempenhado com mais qualidade e eficiência. Esses equipamentos também contribuem para propiciar o desenvolvimento satisfatório das atividades acadêmicas e o melhor uso e aproveitamento dos recursos tecnológicos já existentes, evitando assim o desperdício de recursos e otimizando a oferta de um dos melhores serviços da universidade: geração de conhecimento de qualidade para a comunidade universitária e toda sociedade. Integram a presente justificativa os tópicos 2, 7, 14, 15, 18.1 do Estudo Técnico Preliminar desta Contratação, documento SEI nº 3985861.

2.2. Contribui-se assim, para garantir qualidade de ensino e pesquisa nessa Instituição, que sempre se pautou por maior agilidade, qualidade e inovação técnica, didática e assistência à toda população no seu cotidiano, visando resultados com a melhoria da formação acadêmica dos profissionais que dela se utilizam.

2.3. O registro de preços visa atender à dificuldade de prever, com exatidão, as quantidades que serão consumidas ao longo de 12 (doze) meses. Ainda corrobora para a realização das aquisições através dos preços registrados a permissão legal constante dos incisos I e IV, do art. 3°, do Decreto 7.892, de 23 de janeiro de 2013, quais sejam:

> Art. 3º - O Sistema de Registro de Preços – SRP poderá ser adotado nas seguintes hipóteses:
> I - quando, pelas características do bem ou Material, houver necessidade de contratações frequentes;
> (...)
> IV – quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração. grifos nossos

2.4. A presente licitação está alinhada com os instrumentos de planejamento elencados no art. 6º da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019 a saber:

2.5. A solução de TIC , objeto da presente licitação está alinhada com PAC 2022/2023 - Plano Anual de Contratações da Universidade Federal de Goiás e suas alterações.

2.6. A aquisição da solução de TIC está em consonância com o Planejamento de Tecnologia da Informação desta instituição.

2.7. presente aquisição também guarda alinhamento à Estratégia de Governo Digital (EGD) para o período de 2020 a 2022, instituída pelo Decreto n° 10.332, de 28 de Abril de 2020, no tocante ao **Objetivo Estratégico 16**, qual seja: *Otimização das infraestruturas de tecnologia da informação*. Para alcance deste objetivo estratégico, a EGD enuncia como iniciativa (**Iniciativa n° 16.1)** a realizar, no mínimo, seis compras centralizadas de bens e serviços comuns de tecnologia da informação e comunicação, até 2022.

2.8. A relação entre a necessidade da contratação da solução de TIC e os respectivos volumes e características do objeto constam do Estudo Técnico Preliminar, Apêndice deste Termo de Referência e Anexo ao Edital da Licitação.

3. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

3.1. **Requisitos de Negócio:**

3.1.1. Os requisitos de negócio estão materializados na própria descrição de cada item deste certame, constantes da Tabela 1 e 2, no item 1.1.1. deste termo de referência.

3.1.2. A especificação dos itens deste procedimento licitatório observou regras e princípios de manutenção da padronização do parque computacional adotado na UFG, assim como compatibilidade e desempenho com a solução já existente, visando à ampliação, renovação e continuidade da tecnologia.

3.2. **Requisitos Legais:**

3.2.1. Os requisitos legais para a contratação constam nos itens 2.3 a 2.7 deste termo de referência. Acrescenta-se a esses requisitos o processamento desta licitação com aplicação do Decreto 7.174/2010 e da Instrução Normativa SGD nº 01/2019. Também são requisitos legais o arcabouço legal relativo a legislação de licitações e contratos que constar do preâmbulo do Edital.

3.2.1.1. Os fornecedores deverão apresentar juntamente com a proposta de preços Documento expedido pelo Ministério da Ciência e Tecnologia ou pela SUFRAMA, que comprove o atendimento do Processo Produtivo Básico. Poderá ser emitido eletronicamente, por meio de consulta ao sítio eletrônico oficial do Ministério da Ciência e Tecnologia ou da Superintendência da Zona Franca de Manaus – SUFRAMA nos termos do art. 7º § único do Decreto 7.174/2010, caso venham a optar por exercer o Direito de Preferência.

