Serviço Público Federal
Ministério da Educação
Fundação Universidade Federal de Mato Grosso do Sul

LICITAÇÃO: TERMO DE REFERÊNCIA

Processo nº 23104.004333/2021-88

TERMO DE REFERÊNCIA
PROCESSO ADMINISTRATIVO N.º 23104.004333/2021-88
NOME DO PROJETO / SOLUÇÃO : Solução de antivírus para estações de trabalho.
CIDADE/MÊS/ANO: Campo Grande / 05-2021
UNIDADES RESPONSÁVEIS/REQUISITANTES: AGETIC
Tipo de Licitação: Menor Preço

Referência: Artigos 12 a 24 da IN 01/2019 - SGD/ME

1. **OBJETO**

1.1. Contratação **pelo Sistema de Registro de Preços (SRP)**, de empresa especializada para eventual FORNECIMENTO/CONTRATAÇÃO de **"Licenciamento de software antivírus para ambiente corporativo, com suporte e atualização de até 36 (trinta e seis) meses"**, na modalidade de subscrição (assinatura) para uso nas áreas técnica, administrativa e acadêmica da Universidade Federal de Mato Grosso do Sul (UFMS), conforme especificações do Termo de Referência.

2. **DESCRIÇÃO DA SOLUÇÃO DE TIC**

2.1. **BENS E SERVIÇOS QUE COMPÕEM A SOLUÇÃO**

Item	Código catmat/catser	Descrição	Complemento	Métrica ou Unidade	Qtde	Valor Unitário	Valor Total
1	027.502	Cessão temporária de direitos sobre programas de computador locação de software	Licenciamento de software antivírus para ambiente corporativo, com suporte e atualização de até 36 (trinta e seis) meses.	UNIDADE	4.500	R$ 126,33	R$ 568.485,00
2	3.840	Treinamento informática - sistema , software	Capacitação técnica para o sistema de gerenciamento do software antivírus com turma de até 20 (vinte) pessoas.	UNIDADE	1	R$ 14.833,33	R$ 14.833,33
TOTAL DO LOTE ÚNICO							**R$ 583.318,33**

2.2. A descrição da solução como um todo, conforme minudenciado nos itens 2 e 6 do Estudo Técnico Preliminar (documento SEI 2587410 e atualizado no documento SEI 2832900), abrange a contratação de empresa especializada para fornecimento, de forma eventual e oportuna, de licenças temporárias dos softwares antivírus para estações de trabalho, nas modalidades de subscrição (assinatura) e licenciamento temporário por 36 (trinta e seis) meses, para uso nas áreas

técnica, administrativa e acadêmica da UFMS.

2.3. A solução deverá estar em conformidade com a Instrução Normativa nº 1, de 4 de abril 2019, da Secretaria de Governo Digital do Ministério da Economia, e suas revisões, bem como à legislação que rege os processos de contratação no setor público (Lei 8.666/93, Lei 10.520/02, suas alterações e regulamentações).

2.4. O objeto da licitação tem a natureza de serviço comum de Cessão temporária de direitos sobre programas de computador locação de software.

2.4.1. Tal solução a ser contratada compõe-se de Bens Comuns e possui seus padrões de desempenho e qualidade definidos no presente Termo de Referência, por meio de especificações usuais praticadas no mercado.

2.5. Os quantitativos e respectivos códigos dos itens são os discriminados na tabela 2.1 acima.

2.6. A presente contratação adotará como regime de execução a Contratação do serviço por item – Licença temporária – sob demanda.

2.7. A validade da Ata de Registro de Preços será de 12 (doze) meses, a contar da sua assinatura pela UFMS, não sendo permitidas prorrogações.

2.8. As estimativas de consumo individualizadas, do órgão gerenciador e órgão(s) e entidade(s) participante(s) serão acrescentadas ao termo de referência final, após a divulgação da IRP no Comprasnet, e se houver participantes.

2.9. O prazo de vigência do(s) contrato(s) resultantes da ARP é de 36 (trinta e seis) meses. A unidade requisitante definirá se haverá formalização contratual a cada empenho realizado.

2.10. Terminologia e Definições Relevantes:

2.10.1. Para melhor entendimento e efeitos deste Termo de Referência, valem as seguintes terminologias e definições:

a) O conjunto de obrigações decorrentes deste Edital e da assinatura da Ata de Registro de Preços (ARP) será referenciado como "Contrato".

b) A Universidade Federal de Mato Grosso do Sul (UFMS) será referenciada como "CONTRATANTE".

c) As empresas adjudicadas serão referenciadas como "CONTRATADA" ou "CONTRATADAS".

d) A Agência de Tecnologia da Informação e Comunicação será referenciada como "AGETIC".

e) A Diretoria de Infraestrutura Tecnológica (UNIDADE REQUISITANTE) será referenciada como "DINTEC/AGETIC".

f) O Plano de Desenvolvimento Institucional será referenciado como "PDI".

g) O Plano Diretor de Tecnologia da Informação e Comunicação será referenciado como "PDTIC".

2.11. **Cotas para ME/EPP conforme Decreto n.º 8.538/2015**

2.11.1. Embora os Artigos 6º e 8° do Decreto 8538/2015 prevejam, respectivamente, a destinação exclusiva e a reserva de cotas às microempresas e empresas de pequeno porte em processos licitatórios, isto não será possível na presente contratação devido à política de comercialização de licenças estabelecida pelo fabricante dos softwares e o risco envolvido.

2.11.2. Diante dessa situação, a instituição de cotas e a destinação de itens exclusivos à microempresas e empresas de pequeno porte aumentaria o risco de fracasso da licitação em vários itens da presente contratação. Dada a necessidade de regularização e conformidade legal dos

licenciamentos na Instituição não é desejável incorrer nesse tipo de risco, sendo preferível a adaptação da contratação às políticas de mercado e do fabricante.

2.12. **Quanto à sustentabilidade**

2.12.1. **No que couber,** nos itens relacionados em que a atividade de fabricação ou industrialização for enquadrada no Anexo II da Instrução Normativa IBAMA n° 31, de 03/12/2009, só será admitida a oferta de produto cujo fabricante esteja regularmente registrado no Cadastro Técnico Federal de Atividades Potencialmente Poluidoras ou Utilizadoras de Recursos Ambientais, instituído pelo artigo 17, inciso II, da Lei n° 6.938, de 1981.

2.13. **Não será permita adesão à futura Ata de Registro de Preços**, considerando o Decreto 9488/2018, Artigo 22, Parágrafo 10: "*§ 10. É vedada a contratação de serviços de tecnologia da informação e comunicação por meio de adesão a ata de registro de preços que não seja:*

I - gerenciada pelo Ministério do Planejamento, Desenvolvimento e Gestão; ou

II - gerenciada por outro órgão ou entidade e previamente aprovada pela Secretaria de Tecnologia da Informação e Comunicação do Ministério do Planejamento, Desenvolvimento e Gestão."

3. JUSTIFICATIVA PARA A CONTRATAÇÃO - CONFORME OS ESTUDOS TÉCNICOS PRELIMINARES

3.1. **Contextualização e Justificativa da Contratação.**

3.1.1. A Justificativa e objetivo da contratação encontram-se pormenorizados nos itens 2 e 6 do Estudo Técnico Preliminar (documento SEI 2587410 e atualizado no documento SEI 2832900), apêndice desse Termo de Referência.

3.1.2. A Agência de Tecnologia da Informação e Comunicação (AGETIC), é a responsável pelos serviços de tecnologia da informação da Universidade Federal de Mato Grosso do Sul (UFMS), e tem como meta sempre trabalhar na melhoria das condições de suporte e infraestrutura de TI da instituição. A agência, por meio da Diretoria de Infraestrutura Tecnológica (DINTEC), provê um conjunto de serviços essenciais para os usuários como acesso à rede de dados, à internet, correio eletrônico, antivírus, antispam, firewall, entre outros. Esses serviços e dados são de extrema importância para os objetivos institucionais definidos pelo PDI e pelo PDTIC.

3.1.3. Ao longo dos últimos anos, a UFMS tem utilizado como solução de antivírus: "Kaspersky Endpoint Security for Business - Select Brazilian Edition". Contudo, com o término da vigência das licenças em agosto (1.000 licenças) e dezembro de 2021 (3.500 licenças), as estações de trabalho e servidores pertencentes ao parque tecnológico da instituição ficarão com versões dos softwares e das bases de dados (lista de vírus e vacinas) desatualizados, acarretando em vulnerabilidades nos sistemas corporativos, ampliando o risco de ataques maliciosos com a utilização de vírus, worms, ransomware, rootkits, cavalos de troia entre outros programas potencialmente indesejados capazes de comprometer a integridade e disponibilidade do dispositivos computacionais da instituição.

3.1.4. Para atender as necessidades da UFMS, será necessária a aquisição de 4.500 (quatro mil e quinhentas) licenças de software antivírus com suporte e atualização pelo prazo de até 36 (trinta e seis) meses. Esse quantitativo se justifica pela necessidade de atender a todos os computadores dos tipos: desktop, notebooks e servidores atualmente em operação no ambiente computacional da instituição. Assim, visando a continuidade da proteção do ambiente computacional e em virtude da proximidade do término da vigência dos contratos de licenciamento de software antivírus, há a necessidade de aquisição de novas licenças de software visando manter o atendimento da demanda de segurança nas estações de trabalho da instituição.

3.1.5. *Esses serviços são de extrema importância para os objetivos institucionais definidos pelo Plano de Desenvolvimento Institucional (PDI) e pelo Plano Diretor de Tecnologia da Informação e*

Comunicação (PDTIC). Dessa forma existe a demanda de contratação de licenças de software antivírus, nas modalidades de subscrição (assinatura), para uso nas áreas técnica, administrativa e acadêmica da Instituição, com vistas a regularização e/ou incremento de licenças.

3.2. Alinhamento aos Instrumentos de Planejamento Institucionais

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos**
A1	PDI/UFMS 2020-2024, Matriz Estratégica, Quadro 8, Item: 5. Consolidar as práticas de gestão, de governança, de compliance e de sustentabilidade, Subitem: 5.4 Taxa de melhoria da infraestrutura de TI e serviços digitais. (https://pdi.ufms.br/pdi-2020-2024-publicado/)
A2	PDTIC/UFMS 2021-2024, Quadro 6: Necessidades identificadas e priorizadas utilizando a matriz GUT; Objetivo: Aprimoramento da Segurança da Informação; Eixo Estratégico: Prover Segurança da Informação; Necessidade: Adequar a área de TIC à Lei Geral de Proteção de Dados; Alinhamento: EO.5, EO.16 e EO.17. (https://www.ufms.br/wp-content/uploads/2021/04/SEI_23104.025638_2020_42-1.pdf)
A3	PDTIC/UFMS 2021-2024, Quadro 7: Objetivos e Metas do PDTIC 2021-2024 da UFMS; Id 1: Objetivos: Aprimoramento da Segurança da Informação; Indicador: Projetos voltados à Segurança da Informação. (https://www.ufms.br/wp-content/uploads/2021/04/SEI_23104.025638_2020_42-1.pdf)
A4	PDTIC/UFMS 2021-2024, Quadro 8: Plano de Ações do PDTIC; Objetivo: Aprimoramento da Segurança da Informação; Necessidade: Adequar a área de TIC à Lei Geral de Proteção de Dados. (https://www.ufms.br/wp-content/uploads/2021/04/SEI_23104.025638_2020_42-1.pdf)

ALINHAMENTO AO PDTIC <2021-2024>			
ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
A1	PDTIC/UFMS 2021-2024, Quadro 6: Prover Segurança da Informação	**M1**	PDTIC/UFMS 2021-2024, Quadro 7: Aprimoramento da Segurança da Informação
A2	PDTIC/UFMS 2021-2024, Quadro 8: Adequar a área de TIC à Lei Geral de Proteção de Dados.	**M2**	PDTIC/UFMS 2021-2024, Quadro 7: Aprimoramento da Segurança da Informação

ALINHAMENTO AO PAC - 2021	
Item	**Descrição**
A1	Código do item cadastrado no PAC: 24333. Item do PGC: 32759. Descrição: Serviço de licença pelo uso de software. Descrição sucinta: Aquisição de 4.500 licenças para software antivírus.

