DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA

1. INTRODUÇÃO

Em conformidade com a Instrução Normativa n° 01 de 04 de abril de 2019, emitida pela SGD/ME, a fase de Planejamento da Contratação terá início com o Documento de Oficialização da Demanda - DOD, a cargo da área requisitante da solução.

2. IDENTIFICAÇÃO DO REQUISITANTE

Área Requisitante: Coordenadoria de Segurança da Informação - CSI / DOS / STI	
Nome: Carlos Vinícius Braga dos Santos	**Matrícula/SIAPE: 1654133**
Cargo: Analista de TI	**Função: Coordenadoria de Segurança da Informação**
E-mail Institucional: carlosvbs@unb.br	**Telefone: 3107-0019**

3. IDENTIFICAÇÃO DA DEMANDA

Aquisição de Solução Corporativa de Antivírus Multiplataforma com Gerência Centralizada (solução de antivírus), bem como serviços de instalação, configuração, treinamento e suporte técnico presencial (on-site) 24x7 para atender as necessidades de segurança do ambiente computacional da Universidade de Brasília.

4. MOTIVAÇÃO/JUSTIFICATIVA

É fundamental dispor de uma solução centralizada que proteja as informações armazenadas nos computadores, servidores de rede e nas estações de trabalho da UnB contra a atuação de vírus, Cavalos de Troia, spywares, malwares, programas diversos de códigos maliciosos e proteção contra vazamentos ou perda de dados.

A solução permitirá que as áreas responsáveis pela administração dos recursos de Infraestrutura de Tecnologia da Informação da UnB mantenham os níveis exigidos de segurança das informações trafegadas, processadas ou armazenadas nos computadores desktop, estações de trabalho e servidores, assegurando os controles e políticas necessárias para certificar que tais informações estão sendo acessadas e manipuladas somente por pessoas autorizadas, conforme as melhores práticas.

Fonte de Recurso: Recursos do Tesouro Nacional (Ação: 20RK - Funcionamento de Instituições Federais de Ensino Superior)

5. RESULTADOS ESPERADOS

Resultado 1	Atendimento a todas as especificações técnicas;
Resultado 2	Ser uma alternativa de baixo custo, porém vantajosa à Universidade de Brasília e que componha o seu catálogo de serviços
Resultado 3	Prover a Secretaria de Tecnologia da Informação de capacidade de atendimento às demandas técnicas de segurança no que diz respeito a desktops, estações de trabalho e servidores, e de forma indireta contribuir com a segurança da RedUnB, protegendo o tráfego de informações e os dados;
Resultado 4	Aumentar a confiabilidade dos usuários que acessam os serviços por meio de desktops e estações de trabalho e servidores, e de forma indireta para os usuários de recursos computacionais diversos da Universidade de Brasília.

6. ALINHAMENTO ESTRATÉGICO

Alinhamento ao PDTIC	
Objetivo Estratégico 1:	A presente contratação encontra-se alinhada aos objetivos estratégicos descritos no Plano Diretor de Tecnologia da Informação e Comunicação referente ao ciclo 2019-2022. Conforme o referido documento disponível em http://sti.unb.br/images/Normas/PDTIC_2019-2022_v4.pdf, de acordo com o disposto nas páginas 41 a 42, alguns dos dezesseis objetivos do CPD são: "OETIC7. Promover atualização tecnológica dos sistemas e da infraestrutura de TIC da UnB; OETIC8. Garantir a conectividade, qualidade e segurança dos serviços de TICs;
Objetivo Estratégico 2:	OETIC8. Garantir a conectividade, qualidade e segurança dos serviços de TICs;
Objetivo Estratégico 3:	OETIC9. Garantir a transparência e a segurança da informação e comunicação;
Objetivo Estratégico 4:	OETIC12. Atender à legislação pertinente à área de TI;
Objetivo Estratégico 5:	OETIC15. Garantir o efetivo atendimento às demandas de TIC e melhorar a disponibilidade dos sistemas e serviços de TIC" (sic);
Objetivo Estratégico 6:	A necessidade de manutenção dos softwares de antivírus atualizados também é reforçada pelo Centro de Tratamento de Incidentes de Redes do Governo (CTIR), por meio do documento Alerta No. 07/2020, disponível em https://www.ctir.gov.br/arquivos/alertas/2020/alerta_especial_2020_07_atualizacao_ataques_de_ransomware.pdf (ataques de ransomware) e extensível a outros males, para todos os órgãos e entidades da administração pública como medida de mitigação para a ameaça de sequestro de dados.

Alinhamento ao PAC 2021	
Nº do Item no PAC:	**10752**
Descrição do Item no PAC:	"software" aplicação: informática, tipo: client server suite, características; adicionais: antivírus corporativo, atualização contínua e suporte. Aquisição de solução corporativa de antivírus multiplataforma com gerência centralizada com serviços de instalação, configuração, treinamento e suporte técnico presencial (on-site) 24x7.

7. INDICAÇÃO DO INTEGRANTE PARA COMPOR EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Nome: Marcos Vinicius Linhares Castro	**Matrícula/SIAPE:** 1676387
Cargo: Analista de TI	**Lotação:** STI / DOS / CSI
E-mail: mvlcastro@unb.br	**Telefone:** 3107-0019

8. QUANTIDADE DE SERVIÇOS/PRODUTOS A SEREM CONTRATADOS

SoluçãoCorporativa de Antivírus Multiplataforma com Gerência Centralizada (solução de antivírus) para 4000 estações; Console de gerenciamento centralizado para instalação em servidores e acesso remoto para duas ou mais unidades; Serviços de instalação, configuração e manutenção; Treinamento; Suporte técnico presencial (on-site) 24x7.

Este documento deverá ser assinado por:

- Requisitante.

Documento assinado eletronicamente por **Carlos Vinicius Braga dos Santos**,

Coordenador(a) da Coordenadoria de Segurança da Informação da Secretaria de Tecnologia da Informação, em 28/04/2021, às 10:29, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

A autenticidade deste documento pode ser conferida no site http://sei.unb.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **6604977** e o código CRC **E2D59721**.

Referência: Processo nº 23106.017186/2021-96 SEI nº 6604977

Endereço: Campus Universitário Darcy Ribeiro - Gleba A, , Brasília/DF, CEP 70910-900
Telefone: e Fax: @fax_unidade@ - http://www.unb.br

Universidade de Brasília

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

PROCESSO Nº 23106.017186/2021-96

PROJETO:

AQUISIÇÃO DE SOLUÇÃO CORPORATIVA DE ANTIVÍRUS MULTIPLATAFORMA COM GERÊNCIA CENTRALIZADA.

BRASÍLIA, SETEMBRO DE 2021.

INTRODUÇÃO
Este Estudo Técnico Preliminar - ETP tem o objetivo de verificar a viabilidade técnica e financeira para a contratação de solução corporativa de antivírus multiplataforma com gerenciamento centralizado no âmbito da Universidade de Brasília e fornecer as informações necessárias para subsidiar o respectivo processo de contratação.

1. NECESSIDADE DA CONTRATAÇÃO

Uma solução corporativa de antivírus, que vem integrada com a solução de antimalware, é um software de computador (estação de trabalho e servidor) que serve para prevenir, detectar e remover software malicioso. Contudo, com o surgimento de outros tipos de ameaças como malwares, ransomwares, trojans, dialers, adware, spyware, rootkits, backdoors, phishing, dentre outros, as soluções de antivírus começaram a fornecer proteção estendida (antimalware, anti-spyware, firewall, dentre outros) e também para plataformas diferentes de sistemas operacionais.

Cada fabricante possui solução de antivírus com funcionalidades que podem ser variadas conforme o ambiente computacional do cliente. Com a intenção de que a solução de segurança de endpoint seja completa e satisfatória para o ambiente computacional da Universidade de Brasília, a contratação deve ter, junto ao licenciamento, o serviço de suporte técnico sob demanda com o fabricante, atualizações da solução para versões atuais, ou seja, últimas versões estáveis, e treinamento para a equipe que fará a administração da solução.

A solução de segurança de endpoint vigente na Universidade de Brasília é mantida e atualizada, sendo adquirida no ano de 2016 e documentada pelo SEI UnB No. 23106.098192/2016-79, documento 0717569 (contrato 178/2016), cujo vencimento ocorreria em janeiro/2020. O referido contrato afirma em sua cláusula quinta que a duração tem vigência de 36 meses com a possibilidade de renovação até o limite de 60 (sessenta) meses, desde que comprovada a vantagem para a administração pública conforme inciso II, do artigo 57 da lei Nº 8666/93. Levando em consideração o período inicial de 36 meses a sua renovação poderia ter o prazo estendido em até 24 meses de tal modo a alcançar o prazo máximo de 60 meses. Em 2019 foram realizados estudos e se comprovou a viabilidade de renovação do referido contrato, a qual de fato ocorreu por meio de aditamento descrito e apresentado no Termo Aditivo do Contrato DAF/DCA/CES 4868033, de 10 de janeiro de 2020 (disponível no mesmo processo). A renovação estendeu o prazo do contrato em 24 meses, com data de encerramento em 10 de janeiro de 2022, com respectiva publicação no DOU em 14 de janeiro do mesmo ano. Uma vez que não será possível a renovação do atual contrato, torna-se necessário realizar processo licitatório visando uma nova contratação.

2. ALINHAMENTO ENTRE A CONTRATAÇÃO DA SOLUÇÃO E OS PLANOS ESTRATÉGICOS DA INSTITUIÇÃO

A presente contratação encontra-se alinhada ao Plano de Desenvolvimento Institucional (PDI) referente ao ciclo 2018-2022. Conforme o referido documento disponível em http://deg.unb.br/images/dtg/cil/legislacoes/Plano_de_Desenvolvimento_Institucional_2018-2022.pdf, de acordo com o disposto nas páginas 280 a 282, um dos cinco objetivos da STI é "1. Garantir o efetivo atendimento às demandas de TI e melhorar a disponibilidade dos sistemas e serviços de TI" (sic). A necessidade de manutenção dos softwares de antivírus atualizados também é reforçada pelo Centro de Tratamento de Incidentes de Redes do Governo (CTIR), por meio do documento Alerta No. 07/2017 (ataques de ransomware) e extensível a outros males, para todos os órgãos e entidades da administração pública como medida de mitigação para a ameaça de sequestro de dados.

Outro requisito para a contração de solução deste tipo encontra-se na Política de Segurança da Informação e Comunicação da Universidade de Brasília – PoSIC/UnB, aprovada pela resolução Nº 004/2018 da Câmara de Planejamento e Administração (CPLAD), disponível em http://www.dpo.unb.br/images/phocadownload/cplad/Resolucoes-3-e-4-CPLAD.pdf, que objetiva limitar a exposição ao risco a níveis que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações e comunicações das atividades fundamentais de ensino, pesquisa e extensão da UnB.

A contratação pretendida está alinhada também aos projetos em curso dentro da REDUnB (Rede de Dados da Universidade de Brasília) para modernização do ambiente computacional, como uma camada de segurança para as novas funcionalidades que estão sendo implantadas, como a expansão da rede wi-fi, a implantação do IPV6, a implantação de novos sistemas, com o crescimento no acesso à internet e número de colaboradores da Universidade de Brasília.

3. RESULTADOS PRETENDIDOS

A Universidade de Brasília tem o objetivo de contratar uma solução corporativa de antivírus multiplataforma com gerenciamento centralizado, para atender as necessidades de proteção contra códigos maliciosos na rede computacional administrativa da universidade.