3.3. **Requisitos Temporais:**

3.3.1. As compras dos itens objeto desta licitação serão feitas durante o prazo de vigência da ata de registro de preços, por se tratar de licitação, na modalidade pregão em sua forma eletrônica, que será processada pelo sistema de registro de preços, regulamentado pelo Decreto 7.892/2013.

3.4. **Requisitos Sociais, Ambientais e Culturais**

3.4.1. Para participar deste procedimento licitatório, os fornecedores deverão apresentar juntamente com a proposta de preços documento que comprove a **Certificação de sustentabilidade ambiental** emitida por instituição pública oficial ou instituição credenciada comprovando que a

empresa proponente pratica ações sustentáveis que colaborem para a preservação do Meio Ambiente, consoante artigos artigos 5º e 6º da IN Nº 1 – SLTI/MPOG, de 19 de janeiro de 2010 **ou** esgotada a possibilidade de atendimento de tal exigência, a certificação poderá ser feita mediante **Declaração de Sustentabilidade Ambiental emitida pela própria empresa licitante** declarando que ela (proponente) atende às exigências constantes da IN Nº 1/2010 – SLTI/MPOG.

3.5. **Requisitos de Garantia e Manutenção:**

3.5.1. Conforme detalhes constantes do Estudo Técnico Preliminar, Apêndice I deste Termo de Referência, os fornecedores participantes deste certame deverão ofertar em suas propostas **Garantia ON-SITE** com prazo de garantia não inferior a **36 (trinta e seis) meses** para todos os itens desta licitação.

3.5.2. O prazo de garantia para os itens deverá constar da proposta de preços dos fornecedores e será contado a partir da emissão do Termo de Recebimento Definitivo, relativo a cada aquisição efetuada pela Universidade.

3.5.3. Da proposta de preços dos fornecedores deverão constar os telefones, e-mail, site ou outro canal para o acionamento da garantia dos bens.

3.5.4. A Garantia ON-SITE dos bens ofertada deverá cobrir custos de manutenção e de substituição dos bens, se for o caso.

4. DESCRIÇÃO DA SOLUÇÃO

4.1. A descrição da solução como um todo, encontra-se pormenorizada em Tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência, e encontra-se materializada no documento SEI º 3985861.

5. CLASSIFICAÇÃO DOS BENS COMUNS

5.1. O objeto a ser adquirido foi definido como bens comuns nos termos do parágrafo único, do art. 1°, da Lei 10.520, de 2002.

6. CRITÉRIOS DE SUSTENTABILIDADE

6.1. *Acerca do objeto a ser contratado, não é exigido qualquer requisito ambiental na especificação do objeto, conforme o entendimento do Decreto n. 7.746/12, além da Lei 12.305/10 – Política Nacional de Resíduos Sólidos, assim como, a Instrução Normativa SLTI/MPOG n. 1, de 19/01/10.*

7. MODELO DE EXECUÇÃO E GESTÃO DA CONTRATAÇÃO, ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO

7.1. A ativação e execução dos itens ocorrerá no seguinte prazo de 15 (quinze) dias e deverá ocorrer da seguinte forma: conforme descritos no subitem 1.1.1. (Serviço de Suporte, garantia e atualização), coincidindo o início da execução dos serviços com a data inicial vigência do (s) contrato (s).

Locais para prestação dos serviços:

I - **UNIVERSIDADE FEDERAL DE GOIÁS: Centro de Recursos Computacionais – CERCOMP/UFG,** localizado na Av. Esperança (Alameda Flamboyant) Campus II – Samambaia (saída para Nova Veneza-Go, próximo à Casa do Estudante Universitário), Goiânia – Goiás, CEP: 74.690-900. Telefones (62) 3521-1079, e-mails: comprasti.cercomp@ufg.br. Horário de entrega: Segunda a sexta-feira, em horário comercial (08h00-17h00).

II - **INSTITUTO FEDERAL DE MATO GROSSO/CAMPUS CAMPO NOVO DO PARECIS:** Rodovia MT 235, KM 12, Zona Rural, CEP 78.360-000, Caixa Postal 100, Campo Novo do Parecis - MT. Responsável pelo recebimento: Marcos Aurélio Vargas, Técnico de Tecnologia da Informação, (65) 3382-6219 e/ou Rafael Rodrigues Marquesi (65)3382-6219, Analista de Tecnologia da Informação, cti.cnp@ifmt.edu.br. Horário de entrega: Segunda a sexta-feira - 07h00-12h00 e 13h00-16h00.