O Plano Anual de Contratações (PAC) é o instrumento de planejamento que contempla bens, serviços, obras e soluções de TIC que o órgão ou entidade pretende contratar, elaborado no exercício anterior ao exercício da contratação, conforme regras dispostas na IN Seges/ME nº 1, de 10 de janeiro de 2019. Informações disponíveis em: https://www.gov.br/compras/pt-br/assuntos/plano-anual-de-contratacoes.

3.3. Estimativa de Demanda

3.3.1. Considerando o parque computacional da UFMS, o número de licenças ativas do software antivírus e a vigência estão descritas na tabela a seguir:

Aplicativo	Licenças	Data de Vigência
Kaspersky Endpoint Security for Business - Select Brazilian Edition. 5000+ Node 3 year Public Sector License: Kaspersky Security for WS and FS	3.500	24-12-2021
Kaspersky Endpoint Security for Business - Select Brazilian Edition. 5000+ Node 3 year Public Sector Renewal License: Kaspersky Security for WS and FS	1.000	22-08-2021

3.3.2. As quantidades identificadas no levantamento de demandas realizado pela Equipe de Planejamento da Contratação, estão descritas abaixo:

Solução Antivírus - Quantidades Identificadas		
Item	Quantidade	Métrica ou Unidade
Licenciamento de software antivírus para ambiente corporativo, com suporte e atualização de até 36 (trinta e seis) meses.	4.500	UNIDADE
Capacitação técnica para o sistema de gerenciamento do software de antivírus.	1	UNIDADE

3.3.3. Será necessária uma única aquisição do "Licenciamento de software antivírus para ambiente corporativo, com suporte e atualização de até 36 (trinta e seis) meses", no quantitativo de 4.500 (quatro mil e quinhentas) unidades, para atender as necessidades elencadas.

3.4. **Parcelamento da Solução de TIC**

Considerando, a Súmula TCU nº 247, que dispõe sobre a obrigatoriedade da admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade.

A Equipe de Planejamento da Contratação avalia como inviável o parcelamento da Solução de TIC a ser contratada, por se tratar de aquisição de software com direito a suporte técnico especializado do fabricante (incluindo-se aí o treinamento/capacitação técnica para o sistema de gerenciamento), conforme consta do item 2. Portanto, a modelagem da contratação inclui e inter-relaciona a comercialização de software para esse tipo de solução com o treinamento ofertado pelo contratado.

Diante das justificativas acima expostas, a licitação será realizada por lote único.

Item	Código catmat/catser	Descrição	Complemento	Métrica ou Unidade	Qtde
1	027.502	Cessão temporária de direitos sobre programas de computador locação de software	Licenciamento de software antivírus para ambiente corporativo, com suporte e atualização de até 36 (trinta e seis) meses.	UNIDADE	4.500
2	3.840	Treinamento informática - sistema , software	Capacitação técnica para o sistema de gerenciamento do software antivírus com turma de até 20 (vinte) pessoas.	UNIDADE	1

3.5. **Resultados e Benefícios a serem alcançados**

3.5.1. Manutenção da segurança do ambiente computacional visando proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição.

3.5.2. Evitar esforço em tarefas para tratamento de incidentes em função de infestações virais.

3.5.3. Evitar a indisponibilidade dos serviços em decorrência de ataques maliciosos.

3.5.4. Melhoria nas condições para o desempenho das atividades acadêmicas na instituição.

3.5.5. Melhoria nas condições para o desempenho das atividades administrativas na instituição.

3.5.6. Contribuir com a adequação à Lei Geral de Proteção de Dados Pessoais (LGPD), dos serviços ofertados pela AGETIC.

3.5.7. Software com suporte e garantia de atualização tecnológica.

3.5.8. Continuidade dos serviços da UFMS.

4. **DESCRIÇÃO DA SOLUÇÃO - CONFORME O ESTUDO TÉCNICO PRELIMINAR**

Licenciamento de software antivírus para estações de trabalho e servidores com arquitetura de hardware 32 bits e 64 bits, nas Plataformas Microsoft Windows, Mac e Linux, com suporte, treinamento e vigência por até 36 (trinta e seis meses) meses. Sendo 4.500 (quatro mil e quinhentas) licenças para estações de trabalho conforme Estudo Técnico Preliminar (SEI Nº 2587410 e atualizado no documento SEI 2832900) e Especificações Técnicas, a seguir:

4.1. **Especificações Técnicas**

4.1.1. **ITEM 1 (Cessão temporária de direitos sobre programas de computador locação de software)**

1. **Servidor de Administração e Console Administrativa**
    1. **Compatibilidade:**
        1. Microsoft Windows Server 2012 Standard / Core / Foundation / Essentials / Datacenter x64;
        2. Microsoft Storage Server 2012 e 2012 R2 x64;
        3. Microsoft Windows Server 2012 R2 Standard / Core / Foundation / Essentials / Datacenter x64;
        4. Microsoft Windows Server 2016 Standard / Core / Datacenter x64;
        5. Microsoft Windows Server 2019 Standard / Core / Datacenter x64;
        6. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;
        7. Microsoft Windows 8 SP1 Professional / Enterprise x32/x64;
        8. Microsoft Windows 8 Professional / Enterprise x64;
        9. Microsoft Windows 8.1 Professional / Enterprise x32;
        10. Microsoft Windows 8.1 Professional / Enterprise x64;
        11. Microsoft Windows 10 x32; e
        12. Microsoft Windows 10 x64.
    2. **Suporta as seguintes plataformas virtuais:**
        1. Vmware: Workstation 15.x Pro, vSphere 6.5, vSphere 6.7;
        2. Microsoft Hyper-V: 2012, 2012 R2, 2016, 2019 x64;
        3. Parallels Desktop 14; e
        4. Citrix XenServer 7.1.
    3. **Características:**
        1. A console deve ser acessada via WEB (HTTPS) ou MMC.
        2. Console deve ser baseada no modelo cliente/servidor.

3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade.
4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus.
5. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;
6. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença.
7. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory.
8. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria.
9. Deve armazenar histórico das alterações feitas em políticas.
10. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada.
11. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas.
12. A solução de gerenciamento deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas.
13. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador.
14. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle. Permite-se a utilização de soluções adicionais para a geração de relatórios, desde que, não gerem custos adicionais à CONTRATANTE.
15. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário.
16. Capacidade de gerenciar estações de trabalho e servidores de arquivos (Windows, Linux e Mac) protegidos pela solução antivírus.
17. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede.
18. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto.
19. Capacidade de atualizar os pacotes de instalação com as últimas vacinas.
20. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes.

21. A comunicação entre o cliente e o servidor de administração deve ser criptografada.

22. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes.

23. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

    1. Nome do computador;
    2. Nome do domínio;
    3. Range de IP;
    4. Sistema Operacional;
    5. Máquina virtual.

24. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas.

25. Deve permitir, por meio da console de gerenciamento, a exclusão e a restauração de um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional.

26. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção.

27. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção.

28. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente.

29. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc.

30. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos.

31. Deve fornecer as seguintes informações dos computadores:

    1. Se o antivírus está instalado;
    2. Se o antivírus está iniciado;
    3. Se o antivírus está atualizado;
    4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;
    5. Minutos/horas desde a última atualização de vacinas;
    6. Data e horário da última verificação executada na máquina;
    7. Versão do antivírus instalado na máquina;

8. Se é necessário reiniciar o computador para aplicar mudanças;
9. Nome do computador;
10. Data e horário de quando a máquina foi ligada;
11. Quantidade de vírus encontrados (contador) na máquina;
12. Domínio ou grupo de trabalho do computador;
13. Data e horário da última atualização de vacinas;
14. Sistema operacional com Service Pack;
15. Quantidade de processadores;
16. Quantidade de memória RAM;
17. Sessões de usuários, com informações de contato (caso disponíveis no Active Directory);
18. Endereço IP;
19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
20. Atualizações do Windows Update instaladas;
21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD; e
22. Vulnerabilidades de aplicativos instalados na máquina.

32. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las.
33. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
    1. Alteração de Gateway Padrão;
    2. Alteração de subrede;
    3. Alteração de domínio;
    4. Alteração de servidor DHCP;
    5. Alteração de servidor DNS;
    6. Alteração de servidor WINS;
    7. Resolução de Nome; e
    8. Disponibilidade de endereço de conexão SSL.
34. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet.
35. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes.
36. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus.
37. Capacidade de herança de tarefas e políticas na estrutura hierárquica

de servidores administrativos.

38. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede.

39. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo.

40. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML.

41. Capacidade de gerar traps SNMP para monitoramento de eventos.

42. Capacidade de enviar e-mails para contas específicas em caso de algum evento.

43. Listar em um único local, todos os computadores não gerenciados na rede.

44. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes.

45. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server.

46. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente.

47. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor.

48. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo).

49. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo porém sem comprometer o desempenho do computador.

50. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint).

51. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação.

52. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros.

53. Capacidade de realizar atualização incremental de vacinas nos computadores clientes.

54. Deve armazenar localmente e enviar ao servidor de gerência a

ocorrência de vírus com os seguintes dados, no mínimo:

1. Nome do vírus;
2. Nome do arquivo infectado;
3. Data e hora da detecção;
4. Nome da máquina ou endereço IP; e
5. Ação realizada.

55. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.
56. Capacidade de listar updates nas máquinas com o respectivo link para download.
57. Deve criar um backup de todos arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração.
58. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante.
59. Capacidade de realizar resumo de hardware de cada máquina cliente.
60. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

2. **Estações Windows**

1. **Compatibilidade:**

1. Microsoft Windows 7 Professional/ Enterprise/ Home SP1/ x86/ x64;
2. Microsoft Windows 8 Professional/ Enterprise/ x86/ x64;
3. Microsoft Windows 8.1 Professional/ Enterprise/ x86/ x64;
4. Microsoft Windows 10 Pro/ Enterprise/ Home/ Education/ x86/ x64;
5. Microsoft Windows Server 2019 Essentials/ Standard/ Datacenter;
6. Microsoft Windows Server 2016 Essentials/ Standard/ Datacenter;
7. Microsoft Windows Server 2012 R2 Foundation/ Essentials/ Standard/ Datacenter;
8. Microsoft Windows Server 2012 Foundation/ Essentials/ Standard/ Datacenter;
9. Microsoft Windows Server 2008 R2 Foundation/ Essentials/ Standard/ Datacenter SP1;
10. Microsoft Windows Small Business Server 2011 Standard/ Standard x64; e
11. Microsoft Windows MultiPoint Server 2011 x64.

2. **Características:**

1. Deve prover as seguintes proteções:

1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
2. Antivírus de Web (módulo para verificação de sites e downloads

contra vírus);

3. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
4. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
5. Firewall com IDS;
6. Autoproteção (contra-ataques aos serviços/processos do antivírus);
7. Controle de dispositivos externos;
8. Controle de acesso a sites por categoria, ex.: Bloquear conteúdo adulto, sites de jogos, etc;
9. Controle de acesso a sites por horário;
10. Controle de acesso a sites por usuários;
11. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de vídeo e áudio;
12. Controle de execução de aplicativos;
13. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

2. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota.
3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).
4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação.
5. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado.
6. Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas.
7. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks).
8. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.
9. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.
10. Ter a capacidade de fazer detecções por comportamento, identificando

ameaças avançadas sem a necessidade de assinaturas.