Com isso, a solução contratada deve atingir os seguintes resultados:

- Atender todas as especificações técnicas;
- Ser uma alternativa de baixo custo, porém vantajosa à Universidade de Brasília, compondo seu catálogo de serviços;
- Fazer com que a Secretaria de Tecnologia da Informação possa ter a capacidade de atender às necessidades técnicas de segurança de forma direta para a rede computacional administrativa e de forma indireta para o ambiente da REDUnB, dando proteção no tráfego de informações e retenção de dados;
- Aumentar a confiabilidade direta dos usuários que utilizam os serviços da rede computacional administrativa e de forma indireta dos usuários dos outros recursos computacionais da Universidade de Brasília.

4. REQUISITOS DA CONTRATAÇÃO

Das Condições Ambientais de Operação

A Solução de Segurança será configurada na REDUnB, mais especificamente em estações de trabalho administrativas e equipamentos servidores da Universidade de Brasília, visando à proteção em tempo real, com o regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano), dos componentes, serviços e informações que fazem parte do parque computacional da Universidade de Brasília (estações administrativas).

Dos Componentes

Requisitos Funcionais:

1. Possuir suporte às arquiteturas de 32 e 64 bits;

2. Possuir suporte às plataformas Microsoft e Linux;
3. Possuir suporte ao modo Server Core;
4. Possuir suporte a sistemas virtualizados;
5. Deve ter um único agente;
6. Gerenciado por uma console única;
7. Deve ser capaz de selecionar, no mínimo, dois modos de proteção;
8. Deve ter recurso para armazenamento de arquivos removidos ou desinfetados para posterior análise, verificação ou restauração (quarentena);
9. O download das atualizações a partir do servidor centralizado deve ser capaz de buscar em outras bases ou repositórios para se manter atualizado;
10. Deve emitir relatórios customizáveis pelos usuários.

Requisitos Não-Funcionais:

1. Deve usar baixo poder computacional do cliente ao fazer instalação nas estações de trabalho ou servidores;
2. Os processos de proteção em tempo real e varredura contra vírus e outras ameaças escaneamento de vírus não devem impactar no desempenho dos clientes;
3. As atualizações de software, bibliotecas e definições não devem apresentar impacto para os clientes;
4. Não deve emitir alertas desnecessário para os usuários.

5. LEVANTAMENTO DA DEMANDA

Contratação conforme tabela abaixo (a tabela não trata apenas de licenças):

Item	Produto	Quantidade
1	Solução de segurança (software corporativo de antivírus multiplataforma) para estações de trabalho e servidores no ambiente administrativo da REDUnB (LICENÇAS)	4000
2	Software servidor de gerenciamento centralizado da solução de antivírus corporativo multiplataforma (LICENÇAS)	01
3	Serviço de suporte on-site 24x7x365	36 meses
4	Treinamento na solução – 30 horas (mínimo)	10

Período:

- Itens 1, 2 e 3 por 36 meses de suporte on-site e garantia;
- Item 4 deve ser realizado entre 60 e 120 dias a partir da assinatura do contrato.

Para estimar a demanda de licenças de uso, foi realizada consulta ao anuário estatístico da UnB, acessado em junho de 2021 e disponível em https://anuario-estatistico-unb-2020.netlify.app/geral.html#indicadores-gerais-de-desempenho-da-unb-2011-a-2019 no seu item "2.15 Indicadores gerais de desempenho 2011-2019 – quadro de pessoal", o número de docentes ativos é de 2594 professores, somando-se aos técnicos em 3233 funcionários, totalizando 5827 (cinco mil, quinhentos e noventa e quatro) servidores. O universo de estações de trabalho no âmbito administrativo, se aproxima de 3400 (três mil e quatrocentas) unidades e a gerência destas pela solução de Active Directory é uma meta perseguida a curto prazo. Por sua vez, o quantitativo de servidores criados dentro do ambiente computacional da Secretaria de Tecnologia da Informação já passa de 550 (quinhentos e cinquenta) unidades de máquinas virtuais, destas cerca de 130 em plataforma Microsoft Windows, o que pelo montante já se alinha à cobertura da quantidade de licenças a serem contratadas com margem de segurança para crescimento, e também mais de 420 servidores na plataforma Linux, que também devem ter algum meio de rotina

de antivírus para o perfeito funcionamento. Os computadores servidores são necessários para a realização da missão institucional da STI, uma vez que possibilitam garantir a disponibilidade, confiabilidade, integridade e autenticidade dos dados e dos serviços realizados no âmbito da Universidade de Brasília (UnB) por meio de seus sistemas administrativos e acadêmicos.

Como referência pode-se aplicar os dados de abril de 2019, obtidos da solução atual de antivírus – a qual contempla o ambiente administrativo da universidade – em que constava o total de 2635 (dois mil e seiscentos e trinta e cinco) estações de trabalho gerenciadas e 919 (novecentos e dezenove) estações de trabalho não gerenciadas, totalizando 3554 (três mil quinhentos e cinquenta e quatro) unidades.

O ambiente dentro da REDUnB gerenciado e controlado pela solução Active Directory da Microsoft possui em torno de 2000 (duas mil) estações de trabalho, conforme levantamento realizado em junho de 2021, sendo o restante dos equipamentos não ingressos no referido serviço de diretório, o que não exclui a necessidade de manutenções e instalações em modo stand-alone, não sendo necessário que a estação de trabalho esteja no ambiente gerenciado. A variação do número de estações fora do domínio se dá devido ao momento atual da universidade, que vem passando pela redução do trabalho na modalidade presencial devido às medidas de isolamento social demandadas para combate à epidemia do Covid-19. Com o gradativo retorno ao trabalho em modalidade presencial, estes números tendem a retornar aos indicativos de 2019.

A Secretaria de Tecnologia da Informação, assumindo que terá um crescimento mínimo de 5% ao ano na quantidade de estações de trabalho gerenciadas ou controladas pela solução corporativa de antivírus, justifica a necessidade de adquirir o quantitativo de licenças solicitadas no processo de aquisição.

6. ANÁLISE DE SOLUÇÕES

Para dar seguimento com as avaliações das soluções disponíveis é necessário que se sigam três passos durante a elaboração de um estudo técnico preliminar:

1. A busca de soluções que estejam em utilização por outros órgãos públicos para cessão;

2. A procura por software que desempenhe a função desejada no portal do software público;

3. A busca em soluções disponíveis no mercado.

Um software da natureza do objeto deste estudo, ou uma solução corporativa de antivírus multiplataforma com gerenciamento centralizado, são arranjos de software de alta complexidade e com muitas funções incorporadas, não sendo desenvolvidos sob encomenda: são adquiridos por meio de licenças e necessitam de atualizações periódicas, sendo corriqueiro receberem mais de uma atualização ao dia. Assim, a busca por outro órgão público que possa ceder um software deste tipo, tendo desenvolvido solução semelhante não apresentou resultados positivos, uma vez que as licenças são exclusivas para os respectivos contratantes. Assim a procura seguiu para a busca de uma alternativa no portal Software Público Brasileiro, disponível em https://softwarepublico.gov.br. O referido site lista diversos softwares livres que atendem às necessidades de modernização da administração pública de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios e são compartilhados sem ônus, resultando na economia de recursos públicos e constituindo um recurso benéfico para a administração pública e para a sociedade. Em buscas realizadas no referido portal, não foram encontradas soluções livres que possam ser utilizadas no âmbito da universidade. Dado o resultado negativo, as alternativas se voltam a soluções disponíveis de mercado.

As opções para solução corporativa de antivírus disponíveis no mercado se apresentam em grande quantidade e muitas versões. Para facilitar a escolha existem entidades internacionais de consultoria que classificam os fabricantes conforme a sua desenvoltura no mercado. Uma dessas empresas, Gartner Group, classifica as empresas fornecedoras de produtos e serviços de tecnologia por meio de um quadrante baseado em dois eixos: Completeness of Vision (completude de visão) e Ability to Execute (Habilidade para executar). A imagem abaixo mostra o resultado de um dos levantamentos anuais realizados pela consultoria para soluções centralizadas de antivírus e antispam, ou Endpoint Protection Platform (EPP):

Nesta figura, obtida em https://www.microsoft.com/security/blog/wp-content/uploads/2021/05/Picture1-4.png, apresentam-se como os líderes (Leaders) as empresas que demonstram resultados satisfatórios nos eixos de visão de mercado e capacidade de execução apresentadas pelo Gartner. As desafiadoras (Challengers) são empresas que possuem produtos consolidados, porém ainda não atingiram a visão necessária para o pleno atendimento das necessidades do mercado. As visionárias (Visionaries) são empresas que investem em recursos inovadores que serão significativos na próxima geração de produtos, no entanto ainda apresentam a necessidade de aprimoramento de seus processos para o sucesso das operações. Por fim, as empresas conhecidas como nicho de mercado (Niche Player) oferecem soluções satisfatórias, porém ainda apresentam limitações para atuação em uma maior abrangência no mercado.

Assim, as empresas que figuram nestes quadrantes são empresas consolidadas e capazes de fornecer as soluções de acordo com as demandas de mercado, sobretudo aquelas situadas nos quadrantes visionárias, desafiadoras e líderes.

Baseados na imagem, pode-se concluir que os fornecedores situados nos três quadrantes listados no parágrafo anterior apresentam potencial elevado de atendimento às necessidades da contratante, desde que obedecidos os requisitos técnicos e operacionais previstos nas especificações e necessidades da contratada.

Cabe lembrar ainda que o quadrante é resultado de levantamentos periódicos realizados pela Gartner, assim se deve destacar o caráter dinâmico da colocação das empresas nas posições, as quais variam a cada avaliação.

Comparativo entre soluções de mercado

Com vista a verificar os fabricantes e fornecedores de solução corporativa de antivírus, no quesito de proteção, performance e usabilidade, abaixo seguem dois levantamentos realizados pela instituição AV-TEST, (https://www.av-test.org) conhecida mundialmente por avaliar soluções de antivírus de diversos fabricantes. Ela apresenta periodicamente comparativos entre diversas soluções em versões para usuários domésticos (home users) e também as destinadas a empresas (business users). Para o presente estudo foram consideradas as versões destinadas a uso empresarial.

Ainda sobre os testes mencionados no parágrafo anterior, cabe destacar os seus respectivos critérios, com três notas atribuídas conforme aspectos de proteção (protection), desempenho (performance) e usabilidade (usability), sendo a pontuação final a soma destes quatro, e dispostas na última coluna. A organização define ainda os critérios para escolha dos melhores produtos, sendo aplicado aqueles que atingem a nota final igual ou acima de 17,5 pontos.

A análise a seguir foi extraída do site da referida entidade (https://www.av-test.org/en/news/15-security-solutions-for-corporate-networks), datada de 23 de abril de 2019 e referente a testes realizados em janeiro e fevereiro do mesmo ano, e tendo como referência os mesmos parâmetros, obteve-se um comparativo semelhante, com 15 (quinze) soluções de segurança para redes corporativas. A figura abaixo mostra o resultado do teste:

BUSINESS WINDOWS CLIENT

15 corporate solutions put to the test under Windows 10

AV-TEST

Manufacturer	Product	AV-TEST Certificate	Protection (max. 6 pts)	Performance (max. 6 pts)	Usability (max. 6 pts)	Overall Points Total (max. 18)
F-Secure	PSB Computer Protection	✓	6.0	6.0	6.0	18.0
Kaspersky Lab	Endpoint Security	✓	6.0	6.0	6.0	18.0
Symantec	Endpoint Protection	✓	6.0	6.0	6.0	18.0
Symantec	Endpoint Protection Cloud	✓	6.0	6.0	6.0	18.0
Avast	Business Antivirus Pro Plus	✓	6.0	5.5	6.0	17.5
Bitdefender	Endpoint Security	✓	6.0	5.5	6.0	17.5
Kaspersky Lab	Small Office Security	✓	6.0	5.5	6.0	17.5
McAfee	Endpoint Security	✓	6.0	5.5	6.0	17.5
Sophos	Endpoint Security and Control	✓	6.0	5.5	6.0	17.5
Bitdefender	Endpoint Security (Ultra)	✓	6.0	5.0	6.0	17.0
ESET	Endpoint Security	✓	5.5	5.5	6.0	17.0
Microsoft	Windows Defender Antivirus	✓	6.0	5.5	5.5	17.0
Trend Micro	OfficeScan	✓	5.5	5.5	6.0	17.0
Seqrite	Endpoint Security	✓	5.5	6.0	5.0	16.5
G Data	AntiVirus Business	✓	5.5	4.5	6.0	16.0

AV-TEST January/February 2019

www.av-test.org

De acordo com a figura, acima, a qual descreve os principais fornecedores e seus respectivos produtos disponíveis no mercado, pode-se observar os nove produtos escolhidos pelo site, bem como seus respectivos fabricantes. As pontuações obtidas

mostram que os melhores produtos apresentam uma diferença de 2 (dois) pontos da menor para a maior nota, e observa-se também uma diferença de 0,5 (meio ponto) do conjunto das melhores soluções apontadas. A pequena diferença indica o nível semelhante das soluções, baseadas nos critérios da instituição avaliadora.