III - **INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO - GOIÂNIA-GO:** Rua 88, 310, Setor Sul, Goiânia – GO. CEP: 74.085-010; Telefone:.62) 3605-3610, responsável Fernando Pirkel Tsukahara; fernando.tsukahara@ifgoiano.edu.br. Horário de entrega: Segunda a sexta-feira em horário comercial.

IV - **INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MATO GROSSO/CAMPUS BARRA DO GARÇAS**: Estrada de Acesso a BR-158, Rua José Maurício Zampa, S/N, Loteamento BR-070, Barra do Garças-MT, CEP: 78.605-099. Responsável pelo recebimento: Ednaldo dos Santos Batista Miranda, Técnico de Tecnologia da Informação, ednaldo.miranda@ifmt.edu.br, cti.bag@ifmt.edu.br. Telefone: (66) 3402-0116. Horário de entrega: Segunda a sexta-feira - 08h00-12h00 e 14h00-18h00.

V - **INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MATO GROSSO/CAMPUS CUIABÁ OCTAYDE JORGE DA SILVA:** Rua Professora Zulmira Canavarros, 95 Cuiabá - MT - CEP 78.005-200. Horário de entrega: Segunda a sexta-feira - 08h00-17h00 (horário local). Telefone: (65) 3318-1403.

VI - **INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE GOIÁS :** Avenida C-198, nº 500, Setor Jardim América – GO. CEP: 74.270-040. Responsável pelo recebimento: Leandro Alexandre Freitas, Diretor de Tecnologia da Informação. Horário de Entrega: Segunda a sexta-feira - 08h00-18h00.

VII - **INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO MATO GROSSO DO SUL**: Rua Jorn. Belizário Lima, 236, Vila Glória - Campo Grande/MS - CEP: 79.004-270. Responsável pelo recebimento: Matheus Jardim Guerreiro da Silva, Coordenador de Infraestrutura, Redes e Telecomunicações, e-mail: matheus.silva@ifms.edu.br. Telefone: (67) 3378-9566. Horário de entrega: Segunda a sexta-feira - 08h00 - 17h00.

VIII - **INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MATO GROSSO/CAMPUS TANGARÁ DA SERRA:** Rua José de Oliveira, 980 - N, Jardim Horizonte. Tangará da Serra - MT. CEP 78.302-116. Telefone (65) 3311-8500. E-mail: administracao.tga@ifmt.edu.br. Responsável pelo recebimento: Magno Lopes Ribeiro, Professor EBTT - Área Informática, Chefe do Departamento de Ensino, e-mail: ensino.tga@ifmt.edu.br. Horário de recebimento: Segunda a sexta-feira - 07h00-11h00 e 13h00-17h00.

7.1.1. O prazo de entrega poderá ser dilatado a critério da autoridade competente da Universidade e mediante pedido escrito e fundamentado da Contratada.

7.2. Os bens serão recebidos provisoriamente no prazo de até 15 (quinze) dias, pelo(a)servidor ou Equipe de servidores, conforme o caso, responsável (veis) pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.

7.3. Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 10 (dez) dias corridos, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

7.4. Os bens serão recebidos definitivamente no prazo de 07 (sete) dias**,** contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo circunstanciado.

7.5. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

7.6. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do contrato.

7.7. Durante a validade da contratação a empresa contratada não poderá alegar a indisponibilidade dos produtos ofertados, sob pena de lhe ser aplicadas as sanções previstas no edital.

7.7.1. Se no ato da entrega dos produtos a Nota Fiscal de Venda não for aceita pela Contratante devido a alguma divergência/irregularidade(s) em seu preenchimento, esta será devolvida para as necessárias correções, passando a contar o prazo de pagamento a partir da data de sua reapresentação.

7.7.2. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do contrato.

7.7.3. Os produtos deverão ser entregues devidamente acondicionados em suas embalagens originais e em perfeitas condições de uso, de forma a permitir completa segurança por parte da Contratante, sob pena do não recebimento definitivo dos mesmos.

Dados para emissão da Nota Fiscal de Serviços

Nome: ..... **UNIVERSIDADE FEDERAL DE GOIÁS**

Endereço: ..... Campus II – Samambaia, Goiânia – GO.