11. Capacidade de verificar somente arquivos novos e alterados.
12. Capacidade de verificar objetos usando heurística.
13. Capacidade de agendar uma pausa na verificação.
14. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias.
15. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado.
16. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.
17. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI.
18. Capacidade de verificar tráfego nos browsers: Edge, Google Chrome Internet Explorer e Firefox.
19. Capacidade de verificar links inseridos em e-mails contra phishings.
20. Capacidade de verificação de corpo e anexos de e-mails usando heurística.
21. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas.
22. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.
23. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.
24. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador.
25. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
    1. Perguntar o que fazer, ou;
    2. Bloquear o e-mail;
        1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
        2. Caso positivo de desinfecção:
            1. Restaurar o e-mail para o usuário;
        3. Caso negativo de desinfecção:
            1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);
26. Deve ter suporte total ao protocolo IPv6.
27. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail.
28. O antivírus de web deve realizar a verificação de, no mínimo, duas

maneiras diferentes, sob escolha do administrador:

1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;
2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação.

29. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web.

30. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas.

31. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.

32. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas.

33. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas.

34. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica.

35. Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.

36. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
    1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
    2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

37. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
    1. Discos de armazenamento locais;
    2. Armazenamento removível;
    3. Impressoras;
    4. CD/DVD;
    5. Drives de disquete;
    6. Modems;
    7. Dispositivos de fita;

8. Dispositivos multifuncionais;
9. Leitores de smart card;
10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
11. Wi-Fi;
12. Adaptadores de rede externos;
13. Dispositivos MP3 ou smartphones;
14. Dispositivos Bluetooth; e
15. Câmeras e Scanners.

38. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário.
39. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário.
40. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento.
41. Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc.
42. Capacidade de configurar novos dispositivos por Class ID/Hardware ID.
43. Capacidade de limitar a execução de aplicativos por hash MD5 ou SHA256, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc).
44. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:
    1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras; e
    2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.
45. Capacidade de bloquear execução de aplicativo que está em armazenamento externo.
46. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo.
47. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.
48. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.
49. Capacidade de voltar ao estado anterior do sistema operacional após

um ataque de malware.

50. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

51. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

52. Capacidade de integração com o Windows Defender Security Center.

53. Capacidade de integração com a Antimalware Scan Interface (AMSI).

54. Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).

3. **Estações Mac OS X**

1. **Compatibilidade:**

1. Mac OS Mojave 10.14;
2. Mac OS Catalina 10.15; e
3. Mac OS Big Sur 11.3 ou posterior.

2. **Características:**

1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado.
2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços HTTPS.
3. Possuir módulo de bloqueio á ataques na rede.
4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador.
5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede.
6. Possibilidade de importar uma chave no pacote de instalação.
7. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota.
8. Deve possuir suportes a notificações utilizando o Growl.
9. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).
10. Capacidade de voltar para a base de dados de vacina anterior.
11. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas.
12. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado.
13. Possibilidade de desabilitar automaticamente varreduras agendadas

quando o computador estiver funcionando a partir de baterias (notebooks).

14. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.
15. Capacidade de verificar somente arquivos novos e alterados.
16. Capacidade de verificar objetos usando heurística.
17. Capacidade de agendar uma pausa na verificação.
18. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
    1. O que fazer aplicar, ou;
    2. Bloquear acesso ao objeto;
        1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
        2. Caso positivo de desinfecção:
            1. Restaurar o objeto para uso.
        3. Caso negativo de desinfecção:
            1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).
19. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.
20. Capacidade de verificar arquivos de formato de email.
21. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando.
22. Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

4. **Estações de trabalho Linux**
    1. **Compatibilidade:**
        1. Plataformas 64-bits: Ubuntu e CentOS.
    2. **Características:**
        1. Deve prover as seguintes proteções:
            1. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado.
            2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
            3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
                1. Capacidade de criar exclusões por local, máscara e nome da ameaça;

2. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
3. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

4. Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers;
5. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:
    1. Alta;
    2. Média;
    3. Baixa; e
    4. Recomendado.
6. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.
7. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.
8. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares.
9. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.
10. Capacidade de verificar objetos usando heurística.

5. **Servidores Windows**
    1. **Compatibilidade:**
        1. **Plataforma 64-bits:**
            1. Windows Server 2003 Standard/ Enterprise/ Datacenter SP2 e posterior;
            2. Windows Server 2003 R2 Standard/ Enterprise/ Datacenter SP2 e posterior;
            3. Microsoft Windows Server 2008 Standard/ Enterprise/ DataCenter SP1 ou posterior;
            4. Microsoft Windows Server 2008 Core Standard/ Enterprise/ DataCenter SP1 ou posterior;
            5. Microsoft Windows Server 2008 R2 Foundation/ Standard/ Enterprise/ DataCenter SP1 ou posterior;
            6. Microsoft Windows Server 2008 R2 Core Standard/ Enterprise/ DataCenter SP1 ou posterior;

7. Microsoft Small Business Server 2008 Standard/ Premium;
8. Microsoft Windows Hyper-V Server 2008 R2 SP1 e posterior;
9. Microsoft Microsoft Small Business Server 2011 Essentials/ Standard;
10. Microsoft Windows MultiPoint Server 2011;
11. Microsoft Windows Server 2012 Essentials/ Standard/ Foundation/ Datacenter/ MultiPoint;
12. Microsoft Windows Server 2012 R2 Essentials/ Standard/ Foundation/ Datacenter;
13. Microsoft Windows Server 2012 Core Standard/ Datacenter;
14. Microsoft Windows Server 2012 R2 Core Standard/ Datacenter;
15. Microsoft Windows Storage Server 2012;
16. Microsoft Windows Storage Server 2012 R2;
17. Microsoft Windows Hyper-V Server 2012;
18. Microsoft Windows Hyper-V Server 2012 R2;
19. Windows Server 2016 Essentials/ Standard/ Datacenter/ MultiPoint Premium Server;
20. Windows Server 2016 Core Standard/ Datacenter;
21. Windows Storage Server 2016;
22. Windows Hyper-V Server 2016;
23. Microsoft Windows Server 2019 Core/ Terminal/ Hyper-V; e
24. Windows Server IoT 2019 for Storage.

2. **Características:**
    1. Deve prover as seguintes proteções:
        1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado.
        2. Auto-proteção contra-ataques aos serviços/processos do antivírus.
        3. Firewall com IDS.
        4. Controle de vulnerabilidades do Windows e dos aplicativos instalados
    2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota.
    3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
    4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
        1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).
        2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação).

3. Leitura de configurações.
4. Modificação de configurações.
5. Gerenciamento de Backup e Quarentena.
6. Visualização de relatórios.
7. Gerenciamento de relatórios.
8. Gerenciamento de chaves de licença.
9. Gerenciamento de permissões (adicionar/excluir permissões acima).

5. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
   1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas.
   2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
6. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total.
7. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede.
8. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc).
9. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares.
10. Capacidade de configurar níveis diferentes de verificação para processos.
11. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor.
12. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas.
13. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação.
14. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação.
15. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado.
16. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou

processamento.

17. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.
18. Capacidade de verificar somente arquivos novos e alterados.
19. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.).
20. Capacidade de verificar objetos usando heurística.
21. Capacidade de configurar diferentes ações para diferentes tipos de ameaças.
22. Capacidade de agendar uma pausa na verificação.
23. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado.
24. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.
25. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.
26. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.
27. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).
28. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

6. **Servidores Linux**
    1. **Compatibilidade:**
        1. Plataformas 32 e 64-bits: Ubuntu e CentOS.
    2. **Características:**
        1. Deve prover as seguintes proteções:
            1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado.
            2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
        2. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
            1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas).
            2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de

desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes.

3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena.

4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

3. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares.

4. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento.

5. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo.

6. Capacidade de verificar objetos usando heurística.

7. **Manutenção:**

1. O fabricante da solução deverá manter site na internet em português ou inglês que possua os manuais, atualizações para download, FAQs, instruções, contatos e quaisquer outras informações necessárias para o uso e permanente atualização dos mesmos.

2. O fabricante/fornecedor deverá manter suporte técnico (para resolução de dúvidas e problemas) em português, durante todo o prazo de vigência do contrato, através dos seguintes meios: Telefones fixos em horário comercial (07:00 às 11:00 e 13:00 às 17:00 - horário do MS); Abertura de Chamados On-line; Web Site na Internet; e E-mail.

8. **Segurança:**

1. Devem ser seguidos os atributos básicos, segundo os padrões internacionais (ISO/IEC 17799:2005), a saber:

1. Confidencialidade - propriedade que limita o acesso à informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.

2. Integridade - propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição).

3. Disponibilidade - propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.

4. Irretratabilidade - propriedade que garante a impossibilidade de negar a autoria em relação a uma transação anteriormente feita.

5. Devem ser seguidos os atributos básicos, segundo os padrões internacionais ISO 27001 e ISO 27002.

4.1.2. **ITEM 2 (Treinamento informática - sistema , software)**

1. Possuir carga horária mínima de 20 horas.
2. Turma com até 20 (vinte) representantes da CONTRATANTE.
3. Os treinamentos poderão ser realizados na modalidade de ensino à distância.
4. Os treinamentos deverão ser realizados em dias úteis, em horário comercial.
5. Deverá ser disponibilizado material didático impresso e/ou em mídia, sem custo adicional para a CONTRATANTE. Todo material deverá estar, preferencialmente, em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês).
6. Deverá ser emitido certificado de participação ao final do curso a cada participante.
7. O cronograma efetivo do treinamento será definido em conjunto com a CONTRATANTE, após a assinatura do contrato.
8. Abordar em seu conteúdo programático os seguintes temas:
    1. Solução de Antivírus, Firewall e IPS (Desktops : Windows, Mac, e Linux, e Servidores Windows e Linux).
    2. Controle de Aplicativos.
    3. Controle de Acesso à WEB.
    4. Controle de Dispositivos (USB).
    5. Gerenciamento de vulnerabilidades e correções.
    6. Implementação do sistema operacional (imagens de sistema para aplicar em desktops).
    7. Distribuição de software.
    8. Inventários de hardware e software.
    9. Integração com soluções de SIEM.
    10. Console de Gerenciamento Integrada.
9. Caso o treinamento/atualização fornecido não seja satisfatório, mediante avaliação tempestiva e fundamentada, tanto em relação à qualidade ou à carga horária efetiva, a CONTRATADA deverá realizá-los novamente, sem ônus adicional a CONTRATANTE.

5. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

Conforme o Estudo Técnico Preliminar 2832900, os requisitos mínimos para a contratação abrangem os itens a seguir:

5.1. Requisitos de Negócio

5.1.1. Aquisição de licenças de software antivírus para os servidores e estações de trabalho da CONTRATANTE.

5.1.2. Garantia de compatibilidade.

5.1.3. Treinamento e Atualização Tecnológica.

5.2. Requisitos de Capacitação

5.2.1. Possuir carga horária mínima de 20 horas.

5.2.2. Turma com até 20 (vinte) representantes da CONTRATANTE.

5.2.3. Os treinamentos poderão ser realizados na modalidade de ensino à distância.

5.2.4. Os treinamentos deverão ser realizados em dias úteis, em horário comercial.

5.2.5. Deverá ser disponibilizado material didático impresso e/ou em mídia, sem custo adicional para a CONTRATANTE. Todo material deverá estar, preferencialmente, em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês).