Complementando a análise anterior, que foi extraído do site da mesma entidade (https://www.av-test.org/en/news/18-corporate-solutions-put-to-the-test/), datado de 24 de agosto de 2020 e referente a testes realizados em maio e junho do mesmo ano, e tendo como referência os mesmos parâmetros, obteve-se um comparativo semelhante, com 18 (dezoito) soluções de segurança para redes corporativas. A figura abaixo mostra o resultado do teste:

BUSINESS WINDOWS CLIENT

18 corporate solutions
under Windows 10 put to the test

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Manufacturer	Product	AV-TEST Certificate	Protection (max. 6 pts)	Performance (max. 6 pts)	Usability (max. 6 pts)	Overall Points Total (max. 18)
F-Secure	PSB Computer Protection		6.0	6.0	6.0	18.0
Kaspersky	Endpoint Security		6.0	6.0	6.0	18.0
Microsoft	Defender Antivirus		6.0	6.0	6.0	18.0
Symantec	Endpoint Protection		6.0	6.0	6.0	18.0
Avast	Business Antivirus Pro Plus		6.0	5.5	6.0	17.5
Bitdefender	Endpoint Security		6.0	5.5	6.0	17.5
G Data	AntiVirus Business		6.0	5.5	6.0	17.5
McAfee	Endpoint Security		6.0	5.5	6.0	17.5
Seqrite	Endpoint Security		6.0	6.0	5.5	17.5
Bitdefender	Endpoint Security (Ultra)		6.0	5.0	6.0	17.0
Check Point	Endpoint Security		6.0	5.0	6.0	17.0
ESET	Endpoint Security		6.0	5.0	6.0	17.0
FireEye	Endpoint Security		5.5	6.0	5.5	17.0
Sophos	Intercept X Advanced		5.5	5.5	6.0	17.0
Trend Micro	Apex One		5.0	6.0	6.0	17.0
VMware	Carbon Black Cloud		6.0	4.0	6.0	16.0
Cylance	Protect		4.5	6.0	4.0	14.5
Webroot	SecureAnywhere		3.0	5.0	4.0	12.0

AV-TEST May/June 2020

www.av-test.org

Levando em conta que os critérios foram os mesmos da avaliação anterior, e baseada nos mesmos critérios, é possível notar que uma quantidade maior de soluções atingiu o critério para “melhor produto” (nota igual ou maior a 17,5 pontos). A tabela a seguir mostra os produtos e suas notas:

	Fabricante	Produto	Nota
1	F-Secure	PSB Computer Protection	18,0
2	Kaspersky	Endpoint Security	18,0
3	Microsoft	Defender Antivirus	18,0
4	Symantec	Endpoint Protection	18,0
5	Avast	Business Antivirus Pro Plus	17,5
6	Bitdefender	Endpoint Security	17,5
7	G Data	AntiVirus Business	17,5

8	McAfee	Endpoint Security	17,5
9	Seqrite	Endpoint Security	17,5
10	Bitdefender	Endpoint Security (Ultra)	17,0
11	Check Point	Endpoint Security	17,0
12	ESET	Endpoint Security	17,0
13	FireEye	Endpoint Security	17,0
14	Sophos	Intercept X Advanced	17,0
15	Trend Micro	Apex One	17,0
16	VMware	Carbon Black Cloud	16,0
17	Cylance	Protect	14,5
18	Webroot	SecureAnywhere	12,0

De acordo com a figura e a tabela acima, a qual do mesmo modo das anteriores descreve os principais fornecedores e seus respectivos produtos, pode-se observar que dos 18 (dezoito) produtos aprovados pelo site, 9 (nove) foram selecionados como os melhores, seguindo o mesmo critério da seleção anterior, ou seja, 17,5 (dezessete e meio) pontos. As pontuações obtidas mostram que os produtos aprovados apresentam uma diferença de 6 (seis) pontos da menor para a maior nota, e observa-se também uma diferença de 0,5 (meio ponto) do conjunto das melhores soluções apontadas, com a diferença indicando o nível semelhante das soluções.

A terceira análise, extraída do site da mesma organização (https://www.av-test.org/en/news/16-security-solutions-for-corporate-users-in-a-6-month-endurance-test/) apresenta um informativo de 17 de fevereiro de 2021, e é referente a testes de resistência realizados entre julho a dezembro de 2020:

Manufacturer	Product	Protection (max. 6 pts)	Performance (max. 6 pts)	Usability (max. 6 pts)	Overall Points Total (max. 18)
Kaspersky	Endpoint Security	6.0	6.0	6.0	18.0
Microsoft	Defender Antivirus	6.0	6.0	6.0	18.0
Symantec	Endpoint Security Complete	6.0	6.0	6.0	18.0
Trend Micro	Apex One	6.0	6.0	6.0	18.0
F-Secure	PSB Computer Protection	6.0	5.8	6.0	17.8
AhnLab	V3 Endpoint Security	6.0	6.0	5.7	17.7
ESET	Endpoint Security	6.0	5.7	6.0	17.7
Bitdefender	Endpoint Security	6.0	5.8	5.8	17.6
Avast	Business Antivirus Pro Plus	6.0	5.5	6.0	17.5
G Data	AntiVirus Business	6.0	5.5	6.0	17.5
McAfee	Endpoint Security	6.0	5.5	6.0	17.5
Seqrite	Endpoint Security	5.8	5.7	5.8	17.3
Sophos	Intercept X Advanced	5.7	5.5	5.8	17.0
Bitdefender	Endpoint Security (Ultra)	6.0	4.7	5.8	16.5
FireEye	Endpoint Security	4.7	5.7	6.0	16.4
VMware	Carbon Black Cloud	5.5	3.7	5.8	15.0

Pela figura acima pode-se observar a comparação de 16 (dezesseis) soluções, e neste ranking onze produtos atingiram a referida classificação. A tabela a seguir mostra os produtos e suas notas:

	Fabricante	Produto	Nota
1	Kaspersky Lab	Endpoint Security	18,0
2	Microsoft	Defender antivirus	18,0
3	Symantec	Endpoint Protection Cloud	18,0
4	Trend Micro	Apex One	18,0
5	F-Secure	PSB Computer Protection	17,8
6	Ahn Lab	V3 Endpoint Security	17,7
7	ESET	Endpoint Security	17,7
8	Bitdefender	Endpoint Security	17,6
9	Avast	Business Antivirus Pro Plus	17,5
10	G Data	AntiVirus Business	17,5
11	McAfee	Endpoint Security	17,5
12	Seqrite	Endpoint Security	17,3
13	Sophos	Intercept X Advanced	17,0
14	Bitdefender	Endpoint Security (Ultra)	16,5
15	FireEye	Endpoint Security	16,4
16	VMware	Carbon black Cloud	15,0

De acordo com a figura e a tabela acima, a qual do mesmo modo das anterior descreve os principais fornecedores e seus respectivos produtos, pode-se observar

que dos 16 (dezesseis) produtos aprovados pelo site, 11 (onze) foram selecionados como os melhores, seguindo o mesmo critério das seleções anteriores, ou seja, 17,5 (dezessete e meio) pontos. As pontuações obtidas mostram que os produtos aprovados apresentam uma diferença de 3 (três) pontos da menor para a maior nota, e observa-se também uma diferença de 0,5 (meio ponto) do conjunto das melhores soluções apontadas, com a diferença indicando o nível semelhante das soluções.

Em relação às tabelas acima é importante observar que alguns fabricantes não figuravam na lista anterior (exemplo Cylance), e com um dos últimos colocados (F-Secure) agora figurando nos quatro primeiros da lista. O mesmo pode ser dito de outros fabricantes que antes atingiram notas maiores e nesta avaliação ocupam posição inferior. É possível concluir que, tal como na análise de quadrantes feita pela Gartner, o comportamento dinâmico dos fabricantes e suas soluções faz com que os produtos tenham sua relevância alterada a cada avaliação.

Baseado nos levantamentos realizados pode-se concluir também que constam neles os principais fornecedores de solução corporativa de antivírus, e que, de forma semelhante ao levantamento realizado pelo Gartner, que os produtos listados nos rankings possuem potencial de atendimento aos requisitos definidos pela contratada, desde que atendam às especificações técnicas definidas neste documento de estudo técnico preliminar.

7. ESCOLHA E JUSTIFICATIVA PARA A SOLUÇÃO MAIS ADEQUADA

Continuar oferecendo segurança para a Infraestrutura de TI da Universidade de Brasília.

Oferecer maior rapidez no tratamento dos riscos que envolvam estações de trabalho e servidores da estrutura computacional da Universidade de Brasília.

Permitir o controle de dispositivos não permitidos na REDUnB e mitigar em grande parte os riscos de infecções na tramitação de dados na rede.

Ofertar melhor suporte ao parque computacional da Universidade de Brasília, pois é necessária uma solução corporativa de antivírus que atenda a sistemas operacionais multiplataforma (Windows e Linux) e em versões distintas, pois este é o cenário comumente encontrado na REDUnB. Tal solução auxiliará na remoção, caso necessária, da solução existente hoje na universidade e deve possuir uma gerência centralizada funcional e de fácil gerenciamento.

A administração de uma solução corporativa de antivírus é mais simples e eficiente devido ao seu gerenciamento centralizado, uma vez que a manutenção de todas as estações de trabalho e servidores se torna complexa em função da estrutura computacional da Universidade de Brasília, com isso a necessidade de se ter uma solução corporativa centralizada.

A administração centralizada promove à equipe que administra a solução corporativa de antivírus a confiança de que todas as estações de trabalho e servidores estarão com o mesmo nível de segurança, com isso trazendo maior confiabilidade e padronização.

A contratação desta solução visa ofertar maior garantia à Universidade de Brasília quanto a aplicabilidade de uma política em busca de integridade das informações, processos e demais objetos que possam ser violados mediante ataques de trojans, vírus e quaisquer espécies de pragas virtuais, bem como proteger informações sigilosas e essenciais que possam ser furtadas ou perdidas acidentalmente.

Com a ampliação constante dos casos de violações cibernéticas como invasões e também o aumento de casos de ransomware (vírus de resgate), quaisquer vulnerabilidades são exploradas caso não sejam, em tempo, corrigidas. Com a crescente utilização da Internet, os processos organizacionais e informações ficam mais expostas o que por si só já requer a adoção de tecnologias mais avançadas de proteção, incluindo a prospecção dessas vulnerabilidades e suas imediatas contramedidas.