CEP: 74.690-900

CNPJ: 01.567.601/0001-43

Inscrição Estadual: .. Não se palica

Fone:..... (62)3521-1020

Nome: ..... **INSTITUTO FEDERAL DE MATO GROSSO/CAMPUS CAMPO NOVO DO PARECIS**

Endereço: ..... Rodovia MT 235, KM 12, Zona Rural, Campo Novo do Parecis - MT.

CEP: 78.360-000

CNPJ: 10.784.782/0011-22

Inscrição Estadual: .. Não se aplica

Fone:.....(65) 3382-6219

Nome: ..... **INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA GOIANO - GOIÂNIA-GO**

Endereço: ..... Rua 88, 310, Setor Sul, Goiânia – GO.

CEP: 74.085-010

CNPJ: 10.651.417/0001-78

Inscrição Estadual: .. Não se aplica

Fone:.....(62) 3605-3610

Nome: ..... **INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MATO GROSSO/CAMPUS BARRA DO GARÇAS**

Endereço: ..... Estrada de Acesso a BR-158, Rua José Maurício Zampa, S/N, Loteamento BR-070, Barra do Garças-MT

CEP: 78.605-099

CNPJ: 10.784.782/0008-27

Inscrição Estadual: .. Não se aplica

Fone:..... (66) 3402-0116

Nome: ..... **INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MATO GROSSO/CAMPUS CUIABÁ OCTAYDE JORGE DA SILVA**

Endereço: ..... Rua Professora Zulmira Canavarros, 95 Cuiabá - MT

CEP: 78.005-200

CNPJ: 10.784.782/0002-31

Inscrição Estadual: .. Não se aplica

Fone:..... (65) 3318-1403

Nome: ..... **INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE GOIÁS**

Endereço: ..... Avenida C-198, nº 500, Setor Jardim América – GO

CEP: 74.270-040

CNPJ: 10.870.883/0001-40

Inscrição Estadual: .. Não se aplica

Fone:..... (62)3612-2227

Nome: .....INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO MATO GROSSO DO SUL

Endereço: ..... Rua Jorn. Belizário Lima, 236, Vila Glória - Campo Grande/MS

CEP: 79.004-270

CNPJ: 10.673.078/0001-20

Inscrição Estadual: .. Não se aplica

Fone:..... (67) 3378-9566

Nome: ..... **INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE MATO GROSSO/CAMPUS TANGARÁ DA SERRA**

Endereço: ..... Rua José de Oliveira, 980 - N, Jardim Horizonte. Tangará da Serra - MT

CEP: 78.302-116

CNPJ: 10.784.782/0001-50

Inscrição Estadual: .. Não se aplica

Fone:.....(65)3311-8500

7.7.4. Para agilizar o processo de pagamento, devem ser informados na Nota Fiscal de Venda os dados bancários da Contratada (se possível).

7.8. As situações e a forma que serão aplicadas as sanções á Contratada (s), assegurados o contraditório e a ampla defesa, contam do item denominado: " DAS SANÇÕES ADMINISTRATIVAS, deste termo de referência.

7.9. Em todo processo de aplicação de sanção será observado pela Contratante a proporcionalidade das sanções previstas ao grau do prejuízo causado pelo descumprimento, observadas as faixas para multas e os gêneros de penalidades descritos no item: " SANÇÕES ADMINISTRATIVAS, deste termo de referência.

7.10. **A gestão do presente processo de contratação será executada no que couber com observância pelas áreas competentes das seções III e IV da Instrução Normativa da Secretaria de Governo Digital do Ministério da Economia nº 01/2019 e suas alterações.**

8. DAS OBRIGAÇÕES DA CONTRATANTE

8.1. São obrigações da Contratante:

8.1.1. Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;

8.1.2. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;

8.1.3. Comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

8.1.4. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado;

8.1.5. Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos;

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

8.2.1. Rejeitar os produtos em que as características, qualidade não satisfaçam às exigências contratadas, que sejam impróprias ou diferentes/inferiores daquelas exigidas neste instrumento e respectivo edital, obrigando a adjudicatária a substituir ou se adequar, sem ônus para a UFG e no prazo de 05 (cinco) dias úteis.