5.2.6. Deverá ser emitido certificado de participação ao final do curso a cada participante.

5.2.7. O cronograma efetivo do treinamento será definido em conjunto com a CONTRATANTE, após a assinatura do contrato.

5.3. **Requisitos Legais**

5.3.1. A presente contratação obedecerá, no que for pertinente, ao disposto nas seguintes legislações:

a) Lei nº 8.666, de 21 de junho de 1993, que regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências; e legislação correlata às licitações.

b) Lei nº 10.520, de 17 de julho de 2002, que institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências.

c) Decreto nº 7.174, de 12 de maio de 2010, que regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União.

d) Decreto nº 7.746, de 05 de junho de 2012, que regulamenta o art. 3º da Lei no 8.666/93, para estabelecer critérios, práticas e diretrizes para a promoção do desenvolvimento nacional sustentável nas contratações realizadas pela administração pública federal.

e) Decreto nº 8.250, de 23 de maio de 2014, que Altera o Decreto nº 7.892, de 23 de janeiro de 2013, que regulamenta o Sistema de Registro de Preços previsto no art. 15 da Lei nº 8.666, de 21 de junho de 1993.

f) Decreto nº 8.538, de 06 de outubro de 2015, que regulamenta o tratamento favorecido, diferenciado e simplificado para as microempresas, empresas de pequeno porte, agricultores familiares, produtores rurais pessoa física, microempreendedores individuais e sociedades cooperativas de consumo nas contratações públicas de bens, serviços e obras no âmbito da administração pública federal.

g) Decreto nº 9.412, de 18 de junho de 2018, que atualiza os valores das modalidades de licitação de que trata o art. 23 da Lei nº 8.666, de 21 de junho de 1993.

h) Decreto nº 9.488, de 30 de agosto de 2018, altera o Decreto nº 7.892, de 23 de janeiro de 2013, que regulamenta o Sistema de Registro de Preços previsto no art. 15 da Lei nº 8.666, de 21 de junho de 1993, e o Decreto nº 7.579, de 11 de outubro de 2011, que dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, do Poder Executivo federal.

i) Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.

j) Decreto nº 10.024 de 20 de setembro de 2019, que regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências.

k) Instrução Normativa nº 01, de 19 de janeiro de 2010, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências.

l) Instrução Normativa nº 03 do MP, de 20 de abril de 2017, que altera a Instrução Normativa nº 5, de 27 de junho de 2014, que dispõe sobre os procedimentos administrativos básicos para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral.

m) Instrução Normativa nº 01 do ME, de 01 de janeiro de 2019, que dispõe sobre o Plano Anual de Contratações de bens, serviços, obras e soluções de tecnologia da informação e comunicações no âmbito da Administração Pública Federal direta, autárquica e fundacional e sobre o Sistema de Planejamento e Gerenciamento de Contratações.

n) Instrução Normativa nº 1, de 4 de abril 2019, da Secretaria de Governo Digital do Ministério da Economia, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC, pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

o) Instrução Normativa SGD/ME nº 202, de 18 de setembro de 2019 - altera a Instrução Normativa nº 1, de 4 de abril de 2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

p) Instrução Normativa no 31, de 23 de março de 2021, que altera a Instrução Normativa no 1, de 4 de abril de 2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

q) Portaria SGD/ME no 6.432, de 15 de junho de 2021, que estabelece modelo de contratação de serviços de operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

5.4. **Requisitos de Manutenção**

5.4.1. O fabricante da solução deverá manter site na internet em português ou inglês que possua os manuais, atualizações para download, FAQs, instruções, contatos e quaisquer outras informações necessárias para o uso e permanente atualização dos mesmos.

5.4.2. O fabricante/fornecedor deverá manter suporte técnico (para resolução de dúvidas e problemas) em português, durante todo o prazo de vigência do contrato, através dos seguintes meios:

a) Telefones fixos em horário comercial (07:00 às 11:00 MS);

b) Abertura de Chamados On-line;

c) Web Site na Internet; e

d) E-mail.

5.5. **Requisitos Temporais**

5.5.1. A prestação de serviços será iniciada a partir da assinatura do contrato, de acordo com as necessidades da UFMS.

5.6. **Requisitos de Segurança e Privacidade**

5.6.1. As PARTES comprometem-se a manter sob estrita confidencialidade toda e qualquer informação trocada entre si relativamente à presente prestação de serviços, bem como toda e qualquer informação ou documento dela derivado, sem prejuízo de qualquer outra proteção assegurada às PARTES.

5.6.2. Todas as informações e conhecimentos aportados pelas PARTES para a execução do objeto deste contrato são tratados como confidenciais, assim como todos os seus resultados.

5.6.3. A confidencialidade implica a obrigação de não divulgar ou repassar informações e conhecimentos a terceiros não envolvidos nesta relação contratual sem autorização expressa por escrito dos seus detentores, na forma que dispõe a Lei no 9.279/96, art. 195, XI.

5.6.4. Não são tratadas como conhecimentos e informações confidenciais as informações que foram comprovadamente conhecidas por outra fonte de forma legal e legítima, independentemente da iniciativa das PARTES no contexto deste contrato.

5.6.5. Qualquer exceção à confidencialidade só será possível com a anuência prévia e por escrito dos signatários do presente contrato em disponibilizar a terceiros determinada informação, ficando desde já acordado entre as PARTES que está autorizada a disponibilização das informações confidenciais a terceiros nos casos de exigências legais.

5.6.6. Para fins do presente termo, a expressão “Informação Confidencial” significa toda e qualquer informação revelada, fornecida ou comunicada (seja por escrito, em forma eletrônica ou sob qualquer outra forma material) pelas PARTES entre si, seus representantes legais, administradores, diretores, empregados, consultores ou contratados (em conjunto, doravante designados “REPRESENTANTES”), dentro do escopo supramencionado.

5.6.7. A informação que vier a ser revelada, fornecida ou comunicada verbalmente entre os signatários deste Instrumento deverá integrar ata lavrada entre seus representantes para que possa constituir objeto mensurável para efeito da confidencialidade ora pactuada.

5.6.8. O não cumprimento do estipulado nesta cláusula por qualquer uma das PARTES, inclusive em caso de eventuais danos causados à parte contrária ou a terceiros, responsabilizará quem lhe der causa, nos termos da lei.

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

5.7.1. No que couber, visando a atender ao disposto na legislação aplicável – em destaque às Instruções Normativas 05/2017/SEGES e 01/2019/SGD – a CONTRATADA deverá priorizar, para a execução dos serviços, a utilização de bens que sejam no todo ou em partes compostos por materiais recicláveis, atóxicos e biodegradáveis.

5.8. **Requisitos de Arquitetura Tecnológica**

5.8.1. O CONTRATANTE fornecerá à CONTRATADA:

a) Acesso físico às dependências relacionadas à prestação dos serviços;

b) Acesso lógico e os respectivos privilégios adequados nos sistemas, aplicações e ferramentas necessárias a perfeita execução dos serviços, exclusivamente para os profissionais diretamente envolvidos em sua execução;

c) Instalações, mobiliário e estações de trabalho necessárias à execução dos serviços, não sendo permitido à CONTRATADA alocar nas dependências do CONTRATANTE representantes que não atuem na execução do CONTRATO; e

d) Acesso às soluções de hardware e software de sua propriedade necessárias à execução das atividades contratadas, não desobrigando a CONTRATADA de fornecer eventuais soluções de software especificadas na contratação (quando for o caso).

5.8.2. À CONTRATADA caberá fornecer todos os demais recursos e condições técnicas

necessárias à execução dos serviços, incluindo ferramentas específicas, materiais de apoio, materiais de identificação, equipamentos de proteção individual, etc.

5.8.3. A CONTRATADA somente efetuará as impressões estritamente associadas às atividades técnicas vinculadas aos serviços demandados pelo CONTRATANTE.

5.8.4. A CONTRATADA deverá manter controle das ligações telefônicas (locais, nacionais, internacionais, celulares) realizadas pela sua equipe com finalidade de apoio e suporte à execução dos serviços contratados.

5.8.5. A CONTRATADA deverá observar que, ao optar por utilizar e ou instalar alguma solução tecnológica no ambiente para a prestação de serviços, fica obrigada a solicitar a autorização prévia à implementação para que o CONTRATANTE decida a respeito da adequação e possa adotar todas as providências cabíveis à eventual implementação.

5.8.6. A solicitação por parte da CONTRATADA deverá incluir o projeto detalhado de implementação da solução, informando sua descrição, escopo de atuação, infraestrutura necessária, documentação de licenciamento e propriedade, benefícios e vantagens, os recursos profissionais e tecnológicos envolvidos, prazos e níveis de acesso necessários.

5.8.7. Toda solução tecnológica instalada nas dependências do CONTRATANTE, a pedido da CONTRATADA, será de livre acesso de consulta aos representantes indicados pelo CONTRATANTE que, ocasionalmente e quando aplicável, pode contemplar – além dos servidores da área de Tecnologia da Informação, equipe de fiscalização contratual e representantes de órgão internos/externos de controle.

5.8.8. Caberá à CONTRATADA toda providência junto ao fabricante/fornecedor e/ou detentor da propriedade intelectual da solução tecnológica quanto à ciência e/ou autorização (se aplicável) das condições de uso do produto nas dependências do CONTRATANTE, afastando qualquer interpretação de aquisição da solução tecnológica pelo CONTRATANTE e/ou uso não autorizado.

5.8.9. No caso de uma solução implementada pela CONTRATADA causar instabilidade/indisponibilidade do ambiente computacional, ficando comprovada culpa, esta poderá sofrer sanções administrativas e contratuais cabíveis, além de responder por eventuais prejuízos decorrentes. A CONTRATADA assume todos e quaisquer ônus financeiros referente às eventuais reclamações/processos judiciais de fabricantes/fornecedores da solução tecnológica licenciada para a CONTRATADA contra o uso destas nas dependências do CONTRATANTE.

5.9. **Requisitos de Projeto, Implementação e Implantação**

5.9.1. A CONTRATADA será inteiramente responsável pela instalação, atualização ou migração da solução antivírus atualmente em uso pela CONTRATANTE, bem como às despesas diretas ou indiretas para execução das atividades pela sua equipe técnica.

5.9.2. A instalação, atualização ou migração dos softwares em estações de trabalho poderá ser realizada remotamente, sem causar indisponibilidade do ambiente, devendo ser realizada em horários a serem definidos pela CONTRATANTE.

5.9.3. A instalação, atualização ou migração dos softwares em servidores de rede poderá ser realizada remotamente, devendo ser realizada em horários a serem definidos pela CONTRATANTE.

5.9.4. A CONTRATANTE poderá autorizar a instalação, atualização ou migração durante o horário de expediente se, ao seu exclusivo critério, entender que não oferece risco ao funcionamento de sua rede de computadores e serviços em produção.

5.9.5. O processo de instalação, atualização ou migração da solução deverá ser acompanhado por analistas da CONTRATANTE.

5.9.6. Para garantir que a instalação, atualização ou migração não afetará o ambiente da CONTRATANTE, os procedimentos e atividades deverão ser realizados por técnicos certificados pelo fabricante.

5.10. **Requisitos de Garantia**

5.10.1. Não será exigida garantia por se tratar de contração de licenças de uso de softwares. O pagamento somente será realizado após a confirmação de plena operação da solução contratada.

5.11. **Requisitos de Metodologia de Trabalho**

5.11.1. Na execução das demandas a CONTRATADA deve zelar pela observância às políticas, diretrizes, procedimentos, padrões e modelos para as atividades de gestão e fiscalização de contratos e planejamento de contratações – dentre esses, destacadamente, Manual de Gestão e Fiscalização de Contratos da Fundação Universidade Federal de Mato Grosso do Sul. - disponíveis para acesso e download através do seguinte endereço eletrônico: https://proadi.ufms.br/files/2020/01/Manual-de-Gest%C3%A3o-e-Fiscaliza%C3%A7%C3%A3o.pdf

5.12. **Outros Requisitos Aplicáveis**

5.12.1. A CONTRATADA deverá apresentar:

a) Documento oficial da fabricante da solução ofertada, no qual declare e comprove que é uma revenda autorizada, ou seja, que comprove poder de operacionalizar/vender a solução contratada, prazos e níveis de serviços especificados no presente Termo de Referência.

b) Declaração que ateste a inexistência da prática de “registro de oportunidade”. Essa declaração tem por objetivo garantir o princípio constitucional da isonomia e da seleção da proposta mais vantajosa para a Administração Pública, conforme disposto na Lei no 8.666, de 1993.