A solução corporativa de antivírus é essencial para a segurança das informações que são trabalhadas, armazenadas e trafegadas no ambiente REDUnB, representando um grande risco para este ambiente a falta de cobertura por solução desta natureza.

8. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Para que a solução seja considerada viável para adoção na universidade, devem ser considerados os requisitos do item D deste documento, uma vez que os recursos descritos mencionam gerenciamento centralizado dos clientes em estações e servidores, bem como funcionamento em plataformas Windows e Linux, agente único, repositório central de atualizações e capacidade de armazenamento centralizado de eventos e geração de relatórios customizados.

Uma das soluções que não atende aos itens descritos é a solução Microsoft Windows Defender Antivirus. Ela é considerada inviável por não ser uma solução multiplataforma, ou seja, a mesma só funciona em sistemas operacionais Microsoft, mais precisamente em Windows 10. Além disto, esta solução não dispõe de uma console de gerenciamento centralizado, conforme informado pela própria Microsoft em 21 de outubro de 2020, conforme texto disponível na url https://docs.microsoft.com/pt-br/windows/security/threat-protection/windows-firewall/windows-firewall-with-advanced-security: "Embora o Windows Defender do Painel de Controle de Firewall possa proteger um único dispositivo em um ambiente doméstico, ele não fornece recursos de segurança ou gerenciamento centralizados suficientes para ajudar a proteger o tráfego de rede mais complexo encontrado em um ambiente empresarial típico."

Outras soluções que apresentem as mesmas características também devem ser consideradas inviáveis se não apresentarem os requisitos no item D deste documento.

9. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

1-Cálculo dos Custos Totais de Propriedade:

Solução Viável 1
Custo Total de Propriedade – Memória de Cálculo
Trend Micro – Período 48 meses. Valor Unitário: R$133,50. Considerando o quantitativo de 2100 licenças, ao preço unitário de R$ 133,50 o valor total da proposta é de R$ 280.350,00. Valor mensal do contrato (48 meses): R$ 5.840,63. Para o cenário da universidade, considerando o valor unitário de R$ 133,50 para um total de 4000 unidades, o total resulta em R$534.000,00; considerando o tempo de contrato de 48 meses, o custo mensal fica em torno de R$11.125,00.

Solução Viável 2
Custo Total de Propriedade – Memória de Cálculo
Kaspersky – Período 48 meses. Valor Unitário: R$125,60. Considerando o quantitativo de 5.139 licenças, ao preço unitário de R$ 125,60 o valor total da proposta é de R$ 645.458,40. Valor mensal do contrato (48 meses): R$ 13.447,05. Para o cenário da universidade, considerando o valor unitário de R$ 125,60 para um total de 4000 unidades, o total resulta em R$502.400,00; considerando o tempo de contrato de 48 meses, o custo mensal fica em torno de R$10.466,67.

Solução Viável 3
Custo Total de Propriedade – Memória de Cálculo
Kaspersky Endpoint Security for Business Advanced – Período 36 meses. Valor Unitário:

R$98,18.

Considerando o quantitativo de 1900 licenças, ao preço unitário de R$ 98,18 o valor total da proposta é de R$ 186.542,00. Valor mensal do contrato (36 meses): R$ 5.181,72.

Para o cenário da universidade, considerando o valor unitário de R$ 98,18 para um total de 4000 unidades, o total resulta em R$392.720,00; considerando o tempo de contrato de 36 meses, o custo mensal fica em torno de R$10.908,89.

2-Mapa Comparativo dos Cálculos para os Custos Totais de Propriedade

O comparativo para as três soluções de mercado, bem como os seus comparativos anuais estão dispostos abaixo:

Descrição	Estimativa de TCO ao longo dos anos				Total
	Ano 1	Ano 2	Ano 3	Ano 4	
Trend Micro	133.500,00	133.500,00	133.500,00	133.500,00	534.000,00
Kaspersky	125.600,04	125.600,04	125.600,04	125.600,04	502.400,16
Kaspersky	130.906,67	130.906,67	130.906,67	-	392.720,00

10. DESCRIÇÃO DA SOLUÇÃO DE TI COMO UM TODO

Requisitos Mínimos para a Solução

A solução corporativa de antivírus multiplataforma deve ser fornecida juntamente com o serviço de implantação e configuração do sistema, o respectivo suporte técnico on-site e as atividades de transferência tecnológicas e de conhecimento da solução. Todas as funcionalidades da solução de segurança (função de antivírus, anti-spyware, controle de dispositivos, dentre outros) para estações de trabalho e servidores deverão ser entregues com as funcionalidades totais da solução contratada para uso no ambiente administrativo da REDUnB.

A empresa contratada deverá fazer a instalação e configuração da solução adotada nas instalações e infraestrutura da contratante, compreendendo a instalação de servidores para o gerenciamento centralizado em ambiente virtualizado (console de gerenciamento) e também a instalação e configuração (deployment) dos clientes (endpoints) para servidores e estações de trabalho já disponíveis na solução atual (em produção), bem como a adaptação e/ou transferência das tarefas e políticas em uso da solução anterior, tomadas as devidas providências para mitigar e minimizar eventuais impactos no ambiente administrativo da REDUnB.

As licenças a ativar em endpoints e servidores de gerência deverão ser flutuantes, ou seja, quando um equipamento (computador / estação de trabalho ou servidor) for substituído ou formatado, a licença deverá ser realocada a outro equipamento ou associada novamente à máquina antiga, conforme o caso.

A solução deverá ser implantada na localização determinada pela Secretaria de Tecnologia da Informação da Universidade de Brasília, em ambiente virtualizado, sendo que na gerência da solução implantada devem ser ativadas todas as licenças adquiridas.

Em resumo, a solução corporativa de antivírus a ser contratada, bem como os serviços atrelados a esta solução, devem ser entregues de modo a prover segurança na camada de usuário, mitigando riscos capazes de impactar a produtividade nas atividades laborais dos colaboradores da Universidade de Brasília e degradar o desempenho dos sistemas e do ambiente administrativo da REDUnB.

Especificações Técnicas da Solução

Assim, a solução que será implantada deve prestar os serviços com os seguintes requisitos mínimos, conforme especificações contidas no **Anexo SEI nº 7293842.**

11. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

Não haverá parcelamento do objeto, uma vez que este objeto é único para solução apresentada.

O não parcelamento se justifica ainda no fato de que o suporte técnico e treinamento

são serviços complementares e que sendo realizados de forma desconectada pode gerar à Universidade de Brasília o paradoxo de conflito de garantias entre fornecedores.

12. PROVIDÊNCIAS PARA ADEQUAÇÃO DO AMBIENTE DA INSTITUIÇÃO

Existe a necessidade da Universidade de Brasília adquirir e atualizar alguns sistemas operacionais de estações de trabalho de usuários que não possuem mais suporte como sistemas operacionais Microsoft Windows Vista. Contudo, essa necessidade não impacta na implantação da solução na maior parte do parque computacional da universidade.

13. INDICAÇÃO DE ORÇAMENTO ESTIMADO

Tendo como referência a contratação de solução corporativas de antivírus multiplataforma com gerenciamento centralizado efetuadas por outros órgãos da administração pública, segue abaixo diversos levantamentos com o resumo das recentes contratações e o valor gasto com esses contratos. Esses dados foram levantados no sistema do Ministério da Economia, chamado de Painel de Preços. Para as propostas apresentadas a seguir, seguem-se diversas informações como a descrição resumida dos objetos dos certames, as quantidades, os preços unitários, o número da compra e as descrições do órgão contratante e seu número UASG. Ao final de cada tabela, segue também as informações como média, mediana e o menor preço das propostas. Os dados ao final da tabela serão utilizados para critério da mediana. Em seguida é apresentado 4 levantamentos, o primeiro deles para compras realizadas em 2018 e os demais no ano de 2019:

Levantamento com contratos realizados no ano de 2018:

	QNT.	PREÇO	EMPRESA	COMPRA	UASG / ÓRGÃO	DATA
1	50	26,95	HTI Tecnologia	00002/18	925798 / Coren-MT	05/02/2018
2	20.000	34,00	ISH Tecnologia	00047/18	090027 / TRF Sec. 1a REG/DF	19/10/2018
3	50	44,90	Konttato Informática	00006/18	155884 / IFBA	11/04/2018
4	300	51,34	EsyWorld Sistemas	62174/18	113204 / SAE – IRD/RJ	25/09/2018
5	2.000	80,50	Qualitek Tecnologia	00103/18	060001 / STM	12/12/2018
6	250	108,00	Arrobanet Soluções em Tecnologia	00027/18	090010 / J.F. 1a Instância - AL	30/11/2018
7	850	134,70	Microhard Informática	00022/18	926306 / Câm. Mun. Belo Horizonte	09/07/2018
Média		68,63				
Mediana		51,34				
Menor preço		26,95				

Segundo levantamento, realizado em outubro de 2019:

Data: 23/04/2019 09:00

Pregão: 162019

UASG: 925980 - Ministério Público do Estado do Pará

Objeto: Licença de Software Antivírus para Estações de Trabalho com Gerenciamento Central da SOLUÇÃO e suporte e garantia de evolução por 36 meses. Licenças perpétuas de uso de Software

Quantidade: 2500 unidades

	DESCRIÇÃO	PREÇO	EMPRESA
1	ESET Endpoint Protection	21,34	GLOBAL TRAVEL E TECNOLOGIA DA INFORMACAO LTDA - ME
2	Software Antivírus	45,56	ADIK SOFTWARE LTDA - ME
3	Software Antivírus	64,00	FUTURE TECHNOLOGIES INFORMATICA SA
4	F-Secure - Business Suite Premium	70,00	S G SOLUCOES TECNOLOGICAS LTDA
5	F-Secure - Business Suite Premium	89,98	RCZ SOLUCOES EM INFORMATICA LTDA - ME
6	Software Antivírus	100,00	FAST SECURITY TECNOLOGIA DA INFORMACAO LTDA - ME
7	Software Antivírus	119,44	BCS ELETRONICOS LTDA
8	KES (Kaspersky) for Business	134,98	4F SOLUCOES EM TECNOLOGIA LTDA
9	Kaspersky	200,00	QUALITEK TECNOLOGIA LTDA - ME
10	Bitdefender	200,00	Securisoft do Brasil LTDA
11	Software Antivírus	1500,00	PA LIMPEZA, CONSERVACAO, ADMINISTRACAO, SEGURANCA, PESS
Média		231,39	
Mediana		100,00	
Menor preço		21,34	

O terceiro levantamento, realizado em outubro de 2019:

Data: 09/07/2019 10:13

Pregão: Nº Pregão:22019

UASG: 749000 - Ministério da Defesa - Comando da Marinha

Objeto: Contratação do serviço de upgrade de licenças da solução antivírus da Kaspersky, atualmente em uso na Marinha do Brasil (MB). Período 3 anos

Quantidade: 40000

	DESCRIÇÃO	PREÇO	EMPRESA
1	KES (Kaspersky) for Business	43,53	EsyWorld Sistemas e Informática LTDA
2	KES (Kaspersky) for Business	43,54	MICROHARD INFORMATICA LTDA
3	KES (Kaspersky) for Business	44,14	ITGX SISTEMAS LTDA-ME
4	KES (Kaspersky) for Business	44,15	REAL DIGITAL SERVICOS E SOLUCOES EM TECNOLOGIA EIRELI
5	KES (Kaspersky) for Business	110,5	JOSE MURILO NOGUEIRA JUNIOR-ME
6	KES (Kaspersky) for Business	190	TECSOLUTI COMERCIO E SOLUCOES LTDA-ME
7	KES (Kaspersky) for Business	300	PHDS SERVICOS DE INFORMATICA LTDA-ME
Média		110,84	
Mediana		44,15	
Menor preço		43,53	

O quarto levantamento, realizado em outubro de 2019:

Data: 03/07/2019 10:03

Pregão: 62019

UASG: 158157 - MINISTÉRIO DA EDUCAÇÃO - IFRJ

Objeto: Contratação de serviços de Licenciamento de software antivírus para prover proteção dos equipamentos (desktops, servidores, tablets e notebooks) incluindo atualizações de versões, gerenciamento centralizado, licença de uso de software, implantação, treinamento, garantia de atualização contínua e suporte técnico on-site

Quantidade: 2000

DESCRIÇÃO	PREÇO	EMPRESA
Software Antivírus	30,90	GLOBAL TRAVEL TECNOLOGIA DA INFORMAÇÃO LTDA-ME
Software Antivírus	31,00	Esyworld Sistemas e Informática LTDA
Software Antivírus	31,95	QOS TECNOLOGIA E SERVICOS LTDA -EPP
Software Antivírus	39,75	GLOBAL TECH SOLUCOES TECNOLOGICAS - LTDA ME
KES (Kaspersky) for Business	52,50	4F SOLUCOES EM TECNOLOGIA LTDA
Software Antivírus	61,50	BCS ELETRONICOS LTDA
KES (Kaspersky)	61,84	PRIME TECHNOLOGY SECURITY LTDA-EPP
Software Antivírus	130,00	MP HABERLI TECNOLOGIA-ME
Software Antivírus	350,00	Securisoft do Brasil LTDA
Software Antivírus	500,00	PHDS SERVICOS DE INFORMATICA LTDA-ME
Média	128,94	
Mediana	57,00	
Menor preço	30,90	

Em resumo, com base nos quatro levantamentos listados anteriormente os critérios obtidos foram:

Levantamentos	**1**	**2**	**3**	**4**	**Geral**
Média	68,63	231,39	110,84	128,94	145,46
Mediana	51,34	100,00	44,15	57,00	64,00
Menor preço	26,95	21,34	43,53	30,90	21,34

Importante lembrar que a última coluna (geral) consiste nos valores de média, mediana e menor preço de todas as propostas dos quatro levantamentos.

De acordo com o Art. 5º da IN SDG/ME Nº 73, de 5 de agosto de 2020, temos as três formas citadas para realizar o cálculo para a estimativa de preço, média, mediana e menor preço. A mediana foi usada como critério para realização de cálculos.

Para os valores de menor, maior mediana e mediana geral, as estimativas da solução apresentam os seguintes valores:

Produto: Solução de segurança para estações de trabalho e servidores de rede

Produto: Solução de segurança para estações de trabalho e servidores de rede		
Critérios	Quantidade	Valor Estimado para 36 meses
Menor mediana	4000	(4000 * R$44,15) = R$ 176.600,00
Maior mediana	4000	(4000 * R$100,00) = R$ 400.000,00
Mediana geral	4000	(4000 * R$64,00) = R$ 256.000,00

Assim, baseados nos valores de menor e maior mediana, o valor de aquisição pode ficar entre R$176.600,00 e R$400.000,00, com uma estimativa de R$256.000,00 tomando por base a mediana geral.

14. DECLARAÇÃO DA VIABILIDADE OU NÃO DA CONTRATAÇÃO

O planejamento foi elaborado em conformidade com legislações e instruções normativas vigentes, bem como conformidade com os requisitos técnicos necessários ao cumprimento das necessidades e objeto da aquisição. O objeto está de acordo com as necessidades técnicas, operacionais e estratégicas da Universidade de Brasília.

Com isso, a solução atende adequadamente às demandas da Universidade de Brasília, todos os benefícios pretendidos estão adequados e dentro dos custos previstos. Os riscos envolvidos podem ser administrados e a área requisitante dará prioridade aos elementos relacionados nesse ETP.

15. ESTRATÉGIA DE INDEPENDÊNCIA DA UNB EM RELAÇÃO À CONTRATADA

A Secretaria de Tecnologia da Informação adotará a forma de repasse de

conhecimento entre os integrantes da equipe que gerenciará a solução contratada. O repasse de conhecimento se dará na forma de capacitação ou treinamento na solução e seus recursos. A referida atividade de treinamento deverá ser capaz de dotar aos participantes a capacidade de instalar, operar e manter todos os módulos e recursos da solução fornecida pela contratada. Serão capacitados 10 (dez) integrantes da equipe responsável pelo gerenciamento da solução contratada e os mesmos realizarão anualmente uma capacitação para os demais integrantes da equipe. Juntamente com o repasse de conhecimento, a Secretaria de Tecnologia da Informação deverá realizar o armazenamento da documentação dos produtos contratados em ambiente digital.

16. ESTRATÉGIA PARA TRANSIÇÃO E ENCERRAMENTO CONTRATUAL

Faltando 30 (trinta) dias para o término do contrato, caso o ambiente da solução corporativa de antivírus não esteja integralmente atualizado, a contratada deverá entregar a versão final dos produtos contratados juntamente com toda a documentação de gerenciamento dos produtos. Até o último dia de vigência do contrato, caso venha a surgir qualquer atualização estável ou problema técnico é obrigação da contratada efetuar a atualização e/ou solução do problema junto à equipe técnica da contratante.

Ao final da vigência do contrato da solução corporativa de antivírus a contratada deverá acompanhar a atualização e instalação da solução de contrato futuro, efetuando a desinstalação de softwares como endpoints, agentes e outros sob sua responsabilidade, até que todas as estações de trabalho e servidores passem pelo processo de desinstalação da solução contratada em encerramento de contrato, independentemente do tempo necessário para a remoção dos softwares instalados. Poderão ser utilizadas ferramentas automatizadas de desinstalação, com a devida comprovação de baixo impacto no funcionamento das demais soluções da contratante.

17. ESTRATÉGIA PARA CONTINUIDADE EM EVENTUAL INTERRUPÇÃO DE CONTRATO

A Secretaria de Tecnologia da Informação da Universidade de Brasília está passando pela implementação dos processos e melhores práticas do framework ITIL, dentre eles o processo de Gerenciamento da Continuidade de Serviço.

Com isso, a continuidade do serviço deverá ser suportada pela infraestrutura e corpo técnico da Secretaria de Tecnologia da Informação, a qual deverá ter o conhecimento necessário para dar continuidade ao serviço caso ocorra algum incidente que afete a entrega do mesmo.

Com uma eventual interrupção de contrato poderão ocorrer desdobramentos de diversos cenários, os quais levariam em consideração as etapas do processo de contratação, implantação, manutenção e encerramento da solução, acarretando em impactos como a interrupção dos serviços da solução adquirida e a impossibilidade de troca da solução devido à ausência de recursos financeiros e tempo hábil para um novo certame licitatório.

Recursos materiais e humanos necessários à continuidade do negócio

Recursos materiais:

- Infraestrutura tecnológica está apta para suportar os serviços contratados;
- Estações de trabalho estão interligadas pela rede computacional, grande parte sendo gerenciada pela estrutura de diretórios da UnB e possui acesso à internet;
- Rede de internet para atualização dos produtos contratados disponível para todas as estações de trabalho e servidores.

Recursos Humanos:

- Gestor do contrato ficará sob a responsabilidade da Coordenadoria de Segurança da Informação (STI/DOS/CSI);
- Fiscal técnico do contrato ficará sob a responsabilidade da Coordenadoria de Segurança da Informação (STI/DOS/CSI), área requisitante da solução;

- Fiscal administrativo ficará sob a responsabilidade da Coordenadoria de Gestão e Planejamento da STI (STI/CGESP);
- Gerente de projetos ficará sob a responsabilidade do setor de Divisão de Operações e Serviços (STI/DOS);
- Corpo técnico encarregado do gerenciamento da solução é composto por 10 (dez) servidores públicos da área de TI;

Caso ocorra alguma interrupção no fornecimento de suporte da contratada, a equipe técnica da Secretaria de Tecnologia da Informação deverá suportar o serviço até a solução do problema, conforme as possibilidades técnicas, operacionais e de conhecimento.

18. MODELO DE GESTÃO E EXECUÇÃO DO OBJETO

A contratada deverá efetuar os serviços de instalação, configuração, teste e disponibilização (customização) da solução corporativa de antivírus no ambiente físico da Universidade de Brasília.

Os serviços de instalação, configuração e implantação da solução corporativa de antivírus deverão ser efetuados de forma a não comprometer o funcionamento dos serviços, recursos ou equipamentos atualmente em operação.

Os serviços e entregas da solução corporativa de antivírus deverão ser iniciados e executados somente após prévio agendamento com a Universidade de Brasília.

Para a execução destes serviços, fica estabelecido o horário de funcionamento da Universidade de Brasília, das 07h às 20h, de segunda a sexta-feira. Caso haja a necessidade de execução dos serviços durante finais de semana ou mesmo em horários distintos ao estabelecido, será necessária prévia negociação com a área responsável.

Em caso de ocorrerem situações sanitárias que venham a demandar o isolamento e distanciamento social dos integrantes da STI, contratante e contratada deverão elaborar estratégias para implantar a solução por meio remoto, respeitando as eventuais limitações e necessidades de ambas as partes, e levando em consideração também as resoluções administrativas.

A Contratada deverá realizar a implantação da última versão estável dos módulos e de seus agentes nas estações de trabalho e na rede.

A Contratada deverá instalar o Software Servidor de Gerenciamento do Antivírus em sua última versão estável.

Na conclusão de cada uma das etapas deverá ser apresentado um relatório que será aprovado pela a equipe da Universidade de Brasília, que emitirá um termo de aceitação da fase.

19. ANÁLISE DE RISCOS

A análise de Riscos está disponível em documento separado, no documento “Mapa de Gerenciamento de Riscos”, que segue no processo SEI! correspondente a esta contratação.

20. DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

Assim, diante do exposto acima, entendemos ser **VIÁVEL** a contratação da solução demandada. Os estudos preliminares evidenciaram que a contratação pretendida mostra-se ser técnica, econômica e estrategicamente necessária. Diante do exposto, declara-se ser viável a contratação pretendida. Contudo, ressalta-se que possíveis informações não constantes nesse documento serão detalhadas com maior riqueza no Termo de Referência, e que esse documento visa apenas a demonstração da viabilidade de contratação da solução pretendida. "

21. ASSINATURAS

A Equipe de Planejamento da Contratação foi instituída pelo ato da diretoria da Secretaria de Tecnologia da Informação nº 018/2021, de 26 de abril de 2021, e alterado pelos atos subsequentes respectivos, ou seja, Ato 019/2021 de 29 de abril de 2012, Ato 049/2021 de 09 de setembro de 2021 e Ato 057/2021 de 21 de outubro de 2021.

Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC:

INTEGRANTE REQUISITANTE	INTEGRANTE TÉCNICO
Marcos Vinícius Linhares Castro Analista de TI SIAPE 1676387	David de Souza Cid Analista de TI SIAPE 2085504

22. APROVAÇÃO E DECLARAÇÃO DE CONFORMIDADE

Aprovação do documento e declaração expressa da autoridade máxima da Área de TIC quanto à adequação dos estudos realizados neste artefato aos ditames da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019.

Aprovo este Estudo Técnico Preliminar e atesto sua conformidade às disposições da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019.

AUTORIDADE MÁXIMA DA ÁREA DE TIC (OU AUTORIDADE SUPERIOR, SE APLICÁVEL - § 3º do art. 11)
JACIR LUIZ BORDIM Secretário de TI da UnB SIAPE 14894991

Documento assinado eletronicamente por **Marcos Vinicius Linhares Castro**, **Analista de Tecnologia da Informação da Secretaria de Tecnologia da Informação**, em 26/10/2021, às 15:10, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

Documento assinado eletronicamente por **David de Souza Cid**, **Analista de Tecnologia da Informação da Secretaria de Tecnologia da Informação**, em 26/10/2021, às 16:09, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

Documento assinado eletronicamente por **Jacir Luiz Bordim**, **Secretário(a) de Tecnologia da Informação**, em 28/10/2021, às 09:40, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

A autenticidade deste documento pode ser conferida no site http://sei.unb.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7293814** e o código CRC **925B4495**.