8.2.2. Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento (d**ocumento que pode ser confeccionado pela Contratante no corpo do e-mail que encaminhar o contrato a nota de empenho ou instrumento substituto à Contratada**), de acordo com critérios definidos neste termo de referência, observando-se o disposto nos item 7, no item 9, no item 14 e seus subitens.

8.2.3. **Gerir e fiscalizar a contratação no que couber com observância pelas áreas competentes das seções III e IV da Instrução Normativa da Secretaria de Governo Digital do Ministério da Economia nº 01/2019 e suas alterações.**

9. OBRIGAÇÕES DA CONTRATADA

9.1. A Contratada deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto.

9.1.1. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes neste instrumento, edital e anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade;

9.1.1.1. O objeto deve estar acompanhado do manual do usuário, com uma versão em português e da relação da rede de assistência técnica autorizada;

9.1.2. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do código de defesa do consumidor (Lei nº 8.078, de 1990);

9.1.3. Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste termo de referência, o objeto com avarias ou defeitos;

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

9.1.5. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

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

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

9.1.8. 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;

9.1.9. 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, sempre que considerar a medida necessária;

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

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

9.1.12. manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

10. OBRIGAÇÕES DO ÓRGÃO GERENCIADOR E DOS ÓRGÃOS NÃO PARTICIPANTES

10.1. As regras e obrigações, referentes aos órgãos gerenciador, órgãos participantes e não participantes da licitação, bem como a eventuais adesões são as que constam da minuta de Ata de Registro de Preços , em anexo específico do Edital do Pregão Eletrônico 070/2022.

10.2. A Ata de Registro de Preços é regida pelo Decreto 7.892, de 23 de Janeiro de 2013 e suas disposições são aplicáveis integralmente a esta contratação.

10.3. São obrigações da Universidade Federal de Goiás, como órgão gerenciador do registro de preços, além do disposto no Decreto nº 7.892, de 2013, e atualizações:

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

b) conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;

c) definir a produtividade ou da capacidade mínima de fornecimento da solução de TIC;

d) definir as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a realização de testes em amostras do (s) item (s), observado o disposto no inciso III, alínea "c", item 2 do Artigo 17 da Instrução Normativa SGD nº 01/2019, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

11. DA SUBCONTRATAÇÃO

11.1. Não será admitida a subcontratação do objeto licitatório.

12. ALTERAÇÃO SUBJETIVA

12.1. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

13. DO CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

13.1. Nos termos do art. 67 Lei nº 8.666, de 1993, será designado representante para acompanhar e fiscalizar a entrega dos bens, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

13.1.1. O recebimento de material de valor superior a R$ 176.000,00 (cento e setenta e seis mil reais) será confiado a uma comissão de, no mínimo, 3 (três) membros, designados pela autoridade competente.

13.2. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

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

14. DO PAGAMENTO

14.1. O pagamento será realizado no prazo máximo de até 30 (trinta) dias, contados a partir do recebimento da Nota Fiscal ou Fatura, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

14.1.1. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

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

14.3. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta online ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

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

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

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

14.6. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

14.7. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, 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 da contratante.

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

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

14.10. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

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

14.12. Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por movo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.

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

14.13.1. A Contratada 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.

14.14. Os pagamentos serão realizados somente via ordem bancária e, de acordo com a tramitação formal, não sendo reconhecidos quaisquer outros tipos de documentos de cobrança, tais como duplicatas, boletos e/ou outros tipos de títulos. A responsabilidade pela baixa de qualquer cobrança apontada em cartórios de tulos e protestos ou equivalentes, será de total responsabilidade da Contratada.

14.14.1. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

I=(TX/100) / 365

EM = I x N x VP, sendo:

I = índice de atualização financeira;

TX= Percentual de taxa de juros de mora anual;

EM=Encargos moratórios;

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

VP = Valor da parcela a ser paga.

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

I = (TX)	I = (6/100) / 365	I = 0,00016438 TX = Percentual da taxa anual = 6%.

15. DO REAJUSTE

15.1. Os preços são fixos e irreajustáveis, nos termos do Parecer nº 00001/2016/CPLCA/CGU/AGU não cabe reajuste, repactuação ou reequilíbrio econômico em relação à Ata de Registro de Preços, uma vez que esses institutos estão relacionados à contratação (contrato administrativo em sentido amplo).