5.12.2. Em função da necessidade de gerenciamento centralizado das licenças da presente contratação pela UFMS, além do fato de que podem haver diversas empresas CONTRATADAS, fica estabelecido que:

a) Cada CONTRATADA deverá verificar junto ao Fabricante a pré-existência de um contrato em nome da CONTRATANTE.

b) Caso ainda não exista tal contrato junto ao Fabricante, a CONTRATADA deverá providenciar a geração de um contrato único e principal por meio do qual serão vinculadas todas as demais licenças a serem adquiridas na presente contratação. Neste caso, a CONTRATADA deverá ainda encaminhar as credenciais de acesso à plataforma de gerenciamento de licenças do Fabricante em nome do (a) Diretor (a)da Agência de Tecnologia da Informação e Comunicação (AGETIC), para o endereço eletrônico agetic@ufms.br.

c) Em caso de existência de contrato junto a Fabricante, a CONTRATADA deverá providenciar a vinculação das licenças ao referido contrato.

d) Na ocasião da Assinatura da Ata, as CONTRATADAS deverão informar os canais de atendimento e suporte por telefone e endereço eletrônico.

6. **RESPONSABILIDADES**

6.1. **Deveres e responsabilidades da CONTRATANTE**

a) Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

b) 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 ou Projeto Básico;

c) Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

d) Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis,

comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

e) Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

f) Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

g) Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da contratada, com base em pesquisas de mercado, quando aplicável;

h) Prever que 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, o código-fonte de aplicações, os modelos de dados e as bases de dados, pertençam à Administração;

i) Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;

j) Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

k) Notificar a Contratada por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas;

l) Pagar à Contratada o valor resultante da prestação do serviço, no prazo e condições estabelecidas neste Termo de Referência;

m) Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da contratada, no que couber, em conformidade com o item 6 do Anexo XI da IN SEGES/MP n. 5/2017;

n) Não praticar atos de ingerência na administração da Contratada, tais como:

1. exercer o poder de mando sobre os empregados da Contratada, devendo reportar-se somente aos prepostos ou responsáveis por ela indicados, exceto quando o objeto da contratação previr o atendimento direto, tais como nos serviços de recepção e apoio ao usuário;
2. direcionar a contratação de pessoas para trabalhar nas empresas Contratadas;
3. promover ou aceitar o desvio de funções dos trabalhadores da Contratada, mediante a utilização destes em atividades distintas daquelas previstas no objeto da contratação e em relação à função específica para a qual o trabalhador foi contratado; e
4. considerar os trabalhadores da Contratada como colaboradores eventuais do próprio órgão ou entidade responsável pela contratação, especialmente para efeito de concessão de diárias e passagens.

o) Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando se tratar de contrato oriundo de Ata de Registro de Preços;

p) Proporcionar todas as facilidades para a CONTRATADA executar o fornecimento dos serviços objeto da contratação, permitindo, quando necessário, o acesso dos profissionais da CONTRATADA às suas dependências. Esses profissionais ficarão sujeitos a todas as

normas internas da UFMS, principalmente as de segurança, inclusive àquelas referentes à identificação, trajes, trânsito e permanência em suas dependências;

q) Promover o acompanhamento e a fiscalização da execução dos serviços objeto da contratação, sob o aspecto quantitativo e qualitativo, anotando em registro próprio as falhas detectadas;

r) Comunicar prontamente à CONTRATADA qualquer anormalidade na execução do objeto, podendo recusar o recebimento, caso não esteja de acordo com as especificações e condições estabelecidas no Termo de Referência;

s) Receber o objeto fornecido pela CONTRATADA que esteja em conformidade com a proposta aceita, conforme inspeções realizadas, observando o disposto no art. 17, da Instrução Normativa nº 1, de 4 de abril 2019, da Secretaria de Governo Digital (Ministério da Economia);

t) Liquidar o empenho e efetuar o pagamento à CONTRATADA, dentro dos prazos preestabelecidos em Contrato;

u) Solicitar por escrito, durante o período de recebimento, a troca ou correção das licenças de uso que apresentarem erros ou não estiverem de acordo com a proposta comercial e especificações técnicas do Termo de Referência;

v) Encaminhar formalmente a demanda, preferencialmente por meio de Ordem de Serviço ou Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência ou Projeto Básico, observando se o disposto no arts. 18 e 32 da IN 01/2019;

w) Responsabilizar-se por quaisquer prejuízos advindos da utilização das informações disponibilizadas por meio da solução causados pela CONTRATANTE a terceiros;

x) Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto do contrato;

y) Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento das obrigações pela Contratada;

z) Arquivar, entre outros documentos, projetos, "as built", especificações técnicas, orçamentos, termos de recebimento, contratos e aditamentos, relatórios de inspeções técnicas após o recebimento do serviço e notificações expedidas;

aa) Fiscalizar o cumprimento dos requisitos legais, quando a contratada houver se beneficiado da preferência estabelecida pelo art. 3º, § 5º, da Lei nº 8.666, de 1993;

ab) Assegurar que o ambiente de trabalho, inclusive seus equipamentos e instalações, apresentem condições adequadas ao cumprimento, pela contratada, das normas de segurança e saúde no trabalho, quando o serviço for executado em suas dependências, ou em local por ela designado; e

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

6.2. **Deveres e responsabilidades da CONTRATADA**

a) Indicar formalmente e por escrito, no prazo máximo de 10 (dez) dias úteis após a assinatura do contrato, junto à contratante, um preposto idôneo com poderes de decisão para representar a contratada, principalmente no tocante à eficiência e agilidade da execução do objeto deste Termo de Referência, e que deverá responder pela fiel execução do contrato;

b) Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

c) 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;

d) 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;

e) Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

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

g) Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

h) 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;

i) Executar o objeto do certame em estreita observância dos ditames estabelecido pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);

j) Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do contrato, sem prévia autorização da contratante;

k) Não fazer uso das informações prestadas pela contratante para fins diversos do estrito e absoluto cumprimento do contrato em questão;

l) Manter os sistemas contratados em pleno funcionamento e livres de erros, corrigir as licenças de uso que apresentarem qualquer tipo de erro ou que estiverem fora das especificações contidas no Termo de Referência;

m) Manter, durante a vigência do contrato, em compatibilidade com as obrigações assumidas, as condições de qualificação e habilitação necessárias para a contratação com a Administração Pública, apresentando, sempre que exigidos, os comprovantes de regularidade fiscal, jurídica, técnica e econômica;

n) Responsabilizar-se pelas despesas de quaisquer tributos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, prestação de garantia, e quaisquer outros que incidam ou venham a incidir na execução do contrato;

o) Manter sigilo absoluto sobre informações, dados e documentos provenientes da execução do Contrato e também às demais informações internas do CONTRATANTE, a que a CONTRATADA tiver conhecimento, por força de execução do objeto contratado;

p) Informar a CONTRATANTE sempre que forem disponibilizadas atualizações significativas dos sistemas contratados;

q) Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem nos serviços, até o limite estabelecido no parágrafo 1º do art. 65 da Lei nº. 8.666/1993;

r) 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 do contrato;

s) Quando especificada, manter, durante a execução do Contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da Solução de TIC;

t) Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer e utilizar os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade mínimas especificadas neste Termo de Referência e em sua proposta;

u) Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados (se for o caso);

v) Manter a execução do serviço nos horários fixados pela Administração (se for o caso);

w) Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à União ou à entidade federal, devendo ressarcir imediatamente a Administração em sua integralidade, ficando a Contratante autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos;

x) Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor; (se for o caso);

y) Vedar a utilização, na execução dos serviços, de empregado que seja familiar de agente público ocupante de cargo em comissão ou função de confiança no órgão Contratante, nos termos do artigo 7° do Decreto n° 7.203, de 2010; (se for o caso);

z) Disponibilizar à Contratante os empregados devidamente uniformizados e identificados por meio de crachá, além de provê-los com os Equipamentos de Proteção Individual - EPI, quando for o caso;

aa) Fornecer os uniformes a serem utilizados por seus empregados, conforme disposto neste Termo de Referência, sem repassar quaisquer custos a estes; (se for o caso);

ab) Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, a empresa contratada deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos:

1. prova de regularidade relativa à Seguridade Social;
2. certidão conjunta relativa aos tributos federais e à Dívida Ativa da União;
3. certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado;
4. Certidão de Regularidade do FGTS – CRF; e
5. Certidão Negativa de Débitos Trabalhistas – CNDT, conforme alínea "c" do item 10.2 do Anexo VIII-B da IN SEGES/MP n. 5/2017.

ac) Relatar à Contratante toda e qualquer irregularidade verificada no decorrer da prestação dos serviços;

ad) Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

ae) Não beneficiar-se da condição de optante pelo Simples Nacional, salvo as exceções previstas no § 5º-C do art. 18 da Lei Complementar no 123, de 14 de dezembro de 2006; (se for o caso)

af) Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores

futuros e incertos, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993; (se for o caso);

ag) Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços; (se for o caso)

ah) Prestar todo esclarecimento ou informação solicitada pela Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do serviço;

ai) Paralisar, por determinação da Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros; (se for o caso)

aj) Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram este Termo de Referência, no prazo determinado;

ak) Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina;

al) Submeter previamente, por escrito, à Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou Termo de Referência;

am) Comprovar, ao longo da vigência contratual, a regularidade fiscal das microempresas e/ou empresas de pequeno porte subcontratadas no decorrer da execução do contrato, quando se tratar da subcontratação prevista no artigo 48, II, da Lei Complementar n. 123, de 2006 e artigo 7º do Decreto n. 8.538/2015. (se for o caso);

an) Realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos da contratante ou da nova empresa que continuará a execução dos serviços;(se for o caso)

ao) Manter, durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação; e

ap) Não haverá pagamento adicional pela Contratante à Contratada em razão do cumprimento das obrigações previstas neste item.

6.3. **Deveres e responsabilidades do órgão gerenciador da ata de registro de preços**

6.3.1. Indicação das responsabilidades do órgão gerenciador da ata, nos casos de contratações por Sistema de Registro de Preços – SRP. O rol mínimo abaixo pode ser acrescido com obrigações pertinentes ao objeto da contratação, observando-se sempre o Decreto nº 7.892, de 23 de janeiro de 2013 e suas alterações.

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

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

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

d) Definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:

1. a definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;
2. as regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos 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 pela contratada; e
3. as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a realização de Prova de Conceito, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.
4. **Não será permita adesão à futura Ata de Registro de Preços**, considerando o Decreto 9488/2018, Artigo 22, Parágrafo 10: "*§ 10. É vedada a contratação de serviços de tecnologia da informação e comunicação por meio de adesão a ata de registro de preços que não seja: I - gerenciada pelo Ministério do Planejamento, Desenvolvimento e Gestão; ou II - gerenciada por outro órgão ou entidade e previamente aprovada pela Secretaria de Tecnologia da Informação e Comunicação do Ministério do Planejamento, Desenvolvimento e Gestão.*"

e) Outras obrigações que se apliquem ao objeto da contratação.