Referência: Processo nº 23106.017186/2021-96 SEI nº 7293814

Especificações Técnicas da Solução

Assim, a solução que será implantada deve prestar os serviços com os seguintes requisitos mínimos:

1. Características Gerais da Solução

1.1.1. Deve possuir suporte às arquiteturas 32-bits e 64-bits;
1.1.2. Deve possuir capacidade de instalação e pleno funcionamento dos módulos solicitados em estações de trabalho com no mínimo 3GB de memória RAM;
1.1.3. Deve suportar as seguintes plataformas Microsoft (clientes/desktops):
  1.1.3.1. Windows 10 e superiores;
  1.1.3.2. Windows 8.1;
  1.1.3.3. Desejável suporte ao Windows 8;
  1.1.3.4. Desejável suporte ao Windows 7;
1.1.4. Deve suportar as seguintes plataformas Microsoft (servidores):
  1.1.4.1. Windows Server 2019 e superiores;
  1.1.4.2. Windows Server 2016 e superiores;
  1.1.4.3. Windows Server 2012 R2;
  1.1.4.4. Windows Server 2012;
  1.1.4.5. Windows Storage Server 2012;
  1.1.4.6. Desejável suporte ao Windows Server 2008 R2 nas versões Standard, Datacenter, Enterprise ou Web;
  1.1.4.7. Desejável suporte ao Windows Server 2003 em todas as suas versões;
1.1.5. Deve inclusive suportar o modo Server Core;
1.1.6. Deve suportar, **pelo menos a função de antivírus**, nas seguintes distribuições de Linux:
  1.1.6.1. Red Hat 6 e superiores, 32 e/ou 64bits;
  1.1.6.2. SUSE Server/Desktop 12 e superiores, 64bits (desejável suporte também para versões desktop, bem como versões com 32 bits);
  1.1.6.3. Ubuntu 16.04 e superiores, 64bits (desejável suporte também para versões desktop, bem como versões com 32 bits);
  1.1.6.4. CentOS 6.x e superiores, 64bits (desejável suporte também para versões com 32 bits);
  1.1.6.5. Debian 9 e superiores, 64bits (desejável suporte também para versões com 32 bits);
1.1.7. Deve suportar a instalação de agente e *endpoint* nos sistemas operacionais acima virtualizados nas seguintes plataformas:
  1.1.7.1. AWS;
  1.1.7.2. Azure;
  1.1.7.3. GCP;
  1.1.7.4. Citrix XenApp;
  1.1.7.5. Citrix XenDesktop;

1.1.7.6. Citrix XenServer;
1.1.7.7. Microsoft Hyper-V 2012 R2 e superiores;
1.1.7.8. Vmware ESXi;
1.1.7.9. Vmware Player;
1.1.7.10. Vmware vSphere;
1.1.7.11. Vmware Workstation;
1.1.7.12. OpenStack

1.1.8. Toda a proteção deverá ser realizada através de um único agente de proteção com as funcionalidades descritas neste termo, não sendo aceitos *plug-ins* ou softwares adicionais para a composição do pacote;

1.1.9. O agente único deve compreender, no mínimo, as seguintes funcionalidades:
1.1.9.1. Módulo antimalware;
1.1.9.2. Módulo de proteção contra ameaças avançadas;
1.1.9.3. Desejável módulo de proteção de dados;
1.1.9.4. Desejável módulo para resposta à incidentes;
1.1.9.5. Desejável módulo de inteligência integrada contra ameaças;
1.1.9.6. Módulo para controle de dispositivos removíveis;

1.1.10. Todas as funcionalidades deverão ser geridas por uma console única com as capacidades mínimas de:
1.1.10.1. Relatórios;
1.1.10.2. *Dashboards*;
1.1.10.3. Políticas;
1.1.10.4. Configuração;
1.1.10.5. Instalação/Desinstalação;
1.1.10.6. Integração com produtos de terceiros;

1.1.11. O cliente deve ser capaz de operar em modo autônomo (*self-managed*) e permitir que as configurações sejam aplicadas diretamente no cliente.

1.1.12. O cliente deve ser capaz de atualizar as definições para detecção de ameaças, seus *patches* e *hotfixes* a partir de um servidor definido pelo administrador ou diretamente nos servidores do fabricante.

1.1.13. A solução de prevenção deve ser colaborativa, ou seja, os módulos exigidos devem ser capazes de trocarem informações para uma análise mais inteligente;

1.1.14. A solução deve possuir múltiplas camadas de proteção, não serão aceitas soluções baseadas apenas em assinaturas;

1.1.15. A solução deve conter módulo capaz de proteger contra botnets, negação de serviço, executáveis não confiáveis e conexões web maliciosas;

1.1.16. A solução deve conter módulo capaz de garantir uma navegação web segura, prevenindo contra sites maliciosos, *downloads* de ameaças e garantir a política de acesso (Permitir/Negar);

1.1.17. A plataforma deverá permitir automação de tarefas como: agendar tarefas como varreduras (*scans*), envio de relatórios, atualizações, atribuição de política e iniciar uma ativação de um agente;

1.1.18. Desejável que a solução de segurança para desktops e servidores possa se conectar a módulos de correlação e investigação em nuvem.

2. Características Módulo antivírus/antimalware (Clientes Windows)

2.1. Características da prevenção contra exploração

2.1.1. Deve ser possível selecionar, no mínimo, dois modos de proteção (Padrão/Máximo).
2.1.2. Deve ser possível ativar/desativar a proteção contra escalonamento de privilégios genéricos.
2.1.3. Deve ser possível ativar/desativar a prevenção de execução de dados do Windows.
2.1.4. Deve ser possível selecionar dentre as ações de apenas bloquear ou apenas relatar ou bloquear e relatar;
2.1.5. Deve ser possível bloquear contra falsificação de IP (*IP Spoofing*)
2.1.6. Deve ser possível incluir exclusões por:
  2.1.6.1. Processo;
  2.1.6.2. Nome;
  2.1.6.3. Caminho do Arquivo;
  2.1.6.4. *Hash* MD5;
  2.1.6.5. Módulo chamador:
    2.1.6.5.1. Nome;
    2.1.6.5.2. Caminho;
    2.1.6.5.3. *Hash* MD5;
    2.1.6.5.4. Signatário Digital.
2.1.7. É desejável que a solução tenha a capacidade de bloquear *exploits* que trabalham em nível de "*shell code*" e suas variantes, assim como, implementar a funcionalidade de "*virtual patching*" ou qualquer outra técnica para blindagem para aplicações, sistemas e sistemas operacionais contra exploração de vulnerabilidades conhecidas;

2.2. Características da Proteção de acesso

2.2.1. Deve fornecer regras de proteção de maneira nativa, ou seja, pré-definida pelo fabricante da solução, no mínimo, para:
  2.2.1.1. Acesso remoto a pastas locais;
  2.2.1.2. Alteração de políticas de direitos dos usuários;
  2.2.1.3. Alterar os registros de extensão dos arquivos;
  2.2.1.4. Criação de novos arquivos na pasta Arquivo de Programas;
  2.2.1.5. Criação de novos executáveis na pasta Windows;
  2.2.1.6. Criar/Modificar remotamente arquivos *Portable Executable*, INI, PIF e as localizações do sistema;
  2.2.1.7. Criar ou Modificar remotamente arquivos ou pastas;
  2.2.1.8. Desativar o editor de registro e o gerenciador de tarefas;
  2.2.1.9. Executar arquivos das pastas do usuário;
  2.2.1.10. Execução de *scripts* pelo *host* de *script* do Windows;

2.2.1.11. Instalar objetos de ajuda a navegação ou extensões de *shell*;
2.2.1.12. Instalar novos CLSIDs, APPIDs e TYPELIBs;
2.2.1.13. Modificar configurações de rede;
2.2.1.14. Modificar configurações do Internet Explorer;
2.2.1.15. Modificar processos principais do Windows:
2.2.1.15.1. Navegadores iniciando programas da pasta de *downloads*;
2.2.1.15.2. Registrar programas para execução automática;
2.2.1.16. As regras especificadas devem permitir o:
2.2.1.16.1. Bloqueio, ou
2.2.1.16.2. Evento de Informação, ou
2.2.1.16.3. Bloqueio e Evento de Informação;
2.2.1.17. Deve permitir ao administrador criar regras customizadas com no mínimo os seguintes parâmetros:
2.2.1.17.1. Processos:
2.2.1.17.1.1. Nome do processo;
2.2.1.17.1.2. Hash MD5;
2.2.1.17.1.3. Assinatura Digital;
2.2.1.17.2. Usuário;
2.2.1.17.3. Arquivos:
2.2.1.17.3.1. Criação;
2.2.1.17.3.2. Deletar;
2.2.1.17.3.3. Executar;
2.2.1.17.3.4. Alteração de permissão;
2.2.1.17.3.5. Leitura;
2.2.1.17.3.6. Renomear;
2.2.1.17.3.7. Escrever;
2.2.1.17.4. Chave de Registro:
2.2.1.17.4.1. Escrever;
2.2.1.17.4.2. Criar;
2.2.1.17.4.3. Deletar;
2.2.1.17.4.4. Ler;
2.2.1.17.4.5. Enumerar;
2.2.1.17.4.6. Carregar;
2.2.1.17.4.7. Substituir;
2.2.1.17.4.8. Restaurar;
2.2.1.17.5. Alterar permissão;
2.2.1.17.6. Valor de Registro:
2.2.1.17.6.1. Ler;
2.2.1.17.6.2. Criar;
2.2.1.17.6.3. Deletar;
2.2.1.17.7. Processo:
2.2.1.17.7.1. Qualquer acesso;
2.2.1.17.7.2. Criar *thread*;
2.2.1.17.7.3. Modificar;

2.2.1.17.7.4. Terminar;
2.2.1.17.7.5. Executar;
2.2.1.18. Deve permitir a configuração de exclusões;

2.3. Características da varredura ao acessar

2.3.1. A Varredura deve ser passível de habilitação/desativação por opção do administrador;
2.3.2. Deve iniciar a proteção durante a inicialização do sistema operacional;
2.3.3. Deve ser capaz de realizar análise no setor de boot;
2.3.4. O administrador da solução deve especificar o tempo máximo de análise para um único arquivo;
2.3.5. Deve analisar os processos durante inicialização do serviço e na atualização de conteúdo;
2.3.6. Deve possibilitar ao administrador a análise de instaladores confiáveis;
2.3.7. Deve realizar análise durante cópia entre pastas locais;
2.3.8. A solução deve possuir conexão com Centro de Inteligência do fabricante, passível de ativação ou desativação por parte do administrador;
2.3.9. Deve permitir a configuração do nível de agressividade da análise entre:
2.3.9.1. Muito Baixo
2.3.9.2. Baixo
2.3.9.3. Médio
2.3.9.4. Alto
2.3.9.5. Muito Alto
2.3.10. Deve possibilitar aplicar as configurações a todos os processos do sistema operacional ou a uma lista específica criada pelo administrador;
2.3.11. Deve realizar varredura quando o processo:
2.3.11.1. Ler o disco;
2.3.11.2. Gravar no disco;
2.3.11.3. Deixar a solução decidir;
2.3.12. Deve possibilitar análise em:
2.3.12.1. Unidades de Rede;
2.3.12.2. Arquivos abertos para *backup*;
2.3.12.3. Arquivos compactados, por exemplo .jar, .zip e outros;
2.3.12.4. Arquivos codificados (MIME);
2.3.13. Deve detectar programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas;
2.3.14. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:
2.3.14.1. Limpar o arquivo;
2.3.14.2. Excluir o arquivo;
2.3.14.3. Negar acesso ao arquivo;
2.3.15. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:

2.3.15.1. Limpar o arquivo;
2.3.15.2. Excluir o arquivo;
2.3.15.3. Permitir acesso ao arquivo;
2.3.15.4. Negar acesso ao arquivo;
2.3.16. Deve possibilitar ao administrador a gestão de uma lista de exclusões;
2.3.17. Deve possuir módulo capaz de interceptar *scripts* (Javascript e VBScript) destinados ao *Windows Host Scripting* e analisá-lo para indicar se é malicioso ou não;
2.3.18. Deve permitir a criação de listas de exclusão de URL's que não sofrerão interceptação e análise de *scripts*;
2.3.19. Ao detectar uma ameaça o agente deverá emitir uma notificação ao usuário com uma mensagem a ser customizada pelo administrador da solução.