15.2. Os critérios de revisão e cancelamento são os que constam da minuta da Ata de Registro de Preços.

16. A GARANTIA DA EXECUÇÃO

16.1. Não haverá exigência de garantia de execução contratual da execução, tendo em vista que as aquisições decorrentes desta licitação estarão cobertas por garantia contratual ONSITE, adicional a garantia legal, conforme detalhado no tópico denominado Requisitos da Garantia e Manutenção, e ainda conforme disposto no item 17 e seus subitens, deste expediente.

17. DA GARANTIA CONTRATUAL DOS BENS

17.0.1. O prazo de garantia contratual on site dos bens, complementar à garantia legal para os itens, será de, no mínimo, 36 (trinta e seis) meses , contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

17.0.2. Caso o prazo da garantia oferecida pelo fabricante seja inferior ao estabelecido nesta cláusula, o licitante deverá complementar a garantia do bem ofertado pelo período restante.

17.0.3. **Os licitantes que participarem desta licitação deverão obrigatoriamente fazer constar de suas propostas de preços o prazo da garantia on-site para todos os itens desta contratação e ainda telefone, e-mail ou outro canal para acionamento da garantia legal e contratual dos bens.**

17.0.4. A garantia será prestada com vistas a manter os softwares fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o Contratante.

17.1. A garantia abrange a realização da manutenção corretiva dos bens pela própria Contratada, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

17.2. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, a realização de ajustes, reparos e correções necessárias.

17.3. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.

17.4. Uma vez notificada, a Contratada realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até 10 (dez) dias corridos, contados a partir da data de retirada do equipamento das dependências da Administração pela Contratada ou pela assistência técnica autorizada.

17.5. O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada da Contratada, aceita pelo Contratante.

17.6. Uma vez notificada a contratada promoverá a restauração do serviço em no máximo 04 (quatro) horas, prorrogáveis a pedido da Contratada (s) mediante justificativa e pedido escrito, a critério da Contratante.

17.7. Na hipótese do subitem acima, a Contratada deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pelo Contratante, de modo a garantir a continuidade dos trabalhos administrativos durante a execução dos reparos.

17.8. Decorrido o prazo para reparos e substituições sem o atendimento da solicitação do Contratante ou a apresentação de justificativas pela Contratada, fica o Contratante autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir da Contratada o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos.

17.9. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade da Contratada.

17.10. A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato ou instrumento substituto, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

18. DAS SANÇÕES ADMINISTRATIVAS

18.1. Comete infração administrativa nos termos da Lei nº 10.520, de 2002, a CONTRATADA que:

18.1.1. Inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

18.1.2. Ensejar o retardamento da execução do objeto;

18.1.3. Falhar ou fraudar na execução do contrato;

18.1.4. Comportar-se de modo inidôneo; e

18.1.5. Cometer fraude fiscal.

18.2. Pela inexecução total ou parcial do objeto da contratação a Administração pode aplicar à CONTRATADA as seguintes sanções:

18.2.1. Advertência, por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;

18.2.2. Multa moratória de 0,5% (meio por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida (valor da contratação /empenho), até o limite de 30 (trinta) dias corridos.

18.2.3. **Multa compensatória variando de 10% (dez por cento) até 30% (dez por cento) sobre o valor total da contratação (empenho), no caso de inexecução total do objeto da contratação (valor empenhado);**

18.2.4. Em caso de inexecução parcial, a multa compensatória, **considerando a faixa percentual** do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;

18.2.5. **Suspensão de licitar e impedimento de contratar** com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

18.2.6. **Impedimento de licitar e contratar** com a União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

18.2.7. A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa deste Termo de Referência.

18.2.8. **Declaração de inidoneidade** para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

18.3. As sanções previstas nos subitens acima poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

18.4. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

18.4.1. Tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

18.4.2. Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

18.4.3. Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

18.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

18.6. As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

18.6.1. Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 10 (dez) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

18.7. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

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

18.9. Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização - PAR.

18.10. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

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

18.12. As penalidades serão obrigatoriamente registradas no SICAF.

19. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

19.1. As exigências de habilitação jurídica e de regularidade fiscal e trabalhista são as usuais para a generalidade dos objetos, conforme disciplinado no edital.