7. MODELO DE EXECUÇÃO DO CONTRATO

7.1. Rotinas de Execução

7.1.1. *Da reunião inicial:*

7.1.1.1. *O CONTRATANTE, por intermédio do GESTOR DO CONTRATO, convocará a CONTRATADA, imediatamente após a assinatura do CONTRATO, para reunião de alinhamento de entendimentos e expectativas – ora denominada REUNIÃO INICIAL – com o objetivo de:*

a) *Alinhar a forma de comunicação entre as partes, que deverá ocorrer preferencialmente entre o CONTRATANTE e o PREPOSTO da CONTRATADA;*

b) *Definir as providências necessárias para inserção da CONTRATADA no ambiente de prestação dos serviços;*

c) *Definir as providências de implantação dos serviços;*

d) *Alinhar entendimentos e expectativas quanto aos modelos de execução e de gestão do CONTRATO.*

7.1.1.2. *Na REUNIÃO INICIAL a CONTRATADA deverá:*

a) *Apresentar seu PREPOSTO;*

b) *Apresentar sua equipe técnica que atuará diretamente na prestação dos serviços contratados, com a respectiva documentação de comprovação de atendimento aos perfis exigidos. e*

c) *Realizar apresentação técnica do seu processo de trabalho e das ferramentas para execução dos serviços contratados.*

7.1.1.3. *Havendo necessidade outros assuntos de comum interesse poderão ser tratados na reunião inicial, além dos anteriormente previstos.*

7.1.1.4. *Todas as atas de reuniões e as comunicações entre o CONTRATANTE e a CONTRATADA, assim como todas as demais intercorrências contratuais, positivas ou negativas, serão arquivadas em processo próprio para fins de manutenção do histórico de gestão do CONTRATO.*

7.2. **Quantidade mínima de bens ou serviços para comparação e controle**

7.2.1. Para a perfeita execução do objeto, a CONTRATADA deverá disponibilizar todos os itens nas quantidades determinadas no subitem (3.3.2) deste Termo de Referência promovendo a sua substituição/atualização quando necessário.

7.3. **Mecanismos formais de comunicação**

7.3.1. Na ocasião da Assinatura da Ata, as CONTRATADAS deverão informar os canais de atendimento e suporte por telefone e endereço eletrônico.

7.3.2. A comunicação entre a fiscalização e a CONTRATADA deverá ser realizada formalmente, por meio de Ofício, ou qualquer outra forma que possibilite comprovação nos autos e anotações ou registros no Relatório de Serviços.

7.4. **Manutenção de Sigilo e Normas de Segurança**

7.4.1. A Contratada 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.

7.4.2. A CONTRATADA e seus profissionais envolvidos no projeto deverão seguir os seguintes procedimentos e premissas de segurança envolvidos na execução do objeto:

a) Manter sigilo sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto contratado, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes, sob pena de responsabilidade civil, penal e administrativa.

b) Não veicular publicidade acerca do contrato, salvo se houver prévia autorização do CONTRATANTE.

c) Garantir sigilo e inviolabilidade das conversações realizadas por meio do objeto desta contratação, respeitando as hipóteses e condições constitucionais e legais de quebra de sigilo de telecomunicações.

d) A quebra da confidencialidade ou sigilo de informações obtidas na execução do objeto ensejará a responsabilidade criminal, na forma da lei, sem prejuízo de outras providências nas demais esferas.

7.4.3. A contratada deverá realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos da contratante ou da nova empresa que continuará a execução dos serviços.

8. **MODELO DE GESTÃO DO CONTRATO**

8.1. Para a execução do objeto da presente contratação deverão ser designados os seguintes papéis e respectivas responsabilidades:

a) **Preposto:** representante da Contatada, por ela indicado e formalmente nomeado, responsável por acompanhar a execução do objeto e atuar como interlocutor principal junto à UFMS, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual.

b) **Gestor do Contrato:** é o representante da administração, designado para acompanhar e fiscalizar a execução do contrato, devendo coordenar e comandar todo o processo de fiscalização. Na indicação do Gestor do Contrato, devem ser considerados a compatibilidade com as atribuições do cargo, a complexidade da fiscalização, o quantitativo de contratos por servidor e a sua capacidade para o desempenho das atividades.

O Gestor tem como principais atribuições:

1. acompanhar a execução financeira do contrato;
2. encaminhar as Notas Fiscais atestadas às unidades responsáveis para o pagamento;
3. esclarecer as dúvidas do preposto ou representante da CONTRATADA;
4. informar em tempo hábil, à autoridade competente, eventuais problemas na execução contratual dentre outras atribuições detalhadas no Manual de Gestão e Fiscalização de Contratos da UFMS (Resolução CD nº 193, de 27 de setembro de 2019).

c) **Fiscal Técnico:** profissional de Tecnologia da Informação e Comunicação, preferencialmente lotado na unidade que solicitou a compra, para fiscalizar tecnicamente a execução do objeto, auxiliar os Requisitantes quanto às dúvidas técnicas e interlocuções junto à CONTRATADA, dentre outras atribuições detalhadas no Manual de Gestão e Fiscalização de Contratos da UFMS (Resolução CD nº 193, de 27 de setembro de 2019).

d) **Fiscal Administrativo:** verificar as certidões de regularidade da CONTRATADA, registrar e controlar o saldo do empenho, verificar prazos de entrega, conferir notas fiscais e outros documentos entregues pela CONTRATADA, instruir processo de sanção administrativa com auxílio dos fiscais requisitantes e técnicos quando necessário, dentre outras atribuições a serem detalhadas no Manual de Gestão e Fiscalização de Contratos da UFMS (Resolução CD nº 193, de 27 de setembro de 2019).

e) **Fiscal Setorial:** caberá a qualquer servidor que solicitar a compra de licenças, fiscalizar os bens e serviços contratados, observando os prazos e as obrigações dispostas no Termo de Referência, incluindo atestar o recebimento definitivo dos bens adquiridos que estiverem em conformidade com o objeto contratado, sua marca, modelo e especificações**, solicitar serviços de suporte,** dentre outras atribuições a serem detalhadas no Manual de Gestão e Fiscalização de Contratos da UFMS (Resolução CD nº 193, de 27 de setembro de 2019).

8.2. **RESCISÃO CONTRATUAL**

8.2.1. A rescisão contratual poderá ser:

8.2.1.1. Determinada por ato unilateral e escrito da Administração, nos casos previstos na legislação vigente.

8.2.1.2. Amigável, por acordo entre as partes, reduzida a termo no processo da licitação, desde que haja conveniência para a Administração, devendo ser autorizada por escrito e fundamentada pela autoridade competente.

8.2.1.3. Judicial, nos termos da legislação.

8.2.1.4. A inexecução total ou parcial do contrato enseja a sua rescisão, se houver uma das ocorrências prescritas no art. 78 da Lei nº 8.666, de 21 de junho de 1993.

9. **ESTIMATIVA DO PREÇO DA CONTRATAÇÃO**

9.1. A estimativa de preços total para a presente contratação é de **R$ 583.318,33** (quinhentos e oitenta e três mil trezentos e dezoito reais e trinta e três centavos), para fornecimento por **36** MESES / OU **03** ANOS.

9.2. Os valores foram obtidos por meio das Propostas Comerciais:

9.2.1. Proposta Comercial Empresa WITEC IT Solutions. (SEI nº 2793441)

9.2.2. Proposta Comercial Empresa Microhard Informática LTDA. (SEI nº 2793434)

9.2.3. Proposta Comercial Empresa VTECH Comércio, Serviços e Equipamentos de Informática EIRELI. (SEI nº 2812857)

9.2.4. Consulta Painel de Preços doc SEI 2802959, pelo item 27502 (CATSERV).

9.2.5. Consulta Atas de Pregões realizados com o mesmo objeto - SEI 2793218, 2793226, 2793242, 2793255, 2793282, 2793292, 2793321, 2793332, 2793339, 2793345, 2793362, 2793373, 2793392, 2793400, 2793412, 2793418 e 2793426 onde foram consideradas as médias das propostas apresentadas, convertendo-as para o período demandado pela UFMS (3 ANOS).

9.3. Foi realizado o Documento de Formação de Preços (SEI nº 2802592) visando demonstrar que o valor ofertado nas propostas comerciais encaminhadas estão de acordo com o praticado no mercado.

9.4. O Documento de Formação de Preços foi atualizado (SEI Nº 2834221) para a retirada do item: "Serviço de instalação, transição e configuração de software antivírus", conforme análise e autorização da Direção da AGETIC.

10. EXECUÇÃO ORÇAMENTÁRIA

10.1. A despesa com a execução deste contrato está programada em dotação orçamentária própria do CONTRATANTE, prevista no seu orçamento para o exercício corrente, a ser informado pela PROPLAN.

10.2. Conforme o Parágrafo 2º do Artigo 7º do Decreto 7892/2013: § 2º Na licitação para registro de preços não é necessário indicar a dotação orçamentária, que somente será exigida para a formalização do contrato ou outro instrumento hábil.

10.3. Nos casos de Sistema de Registro de Preços, a fonte de recursos poderá ser informada no momento da contratação.

11. DA VIGÊNCIA DO CONTRATO

11.1. O contrato vigorará por 36 (trinta e seis) meses, contados a partir da data da sua assinatura, limitado a 48 (quarenta e oito) meses, desde que haja preços e condições mais vantajosas para a Administração, nos termos do Inciso II, Art. 57, da Lei nº 8.666, de 1993.

12. DO REAJUSTE DE PREÇOS (QUANDO APLICÁVEL)

12.1. A prorrogação contratual (dentro do prazo dos 48 meses) poderá ocorrer:

12.1.1. Quando os serviços forem prestados regularmente.

12.1.2. A CONTRATADA não tenha sofrido qualquer sanção que a impeça de contratar com a Administração Pública.

12.1.3. A administração tenha interesse na realização/manutenção do serviço.

12.1.4. O valor do contrato permaneça economicamente vantajoso.

12.1.5. A CONTRATADA concorde expressamente com a prorrogação.

12.1.6. Em caso de renovação, os preços contratados das parcelas anuais poderão sofrer reajuste, aplicando-se o Índice de Custos de Tecnologia da Informação - ICTI, conforme Portaria no 6.432 de 11 de julho de 2018, do Ministério do Planejamento, Desenvolvimento e Gestão, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

12.1.7. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE

pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

12.1.8. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

12.1.9. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

12.1.10. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

12.1.11. O reajuste será realizado por apostilamento.

12.1.12. Nas contratações de serviços de Tecnologia da Informação em que haja previsão de reajuste de preços por aplicação de índice de correção monetária, é obrigatória a adoção do Índice de Custos de Tecnologia da Informação – ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada – IPEA. Acesso em: http://www.ipea.gov.br/cartadeconjuntura/index.php/tag/icti/

13. DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

13.1. Regime, Tipo e Modalidade da Licitação

13.1.1. A presente licitação se dará por Pregão, na forma Eletrônica (Pregão Eletrônico), conforme Lei no 10.520 de 17 de julho de 2002, regulamentado pelo Decreto no 10.024 de 20 de setembro de 2019, modalidade obrigatória, do tipo Menor Preço POR LOTE, preferencial utilizado na Administração Pública Federal para aquisição de bens e serviços comuns.

13.1.2. A justificativa para a adoção do Sistema de Registro de Preços se baseia nos Incisos I, II e IV, do Art. 3o, do Decreto 7.892/2013: "I - quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes; II - quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa; e IV - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração".

13.2. Justificativa para a Aplicação do Direito de Preferência e Margens de Preferência

13.2.1. Não se aplica para este certame.

13.3. Critérios de Qualificação Técnica para a Habilitação

13.3.1. Para a definição dos critérios técnicos para seleção do fornecedor, deverão ser observados:

I – a utilização de critérios correntes no mercado;

II – a necessidade de justificativa técnica nos casos em que não seja permitido o somatório de atestados para comprovar os quantitativos mínimos relativos ao mesmo quesito de capacidade técnica;

III – a vedação da indicação de entidade certificadora, exceto nos casos previamente dispostos em normas da Administração Pública;

IV – a vedação de exigência, para fins de qualificação técnica na fase de habilitação, de atestado, declaração, carta de solidariedade, comprovação de parceria ou credenciamento emitidos por fabricantes;

V – a vedação de pontuação com base em atestados relativos à duração de trabalhos realizados pelo licitante, para licitações do tipo técnica e preço; e

VI – a justificativa dos critérios de pontuação em termos do benefício que trazem para a contratante, para licitações do tipo técnica e preço>.

13.4. **Diligências e Provas de Conceito**

13.4.1. Poderão ser realizadas, sempre que necessárias, diligências, para fins de comprovação de atendimento das especificações técnicas ou para dirimir quaisquer outras dúvidas, quando aplicável.

13.4.2. Não será realizada, neste certame, Prova de Conceito (POC) com os licitantes.

13.4.3. É facultado as autoridades que conduzirem a licitação, em qualquer de suas fases, promover diligências com vistas a esclarecer ou a complementar a instrução do processo.

13.5. **Documentação Mínima Exigida**

13.5.1. O licitante deverá encaminhar juntamente com a proposta:

a) Documento no qual declare estar apto a revender licenças de software da *antivírus* ao Governo, bem como prestar o suporte de acordo com as condições, prazos e níveis de serviços especificados no presente Termo de Referência.

b) Declaração que ateste a inexistência da prática de "registro de oportunidade". Essa declaração tem por objetivo garantir o princípio constitucional da isonomia e da seleção da proposta mais vantajosa para a Administração Pública, conforme disposto na Lei nº 8.666, de 1993.

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

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

13.8. Os critérios de qualificação técnica a serem atendidos pelo fornecedor além dos descritos no sub item 5.8- Requisitos de Arquitetura Tecnológica, também devem atender ao preconizado no edital.

13.9. Os critérios de aceitabilidade de preços será o Valor Por Item.

13.10. O critério de julgamento da proposta é o menor preço por item.

13.11. As regras de desempate entre propostas são as discriminadas no edital.

13.12. **Admissão ou Não-Admissão de Consórcio**

13.12.1. A presente licitação não admitirá a participação de empresas em regime de consórcio, vez que o mercado está preparado para atendimento do objeto sem a necessidade de recorrência a parcerias do tipo consórcio.

14. **DA SUBCONTRATAÇÃO**

14.1. Para a presente licitação não será admitida a subcontratação, vez que o mercado está preparado para atendimento do objeto sem a necessidade de recorrer a subcontratação.

15. **ALTERAÇÃO SUBJETIVA**

15.1. 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.

16. **CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO**

16.1. As informações sobre execução contratual estão disponíveis no item 7 deste termo.

16.2. As atividades de gestão e fiscalização da execução contratual serão pautadas também observando a análise dos riscos apresentadas no processo, conforme doc. SEI 2591891.

16.3. A Fiscalização Técnica será realizada de forma a acompanhar e avaliar a execução do objeto nos moldes contratados e, se for o caso, aferir se a quantidade, qualidade, tempo e modo da prestação dos serviços estão compatíveis com os indicadores de desempenho estipulados no item 5 deste termo, bem como na descrição da solução, para efeito de pagamento conforme o resultado, podendo ser auxiliado pela fiscalização pelo público usuário;

16.4. A Fiscalização Administrativa será realizada com o acompanhamento dos aspectos administrativos da execução dos serviços, quanto às obrigações previdenciárias, fiscais e trabalhistas, bem como quanto às providências tempestivas nos casos de inadimplemento;

16.5. O descumprimento das obrigações trabalhistas ou a não manutenção das condições de habilitação pela CONTRATADA poderá dar ensejo à rescisão contratual, sem prejuízo das demais sanções.

16.6. A CONTRATANTE poderá conceder prazo para que a CONTRATADA regularize suas obrigações trabalhistas ou suas condições de habilitação, sob pena de rescisão contratual, quando não identificar má-fé ou a incapacidade de correção.

16.7. O gestor deverá verificar a necessidade de se proceder a repactuação do contrato, inclusive quanto à necessidade de solicitação da contratada.

16.8. O fiscal técnico deverá apresentar ao preposto da CONTRATADA a avaliação da execução do objeto ou, se for o caso, a avaliação de desempenho e qualidade da prestação dos serviços realizada.

16.9. Em hipótese alguma, será admitido que a própria CONTRATADA materialize a avaliação de desempenho e qualidade da prestação dos serviços realizada.

16.10. O representante da Contratante deverá ter a qualificação necessária para o acompanhamento e controle da execução dos serviços e do contrato.

16.11. A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste Termo de Referência.

16.12. A fiscalização de que trata este tópico não exclui nem reduz a responsabilidade da CONTRATADA, 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 da CONTRATANTE ou de seus agentes, gestores e fiscais, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

17. DO RECEBIMENTO E ACEITAÇÃO DO OBJETO

17.1. O prazo de entrega das licenças será de até 10 dias úteis após a assinatura do contrato por parte da UFMS.

17.2. **O recebimento provisório** será realizado pelo fiscal técnico / administrativo ou pela equipe de fiscalização após a confirmação do recebimento das chaves de licenças.

17.3. **O Recebimento definitivo:** compreenderá o ateste da nota fiscal pelo requisitante e poderá ser realizado em data posterior, após a conferência qualitativa das especificações e requisitos solicitados, com base nas exigências especificadas no Termo de Referência. O prazo máximo para o recebimento definitivo será de 10 (dez) dias úteis a partir do recebimento provisório, independentemente de aceite formal pelo requisitante.

17.4. Quando constatada alguma inconformidade com a solução durante o período compreendido entre o recebimento provisório e o recebimento definitivo, a UFMS notificará a CONTRATADA por e-mail ou chamado técnico, que deverá substituir o bem ou serviço em inconformidade num prazo máximo de 5 (cinco) dias úteis contados da notificação. Extensões de prazo não são aplicáveis nesta hipótese.

17.5. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da

Contratada pelos prejuízos resultantes da incorreta execução do contrato, ou, em qualquer época, das garantias concedidas e das responsabilidades assumidas em contrato e por força das disposições legais em vigor.

17.6. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigidos/refeitos /substituídos no prazo fixado pelo fiscal do contrato, às custas da Contratada, sem prejuízo da aplicação de penalidades.

18. **DO PAGAMENTO**

18.1. 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.

18.1.1. 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.

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

18.3. 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. 29 da Lei nº 8.666, de 1993.

18.3.1. 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.

18.4. 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.

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

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

18.7. 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.

18.8. 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.

18.9. 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.

18.10. 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.

18.11. 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.

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

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

18.12.1. 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.

18.13. 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:

EM = I x N x VP, sendo:

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%**

19. ~~**ANTECIPAÇÃO DE PAGAMENTO**~~

19.1. ~~*A Contratada emitirá recibo correspondente ao valor da antecipação de pagamento de R$ ..... (valor por extenso), tão logo ... (incluir condicionante – ex: seja assinado o termo de contrato ou seja prestada a garantia etc.), para que a Contratante efetue o pagamento antecipado.*~~

19.2. ~~*Para as etapas seguintes do contrato, a antecipação do pagamento ocorrerá da seguinte forma:*~~

19.2.1. ~~*R$..... (valor em extenso) quando do início da segunda etapa.*~~

19.3. ~~*Fica a Contratada obrigada a devolver a integralidade do valor antecipado na hipótese de inexecução do objeto.*~~

19.4. ~~*No caso de inexecução parcial, deverá haver a devolução do valor relativo à parcela não-executada do contrato.*~~

~~A previsão dos itens acima é obrigatória caso seja adotado o pagamento antecipado~~

19.5. ~~*A liquidação do recibo relativo ao pagamento antecipado ocorrerá de acordo com as regras do item 10 deste documento.*~~

19.6. ~~*A antecipação de pagamento dispensa o ateste ou recebimento prévio do objeto ou a anterior emissão de Nota Fiscal/Fatura.*~~

19.7. ~~*A emissão da nota fiscal ou fatura referente ao valor antecipado ocorrerá após a execução contratual da parcela respectiva, devendo ser submetida a procedimentos regulares de recebimento e ateste.*~~

19.8. ~~*O pagamento de que trata este item está condicionada à tomada das seguintes providências pela Contratada:*~~

19.8.1. ~~*comprovação da execução da etapa imediatamente anterior do objeto pelo contratado, para a antecipação do valor remanescente;*~~

19.8.2. ~~*prestação da garantia nas modalidades de que trata o art. 56 da Lei nº 8.666/93, no percentual de ...% (até trinta por cento), observando as seguintes disposições:*~~

19.8.2.1. ~~*A garantia deverá ser prestada no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do contratante, contados da assinatura do contrato, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.*~~

19.8.2.2. ~~*A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso, até o máximo de 2% (dois por cento).*~~

19.8.2.3. ~~*O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei n. 8.666 de 1993.*~~

19.8.2.4. ~~*A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger o período contratual.*~~

19.8.2.5. ~~*A garantia assegurará, qualquer que seja a modalidade escolhida, o ressarcimento do valor antecipado, no caso de inexecução total ou parcial do objeto contratual.*~~

19.8.2.6. ~~*A garantia em dinheiro deverá ser efetuada em favor da Contratante, em conta específica na Caixa Econômica Federal, com correção monetária.*~~

19.8.2.7. ~~*Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Economia.*~~

19.8.2.8. ~~*No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.*~~

19.8.2.9. ~~*Será considerada extinta a garantia com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Contratante, mediante termo circunstanciado, de que a Contratada cumpriu as obrigações relativas ao valor que foi antecipado;*~~

19.8.2.10. ~~*emissão de título de crédito pelo contratado, no valor de R$ ... (por extenso);*~~

19.8.2.11. ~~*o título de crédito somente poderá ser utilizado para fins de ressarcimento do valor antecipado, no caso de inexecução total ou parcial do objeto contratual.*~~

19.8.2.12. ~~*Havendo a execução da parcela do objeto contratual referente ao valor antecipado, haverá a devolução do título de crédito à contratada, mediante recibo, o qual será anexado aos autos.*~~

19.8.2.13. ~~*apresentação da seguinte certificação específica do produto ou do próprio contratado fornecedor:*~~

~~...~~

19.9. ~~*O pagamento do valor a ser antecipado ocorrerá respeitando eventuais retenções tributárias incidentes.*~~

20. **GARANTIA DE EXECUÇÃO**

20.1. *Não haverá exigência de garantia contratual da execução, pelas razões abaixo justificadas:*

20.1.1. A garantia não se aplica, pois a prestação de serviço envolve a liberação da licença de uso apenas e o pagamento é realizado somente após a entrega da licença.

20.1.2. A exigência de garantia, como regra, representa um valor que seria agregado às propostas dos licitantes, o que equivale dizer que os custos dessa exigência seriam repassados à própria CONTRATANTE. Portanto, essa exigência vai de encontro à economicidade da contratação.

20.1.3. A exigência da garantia, por conta desses fatores, pode representar diminuição do universo de interessados e ao caráter competitivo do certame.