19.2. Os critérios de qualificação econômica a serem atendidos pelo fornecedor estão previstos no edital.

19.3. Os critérios de qualificação técnica a serem atendidos pelo fornecedor serão:

19.3.1. **Comprovação de aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta licitação mediante a apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.**

19.3.1.1. Para fins da comprovação de que trata este subitem, **considerando as disposições do Acórdão TCU 914/2019, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas: comprovar o fornecimento de no mínimo 20% (vinte por cento) do quantitativo total para cada item desta licitação, que vier a participar.**

19.3.1.2. Se da aplicação do percentual referido no subitem anterior, resultar em número decimal, deverá ser efetuado o arredondamento para o próximo número inteiro.

19.4. **O critério de aceitabilidade de preços é o menor preço unitário por item.**

19.5. **O Fornecedor deverá encaminhar um documento comprovando ponto a ponto a aderência da solução ofertada a cada item do termo de referência, descritos no subitem 1.1.1. - Tabela 2, constando no mínimo: objeto, item do termo de referência do objeto, descrição da solução do produto ofertado que atende ao item, documento comprobatório ou URL, página documento referenciado associado ao requisito do item, como segue modelo do Anexo I.**

20. ESTIMATIVA DE PREÇOS E PREÇOS REFERENCIAIS

20.1. O valor unitário para cada item e o valor total estimados constam descritos na Tabela 1 deste Termo de Referência.

21. DOS RECURSOS ORÇAMENTÁRIOS

21.1. Por se tratar de licitação processada pelo sistema de registro de preços, tendo em vista as prerrogativas constantes no art. 7º, §2º do Decreto 7.892/2013, a dotação orçamentária será juntada aos autos previamente a emissão de empenho relativa a cada compra que ocorrer, durante a vigência da ata de registo de preços.

22. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

22.1. As despesas para atender a esta licitação estão programadas em dotação orçamentária própria, prevista no orçamento da União para o exercício de 2022 e 2023 (a depender da época da aquisição e período de vigência da ata de registro de preços), a indicação da fonte e centro de custos, por se tratar de registro preços, será feito a cada parcela solicitada.

23. AMOSTRA DO OBJETO

23.1. Não haverá exigência de amostra do objeto.

24. DA PARTICIPAÇÃO DE CONSÓRCIOS

24.1. Não será permitida a participação de licitantes em consórcio.

25. ANEXO I

OBJETO: ITEM X				
ITEM. T.R	DESCRIÇÃO	REFERÊNCIA (DOCUMENTO OU URL)	PÁGINA	OBVERVAÇÕES
1.2.48	Solução antivirus...	Datasheet.pdf	123	

Goiânia, 05 de setembro de 2023.

Integrantes Requisitante:
Bruno de Oliveira Bastos
Centro de Recursos Computacionais - CERCOMP/UFG

Integrantes Técnico:
Kleiton Rodrigues de Araújo
Centro de Recursos Computacionais - CERCOMP/UFG

Integrante Administrativo:
Michelle Maria de Oliveira Landim
Coordenação de Licitações - DCOM/UFG

Autoridade máxima da Área de TIC
Jean Teixeira Lima
Diretor do Centro de Recursos Computacionais - CERCOMP

Apêndice - Estudo Técnico Preliminar

Estudo Técnico Preliminar, materializado pelo documento SEI nº 3985861, constante dos autos do presente procedimento, será publicado compactado como um dos anexos do edital da licitação, quando da divulgação desta licitação, no endereço eletrônico: www.comprasgovernamentais.gov.br.

Documento assinado eletronicamente por **Michelle Maria De Oliveira Landim**, **Assistente em Administração**, em 05/09/2023, às 14:58, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Bruno De Oliveira Bastos**, **Técnico de Tecnologia da Informação**, em 05/09/2023, às 15:01, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Kleiton Rodrigues De Araújo**, **Técnico de Tecnologia da Informação**, em 05/09/2023, às 15:03, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Igor Rodrigues Vieira**, **Diretor**, em 05/09/2023, às 15:04, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Jean Teixeira Lima**, **Diretor Substituto**, em 05/09/2023, às 15:20, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **4016918** e o código CRC **0404897A**.

Referência: Processo nº 23070.054244/2022-06 SEI nº 4016918