20.2. ~~*O adjudicatário, no prazo de ..... (.....dias) após a assinatura do Termo de Contrato ou aceite do instrumento equivalente, prestará garantia no valor correspondente a ..... (.....) do valor do Contrato, que será liberada de acordo com as condições previstas neste Edital, conforme disposto no art. 56 da Lei nº 8.666, de 1993, desde que cumpridas as obrigações contratuais.*~~

20.3. ~~Caberá ao contratado optar por uma das seguintes modalidades de garantia:~~

20.3.1. ~~caução em dinheiro ou em títulos da dívida pública, devendo estes ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda;~~

20.3.2. ~~seguro-garantia;~~

20.3.3. ~~fiança bancária.~~

20.4. ~~*A garantia em dinheiro deverá ser efetuada em favor da Contratante, na Caixa Econômica Federal, com correção monetária, em favor do contratante.*~~

20.5. ~~*No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada ou renovada nas mesmas condições.*~~

20.6. ~~*Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a Contratada obriga-se a fazer a respectiva reposição no prazo máximo de ..... (.....) dias úteis, contados da data em que for notificada.* ***Definir o prazo, em caso de prestação de garantia.***~~

20.7. ~~*A Contratante executará a garantia na forma prevista na legislação que rege a matéria.*~~

20.8. ~~*A garantia prestada pelo contratado será liberada ou restituída após a execução do contrato e, quando em dinheiro, atualizada monetariamente. (artigo 56, §4º da Lei nº 8666/93).*~~

21. **DAS SANÇÕES ADMINISTRATIVAS**

21.1. Comete infração administrativa nos termos da Lei nº 10.520, de 2002, e da Resolução 143 CD, de 28 de agosto de 2019 da UFMS a Contratada que, na fase de execução contratual:

21.2. **Não celebrar o contrato:**

21.2.1. recusar ou deixar de enviar documento necessário para comprovar a capacidade de assinatura do contrato/ata de registro de preços;

21.2.2. recusar ou deixar de assinar contrato/ata de registro de preços dentro do prazo de convocação;

21.2.3. recusar ou deixar de confirmar o recebimento da Nota de Empenho referente ao contrato/ata de registro de preços

21.3. **Sanções aplicáveis para as condutas 21.2.1, 21.2.2, 21.2.3:**

21.3.1. Impedimento de licitar e contratar com a União pelo prazo de até 04 meses;

21.3.2. Descredenciamento do Sicaf pelo prazo de até 5 (cinco) anos;

21.3.3. Multa de 1% do valor total do contrato/ata de registro de preços, por dia de descumprimento, no limite máximo de 15%

21.4. **Apresentar documentação falsa:**

21.4.1. omitir informações em documentos exigidos no certame;

21.4.2. adulterar documento, público ou particular;

21.4.3. encaminhar contrato/ata de registro de preços adulterada.

21.5. **Sanções aplicáveis para as condutas 21.4.1, 21.4.2, 21.4.3:**

21.5.1. Impedimento de licitar e contratar com a União pelo prazo de até 3 (três) anos;

21.5.2. Descredenciamento do Sicaf pelo prazo de até 3 (três) anos;

21.5.3. Multa de 20% do valor total do contrato/ata de registro de preços;

21.6. **Ensejar o retardamento da execução do objeto contratual:**

21.6.1. praticar qualquer ação ou omissão que prejudique o bom andamento da execução do contrato.

21.6.2. deixar de prestar garantia quando exigido.

21.7. **Sanções aplicáveis para a conduta 21.6.1:**

21.7.1. Impedimento de licitar e contratar com a União pelo prazo de até 1 (um) ano.

21.7.2. Multa de 15% do valor total do contrato/ata de registro de preços

21.8. **Sanções aplicáveis para a conduta 21.6.2:**

21.8.1. Impedimento de licitar e contratar com a União pelo prazo de até 01 ano;

21.8.2. Descredenciamento do Sicaf pelo prazo de até 01 (ano) ano;

21.8.3. Multa de 1% do valor total do contrato/ata de registro de preços, por dia de descumprimento, no limite máximo de 15%

21.9. **Falhar na execução do contrato**

21.9.1. entregar materiais com características diversas daquelas constantes na proposta, no contrato ou na ata de registro de preços;

21.9.2. deixar de substituir materiais com características diversas daquelas constantes na proposta, no contrato ou na Ata de Registro de Preços, no prazo estipulado pela Administração;

21.9.3. atrasar a entrega de quaisquer dos itens solicitados por prazo superior a 30 (trinta) dias;

21.9.4. recusar-se ou deixar de fornecer quaisquer dos itens contratados/registrados;

21.9.5. deixar de entregar documentação fundamental para execução contratual.

21.10. **Sanções aplicáveis para as condutas 21.9.1, 21.9.2, 21.9.3, 21.9.4, 21.9.5:**

21.10.1. Impedimento de licitar e contratar com a União pelo prazo de 06 meses;

21.10.2. Multa de 1% do valor total do material, por dia de descumprimento, no limite máximo de 10%; e/ou Multa de 10% do valor total do material contratado;

21.10.3. Descredenciamento do SICAF pelo prazo de até 05 anos;

21.11. **Fraudar na execução do contrato**

21.11.1. elevar arbitrariamente os preços;

21.11.2. fornecer, como verdadeiro ou perfeito, material falsificado ou deteriorado;

21.11.3. entregar um material por outro;

21.11.4. alterar substância, qualidade ou quantidade do material fornecido;

21.11.5. tornar, por qualquer modo, injustamente, mais onerosa a proposta ou a execução do contrato;

21.12. **Sanções aplicáveis para as condutas 21.11.1, 21.11.2, 21.11.3, 21.11.4, 21.11.5:**

21.12.1. Impedimento de licitar e contratar com a União pelo prazo de até 5 (cinco) anos;

21.12.2. Multa de 20% do valor total do evento não cumprido

21.13. **Comportar-se de modo inidôneo**

21.13.1. realizar atos comprovadamente de má- fé ou com dolo;

21.13.2. participar de empresa constituída com a finalidade de burlar penalidade aplicada anteriormente;

21.13.3. não realizar o recolhimento do FGTS dos empregados e das contribuições sociais previdenciárias;

21.13.4. não realizar o pagamento do salário, do vale-transporte e do auxílio alimentação;

21.14. **Sanções aplicáveis para as condutas 21.13.1, 21.13.2, 21.13.3, 21.13.4:**

21.14.1. Impedimento de licitar e contratar com a União pelo prazo de 3 anos;

21.14.2. Multa de 20% do valor total do evento não cumprido; e/ou Multa de 1% do valor total da obrigação, por dia de descumprimento, no limite máximo de 20%

21.15. **Cometer fraude fiscal**

21.15.1. fazer declaração falsa sobre seu enquadramento fiscal;

21.15.2. omitir informações em suas notas fiscais;

21.15.3. falsificar ou alterar notas fiscais

21.16. **Sanções aplicáveis para as condutas 21.15.1, 21.15.2, 21.15.3:**

21.16.1. Impedimento de licitar e contratar com a União pelo prazo de 5 anos;

21.16.2. Multa de 20% do valor total do evento não cumprido.

21.16.3. 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;

21.17. 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 10520/2002, subsidiariamente a Lei 8.666, de 1993, e Lei nº 9.784, de 1999.

21.18. 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.

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

21.20. 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.

21.21. 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.

21.22. 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.

21.23. 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.

21.24. 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.

21.25. As penalidades serão obrigatoriamente registradas no SICAF. Para efeito de aplicação de multas, às infrações são atribuídos graus, de acordo com as tabelas 1 e 2:

Tabela 1.

GRAU/ID	CORRESPONDÊNCIA
1	1% AO DIA SOBRE O VALOR MENSAL DO CONTRATO
2	1,05% AO DIA SOBRE O VALOR MENSAL DO CONTRATO
3	1,08% AO DIA SOBRE O VALOR MENSAL DO CONTRATO
4	2% AO DIA SOBRE O VALOR MENSAL DO CONTRATO
5	3,2% AO DIA SOBRE O VALOR MENSAL DO CONTRATO

Tabela 2.

INFRAÇÃO		
ITEM	**DESCRIÇÃO**	**GRAU**
1	SUSPENDER OU INTERROMPER, SALVO MOTIVO DE FORÇA MAIOR OU CASO FORTUITO, OS SERVIÇOS CONTRATUAIS POR DIA E POR UNIDADE DE ATENDIMENTO	5
PARA OS ITENS A SEGUIR, DEIXAR DE:		
2	CUMPRIR DETERMINAÇÃO FORMAL OU INSTRUÇÃO COMPLEMENTAR DO ÓRGÃO FISCALIZADOR, POR OCORRÊNCIA	2
3	CUMPRIR QUAISQUER DOS ITENS DO EDITAL E SEUS ANEXOS NÃO PREVISTOS NESTA TABELA DE MULTAS, APÓS REINCIDÊNCIA FORMALMENTE NOTIFICADA PELO ÓRGÃO FISCALIZADOR, POR ITEM E POR OCORRÊNCIA	3

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

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

21.26.2. tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

21.26.3. demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

21.27. 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.

21.27.1. Nos casos em que a empresa inadimplente entregar os produtos durante o processo para sua penalização, fica facultado à UFMS receber o produto e reduzir a multa de acordo com os critérios:

a) O dano causado à Administração.

b) O caráter educativo da pena.

c) A reincidência como maus antecedentes.

d) A proporcionalidade.

21.27.2. Deixando de aplicar a penalidade de impedimento de licitar, de acordo com o prejuízo sofrido pela Administração.

21.28. 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.

21.28.1. No caso de aplicação da penalidade de Multa, após a notificação da decisão da autoridade competente, os contratos costumam estabelecer que as multas devem ser recolhidas aos cofres da União em um prazo máximo de 10 (dez) dias.

21.28.1.1. Juntamente com a notificação da decisão da autoridade competente, deve ser encaminhado também a Guia de Recolhimento da União. Caso decorra o prazo e não seja efetivado o pagamento, deverá ser providenciado o desconto da garantia contratual apresentada pelo contratado, se houver, ou então das faturas de serviços a serem pagas pela Administração, no caso de prestação de serviços.

21.28.1.2. Caso o contratado não tenha apresentado garantia contratual e nem tenha valores a receber do contratante, deve-se providenciar a inscrição do débito na Dívida Ativa da União em encaminhamento a ser realizado pela Pró-reitoria junto às unidades competentes dentro do respectivo processo sancionador.

21.28.1.3. A penalidade de multa deve ter sua inscrição realizada no Sicaf, sem a necessidade de publicação no Diário Oficial da União

21.29. 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.

21.30. 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.

21.31. 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.

21.32. 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.

21.33. As penalidades serão obrigatoriamente registradas no SICAF.

22. **DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E APROVAÇÃO**

22.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 191, de 03 de março de 2021 - doc SEI (2434826).

22.2. Conforme o §6º do art. 12 da IN SGD/ME nº 01, de 2019, o Termo de Referência ou Projeto Básico será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC e aprovado pela autoridade competente.

_____ **Integrante Requisitante** *Anaximandro Bastos Pacheco* *Siape nº 31383046*	_____ **Integrante Técnico** *Rodrigo Pereira de Almeida* Siape nº 2298310	_____ **Integrante Administrativo** *Laércio Reindel* Siape nº 11449947

Autoridade Máxima da Área de TIC
_____ *Luciano Gonda* *Diretor Agetic*

Aprovo,

Autoridade Competente
_____ *Luciano Gonda* *Diretor Agetic*

Adaptado, seguindo modelo atualizado em junho de 2021- Modelo Extraído da página https://www.gov.br/governodigital/pt-br/contratacoes/templates-e-listas-de-verificacao

Documento assinado eletronicamente por **Rodrigo Pereira de Almeida**, **Auxiliar em Administração**, em 07/10/2021, às 15:59, conforme horário oficial de Mato Grosso do Sul, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Laercio Reindel**, **Assistente em Administração**, em 07/10/2021, às 16:03, conforme horário oficial de Mato Grosso do Sul, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Anaximandro Bastos Pacheco**, **Analista de Tecnologia da Informação**, em 07/10/2021, às 16:22, conforme horário oficial de Mato Grosso do Sul, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Luciano Gonda**, **Diretor(a)**, em 07/10/2021, às 16:28, conforme horário oficial de Mato Grosso do Sul, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufms.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2825855** e o código CRC **303CDFEE**.

Referência: Processo nº 23104.004333/2021-88 SEI nº 2825855