2.4. Características Varredura sob demanda

2.4.1. Deve ser possível realizar varreduras agendadas com periodicidade diária ou semanal.
2.4.2. Deve permitir a criação de repetição da tarefa.
2.4.3. Deve permitir definir a hora da execução da tarefa de análise;
2.4.4. Deve permitir a criação da tarefa de varredura de maneira aleatória;
2.4.5. Deve permitir a realização de varreduras agendadas após *logon* do usuário ou durante inicialização do sistema operacional.
2.4.6. Deve permitir escolher (um ou mais) alvos da varredura, dentre eles:
2.4.6.1. Os locais da varredura:
2.4.6.1.1. Memória para rootkits;
2.4.6.1.2. Processos em execução;
2.4.6.1.3. Arquivos registrados;
2.4.6.1.4. Meu computador;
2.4.6.1.5. Todas as unidades locais;
2.4.6.1.6. Todas as unidades fixas;
2.4.6.1.7. Todas as unidades removíveis;
2.4.6.1.8. Todas as unidades mapeadas;
2.4.6.1.9. Pasta inicial;
2.4.6.1.10. Pasta de perfil do usuário;
2.4.6.1.11. Pasta Windows;
2.4.6.1.12. Pasta de arquivos de programas;
2.4.6.1.13. Pasta temporária;
2.4.6.1.14. Lixeira;
2.4.6.1.15. Arquivo ou pasta especificada pelo administrador;
2.4.6.1.16. Setor de inicialização (boot);
2.4.6.1.17. Arquivos compactados;
2.4.6.1.18. Arquivos MIME;
2.4.6.2. Os tipos de arquivos que serão analisados;

2.4.6.3. Opções adicionais, como por exemplo, detecção de programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas.
2.4.6.4. Áreas de exclusão que não deverão ser varridas;
2.4.7. Deve permitir a integração com o Centro de Inteligência do fabricante durante a varredura agendada.
2.4.8. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:
2.4.8.1. Limpar o arquivo;
2.4.8.2. Excluir o arquivo;
2.4.8.3. Negar acesso ao arquivo;
2.4.9. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:
2.4.9.1. Limpar o arquivo;
2.4.9.2. Excluir o arquivo;
2.4.9.3. Permitir acesso ao arquivo;
2.4.9.4. Negar acesso ao arquivo;
2.4.10. Para minimizar o impacto ao usuário, a solução deve permitir:
2.4.10.1. Utilização de *cache*, ou seja, arquivos que já foram analisados e não tiveram seu conteúdo alterado não serão novamente analisados;
2.4.10.2. Iniciar a varredura apenas quando o sistema estiver ocioso;
2.4.10.3. Permitir ao usuário retomar varreduras pausadas;
2.4.11. Deve permitir ao administrador inserir uma conta de domínio para realizar a análise de dispositivos de rede;

2.5. Características módulo de ameaças avançadas

2.5.1. A solução deve permitir o confinamento dinâmico de aplicativos e arquivos executáveis com indícios maliciosos (*ransomware*);
2.5.2. A solução deve ser capaz de avaliar aplicações desconhecidas e potencialmente maliciosas executando-as em ambiente controlado;
2.5.3. Deve permitir a indicação de aplicações confiáveis para que não caiam no filtro de confinamento dinâmico;
2.5.4. Não deve requerer conexão com centro de inteligência do fabricante para que a proteção seja ativada ou executada;
2.5.5. Solução deve manter um cache de reputação local com informações de aplicações - conhecidas, desconhecidas e maliciosas;
2.5.6. Dentre os comportamentos maliciosos, deve ser capaz de:
2.5.6.1. Bloquear acesso local a partir de cookies;
2.5.6.2. Bloquear a criação de arquivos a partir de arquivos com extensão .bat, .exe, html, hpg, jpg, bmp, job e .vbs;
2.5.6.3. Bloquear a criação de arquivos em qualquer local de rede;
2.5.6.4. Bloquear a criação de novos CLSIDs, APPIDs e TYPELIBs;
2.5.6.5. Boquear a criação de threads em outro processo;

2.5.6.6. Bloquear a desativação de executáveis críticos do sistema operacional;
2.5.6.7. Bloquear a leitura / exclusão / gravação de arquivos visados por ransomwares;
2.5.6.8. Bloquear a gravação e leitura na memória de outro processo;
2.5.6.9. Bloqueio de modificação da política de firewall do Windows;
2.5.6.10. Bloqueio de modificação da pasta de tarefas do Windows;
2.5.6.11. Bloqueio de modificação de arquivos críticos do Windows e Locais do Registro;
2.5.6.12. Bloqueio de modificação de arquivos executáveis portáteis;
2.5.6.13. Bloqueio de modificação de bit de atributo oculto;
2.5.6.14. Bloqueio de modificação de bit de atributo somente leitura;
2.5.6.15. Bloqueio de modificação de entradas de registro de DLL *AppInit*;
2.5.6.16. Bloqueio de modificação de locais do registro de inicialização;
2.5.6.17. Bloqueio de modificação de pastas de dados de usuários;
2.5.6.18. Bloqueio de modificação do local do Registro de Serviços;
2.5.6.19. Bloqueio de Suspensão de um processo;
2.5.6.20. Bloqueio de Término de outro processo;

2.5.7. Dos comportamentos observados, deve ser possível bloquear ou apenas informar caso o mesmo ocorra;
2.5.8. Deve ser capaz de informar ao usuário as ameaças encontradas através de mensagem customizada;
2.5.9. O modo de ativação do confinamento dinâmico para quaisquer arquivos desconhecidos acessados pelo sistema operacional e nunca antes visto pela solução;
2.5.10. Deve ser possível atribuir a regra conforme política equilibrada, visando maior segurança ou produtividade do usuário;
2.5.11. A proteção deve estar contida no mesmo agente de proteção, não requerendo outro software ou aplicação adicional na estação de trabalho para a execução e ativação da proteção
2.5.12. Deve possuir capacidade de inspecionar arquivos suspeitos e detectar comportamentos maliciosos utilizando técnicas de "*machine-learning*";

2.6. Módulo para controle de dispositivos removíveis

2.6.1. Controlar o modo como os usuários copiam dados em drives USB, iPods, CDs regraváveis e DVDs, disquetes, dispositivos *Bluetooth* e IrDA, dispositivos de leitura de imagens, portas COM e LPT e outros;
2.6.2. Especificar quais dispositivos podem ou não ser usados por qualquer parâmetro de dispositivo, inclusive códigos de produtos, códigos de fornecedor, números de série, classes de dispositivos, nomes de dispositivos;
2.6.3. Coletar dados de incidentes tais como dispositivo, data/hora, evidências de dados e outros, para reação, investigação e auditoria;
2.6.4. Permitir regra de reação para unidades de mídia removível (ex.: *pendrive*) com as opções de bloqueio total, somente leitura e monitoramento;
2.6.5. Monitorar automaticamente o uso e bloquear todas as tentativas de uso

dos dispositivos ou transferência de dados contrários às políticas definidas;

2.6.6. Integração com a ferramenta de gerenciamento centralizado para a coleta de dados essenciais de uso, tais como dispositivo, data/hora e evidências de dados;

2.6.7. Integração com estrutura de *Active Directory* para criação de regras baseadas em usuários ou grupos de usuários;

2.6.8. Bloquear a remoção do agente da estação mediante senha fornecida pelo administrador.

2.7. Características do módulo de gerenciamento centralizado

2.7.1. Deve suportar a instalação nos seguintes sistemas operacionais:

2.7.1.1. Windows Server 2019 e superiores;

2.7.1.2. Windows Server 2016 e superiores;

2.7.1.3. Desejável a instalação e execução em Windows Server 2012 Release 2 e superiores;

2.7.1.4. Desejável a instalação e execução em Windows Server 2012;

2.7.1.5. Desejável a instalação e execução em Windows Server 2008 Service Pack 2 (SP2) Standard, Enterprise ou Datacenter;

2.7.1.6. Desejável a instalação e execução em Windows Server 2008 R2 Standard, Enterprise ou Datacenter;

2.7.1.7. Desejável o fornecimento de um *appliance* pela Contratada, ou seja, um arquivo para instalação em ambiente de virtualização ou *hardware* que contemple os requisitos listados nesse ETP;

2.7.2. A arquitetura dos Sistemas Operacionais deve ser 64-bits;

2.7.3. Deve suportar a instalação em *cluster* Microsoft;

2.7.4. Deve suportar Ipv4 e Ipv6;

2.7.5. Deve suportar a virtualização do sistema operacional com base nos seguintes *hypervisors*:

2.7.5.1. Vmware ESX

2.7.5.2. Citrix Xen Server

2.7.5.3. Microsoft Hyper-V

2.7.6. Deve possuir suporte a base de dados:

2.7.6.1. SQL Server 2012 ou superior;

2.7.6.2. Desejável suporte a MySQL versões Standard ou Enterprise 5.7 ou superior, 32 ou 64 bits;

2.7.6.3. Desejável suporte a MariaDB Server 10.3 32 ou 64 bits;

2.7.7. A console de gerência deve ser acessada via WEB;

2.7.8. Deve possuir compatibilidade com os seguintes browsers:

2.7.8.1. Google Chrome;

2.7.8.2. Firefox;

2.7.8.3. Internet Explorer 7 ou superior;

2.7.8.4. Safari 6.0 ou superior;

2.7.8.5. Microsoft Edge;

2.7.9. Deve ser possível segregar a instalação da solução em:
2.7.9.1. Servidor Console Central
2.7.9.2. Servidor Base de Dados
2.7.9.3. Servidor de Interação com os Agentes
2.7.9.4. Agentes Distribuidores de Vacina
2.7.10. Deve suportar o uso do SQL Server em ambientes SAN;
2.7.11. Permitir a instalação dos Módulos da Solução a partir de um único servidor;
2.7.12. Permitir a alteração das configurações Módulos da Solução nos clientes de maneira remota;
2.7.13. Possuir a integração com o gerenciamento da solução de segurança de estações de trabalho e servidores, deste mesmo fabricante a fim de prover uma única console de gerenciamento centralizado de todas as soluções de segurança que possam ser utilizadas pela CONTRATANTE nesta contratação presente ou futura;
2.7.13.1. Permitir a atualização incremental da lista de definições de vírus nos clientes, a partir de um único ponto da rede local.
2.7.14. Visualização das características básicas de hardware das máquinas;
2.7.15. Integração e Importação automática da estrutura de domínios do *Active Directory* já existentes na rede local;
2.7.16. Permitir a criação de tarefas de atualização, verificação de vírus e upgrades em períodos de tempo pré-determinados, na inicialização do Sistema Operacional ou no *logon* na rede;
2.7.17. Permitir o armazenamento das informações coletadas nos clientes em um banco de dados centralizado;
2.7.18. Permitir diferentes níveis de administração do servidor, de maneira independente do *login* da rede;
2.7.19. Suporte a múltiplos usuários, com diferentes níveis de acesso e permissões aos produtos gerenciados;
2.7.20. Criação de grupos de máquinas baseadas em regras definidas em função do número IP do cliente;
2.7.21. Permitir a criação de grupos virtuais através de marcadores;
2.7.22. Permitir aplicar as marcações nos sistemas por vários critérios incluindo: produtos instalados, versão de sistema operacional, quantidade de memória, dentre outros;
2.7.23. Forçar a configuração determinada no servidor para os clientes;
2.7.24. Caso o cliente altere a configuração, a mesma deverá retornar ao padrão estabelecido no servidor, quando a mesma for verificada pelo agente.
2.7.25. A comunicação entre as máquinas clientes e o servidor de gerenciamento deve ser segura usando protocolo de autenticação HTTPS;
2.7.26. Forçar a instalação dos Módulos da Solução nos clientes;
2.7.27. Caso o cliente desinstale os Módulos da Solução, os mesmos deverão ser reinstalados, quando o agente verificar o ocorrido;
2.7.28. A solução deverá ser capaz de desinstalar versões antigas e soluções de antivírus (agentes e *endpoints*) de terceiros;
2.7.29. O módulo de gestão deverá realizar a gestão, de no mínimo, as seguintes

soluções propostas neste termo de referência:

2.7.29.1. Solução para proteção de estações de trabalho e servidores;
2.7.29.2. Desejável solução para resposta a incidentes;
2.7.29.3. Desejável solução para proteção de servidores críticos;
2.7.29.4. Deve ser possível realizar a customização dos relatórios gráficos gerados;
2.7.29.5. Exportação dos relatórios para os seguintes formatos: HTML, CSV, PDF, XML
2.7.29.6. Geração de relatórios que contenham as seguintes informações:
2.7.29.6.1. Máquinas com a lista de definições de vírus desatualizada;
2.7.29.6.2. Qual a versão do software (inclusive versão gerenciada pela nuvem) instalado em cada máquina;
2.7.29.6.3. Os vírus que mais foram detectados;
2.7.29.6.4. As máquinas que mais sofreram infecções em um determinado período de tempo;
2.7.29.6.5. Os usuários que mais sofreram infecções em um determinado período de tempo;
2.7.29.7. Gerenciamento de todos os módulos da suíte.
2.7.29.8. A solução de gestão deve possuir dashboards no gerenciamento da solução;
2.7.29.9. Estes dashboards devem conter no mínimo todos os seguintes relatórios de fácil visualização:
2.7.29.9.1. Relatório dos últimos 30 dias da detecção de códigos maliciosos;
2.7.29.9.2. Top 10 computadores com infecções;
2.7.29.10. Gerenciar a atualização do antivírus em computadores portáteis (notebooks), automaticamente, mediante conexão em rede local ou remota (VPN);
2.7.29.11. Suportar o uso de múltiplos repositórios para atualização de produtos e arquivo de vacina com replicação seletiva;
2.7.29.12. Ter a capacidade de gerar registros/logs para auditoria
2.7.29.13. A solução de gerenciamento deve ter a capacidade de atribuir etiquetas as máquinas, facilitando assim a distribuição automática dentro dos grupos hierárquicos na estrutura de gerenciamento.
2.7.29.14. A solução de gerenciamento deve permitir acesso a sua console via web.

2.8. Da Assistência Técnica e Nível de Serviço

2.8.1. As aberturas das ordens de serviço se darão via ligação telefônica gratuita (0800), chamado telefônico local, portal web (site) e/ou e-mail específico.
2.8.2. Os atendimentos para aberturas das ordens de serviço deverão estar disponíveis 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano.
2.8.3. O tempo máximo de espera (TME) deve ser de até 4 (quatro) horas para as ordens de serviço devidamente registradas, contadas a partir da abertura do chamado. O Tempo máximo de Reparo (TMR) de até 8 (oito)

horas.

2.9. Da Transferência de Tecnologia

2.9.1. Deverá ser fornecida uma atividade de capacitação para os profissionais da contratante com a finalidade de transferência tecnológica e de conhecimento da solução, da contratada para a contratante, com carga horário mínima de 30 horas, para 10 participantes;

2.9.2. As atividades deverão ser realizadas e ministradas pela empresa contratada, fornecendo aos participantes a capacitação do fabricante para a solução apresentada em proposta, cujos instrutores detenham os certificados oficiais do fabricante para o respectivo produto;

2.9.3. As atividades devem abordar todos os recursos e características disponíveis para a solução contratada, bem como apresentação para solução de problemas referentes à sua administração e gerenciamento;

2.9.4. As atividades devem contemplar, por parte da empresa contratada, o fornecimento ou criação de uma estrutura própria para tal evento, bem como sua estrutura necessária (redes, máquinas virtuais, dentre outros recursos), em um arranjo de hardware e/ou software separado do ambiente de produção da contratante, com o intuito de se evitar impactos negativos para o funcionamento da solução contratada;

2.9.5. As atividades deverão ser fornecidas preferencialmente em modalidade presencial, podendo ser em ambiente externo à empresa contratante ou em suas próprias instalações (*in company*), respeitados os pontos referentes ao ambiente de treinamento descrito no item 2.9.4; caso ainda persistam as regras de isolamento social decorrentes dos efeitos da pandemia de COVID-19, o treinamento poderá ser realizado em modalidade virtual, em ambiente remoto fornecido pela contratada; ambos os cenários (presencial ou remoto) deverão seguir as recomendações descritas no item 2.9.4;

Universidade de Brasília

TERMO DE REFERÊNCIA

UNIVERSIDADE DE BRASÍLIA - UNB

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO - STI

PROCESSO Nº 23106.017186/2021-96

REFERÊNCIA: ARTS. 12 A 24 DA IN SGD/ME Nº 1/2019

AQUISIÇÃO DE SOLUÇÃO CORPORATIVA DE ANTIVÍRUS MULTIPLATAFORMA COM GERÊNCIA CENTRALIZADA.

1. DO OBJETO DA CONTRATAÇÃO

1.1. Solução corporativa de antivírus multiplataforma com gerenciamento centralizado, compreendendo fornecimento de software de segurança para desktops e servidores (endpoint), software para gerenciamento centralizado, a respectiva instalação e configuração da solução adquirida, suporte técnico on-site e transferência de tecnologia e conhecimento.

2. DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1. Bens e serviços que compõem a solução:

Item	Descrição do Bem ou Serviço	Código CATSER	Quantidade	Métrica ou Unidade
1	Solução de segurança (software corporativo de antivírus multiplataforma) para estações de trabalho e servidores no ambiente administrativo da REDUnB (LICENÇAS)	27456	4000	Licença

2.1.1. O suporte e garantia para o Item 1 compreende o período de 36 (trinta e seis) meses para suporte on-site.

2.1.2. A empresa vencedora deverá fornecer módulo de gerenciamento centralizado com características conforme item 4.8.26 deste Termo de Referência.

3. JUSTIFICATIVA PARA CONTRATAÇÃO

3.1. Contextualização e Justificativa da Contratação:

3.1.1. O conteúdo do presente Termo de referência baseou-se nas conclusões constantes do Estudo Técnico Preliminar - ETP instruído no processo administrativo SEI nº 23106.017186/2021-96 como justificativas para a contratação que podemos elencar as seguintes:

3.1.1.1. Oferecer maior rapidez no tratamento dos riscos que envolvam estações de trabalho e servidores da estrutura computacional da Universidade de Brasília;

3.1.1.2. Permitir o controle de dispositivos não permitidos na REDUnB e mitigar em grande parte os riscos de infecções na tramitação de dados na rede;

3.1.1.3. Ofertar melhor suporte ao parque computacional da Universidade de Brasília, pois é necessária uma solução corporativa de antivírus que atenda a sistemas operacionais multiplataforma (Windows e Linux) e em versões distintas, pois este é o cenário comumente encontrado na REDUnB. Tal solução auxiliará na remoção, caso necessária, da solução existente hoje na universidade e deve possuir uma gerência centralizada funcional e de fácil gerenciamento;

3.1.1.4. A administração de uma solução corporativa de antivírus é mais simples e eficiente devido ao seu gerenciamento centralizado, uma vez que a manutenção de todas as estações de trabalho e servidores se torna complexa em função da estrutura computacional da Universidade de Brasília, com isso a necessidade de se ter uma solução corporativa centralizada;

3.1.1.5. A administração centralizada promove à equipe que administra a solução corporativa de antivírus a confiança de que todas as estações de trabalho e servidores estarão com o mesmo nível de segurança, com isso trazendo maior confiabilidade e padronização;

3.1.1.6. A contratação desta solução visa ofertar maior garantia à

Universidade de Brasília quanto a aplicabilidade de uma política em busca de integridade das informações, processos e demais objetos que possam ser violados mediante ataques de trojans, vírus e quaisquer espécies de pragas virtuais, bem como proteger informações sigilosas e essenciais que possam ser furtadas ou perdidas acidentalmente;

3.1.1.7. Com a ampliação constante dos casos de violações cibernéticas como invasões e também o aumento de casos de ransomware (vírus de resgate), quaisquer vulnerabilidades são exploradas caso não sejam, em tempo, corrigidas. Com a crescente utilização da Internet, os processos organizacionais e informações ficam mais expostas o que por si só já requer a adoção de tecnologias mais avançadas de proteção, incluindo a prospecção dessas vulnerabilidades e suas imediatas contramedidas;

3.1.1.8. A solução corporativa de antivírus é essencial para a segurança das informações que são trabalhadas, armazenadas e trafegadas no ambiente REDUnB, representando um grande risco para este ambiente a falta de cobertura por solução desta natureza;

3.1.2. A Solução de Segurança deverá ser instalada e configurada para operação na REDUnB, mais especificamente em estações de trabalho administrativas e equipamentos servidores da Universidade de Brasília, visando a proteção em tempo real, com o regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano), dos componentes, serviços e informações que fazem parte do parque computacional (estações administrativas e servidores) da Universidade de Brasília.

3.2. Alinhamento aos Instrumentos de Planejamento Institucionais

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos**
PDI 2018_2022	Item 3. Garantir a transparência e a segurança da informação e comunicação.
Alerta No. 07/2020: Centro de Tratamento de Incidentes de Redes do Governo - (CTIR)	A necessidade de manutenção dos softwares de antivírus (Medida de mitigação para a ameaça de sequestro de dados - Governo Federal).
EGD 2020_22 - Objetivo 10 - Implementação da Lei Geral de Proteção de Dados no âmbito do Governo federal	Iniciativa 10.1. Estabelecer adequação e conformidade com os requisitos da Lei Geral de Proteção de Dados.
EGD 2020_22-Objetivo 11: Garantia da segurança das plataformas de governo digital e de missão crítica	Iniciativa 11.1. Garantir disponibilidade das plataformas compartilhadas de governo digital. Iniciativa 11.3. Definir padrão mínimo de segurança cibernética a ser aplicado nos canais e serviços digitais.
EGD 2020_22-Objetivo 16 - Otimização das infraestruturas de tecnologia da informação	Iniciativa 16.1. Realizar compras centralizadas de bens e serviços comuns de tecnologia da informação e comunicação. Iniciativa 16.2. Ampliar o compartilhamento de soluções de softwares estruturantes. Iniciativa 16.4. Otimizar a infraestrutura de datacenters. Iniciativa 16.5. Migração de serviços para a nuvem. Iniciativa 16.6. Negociar acordos corporativos com os maiores fornecedores de tecnologia da informação e comunicação de forma a resultar na redução dos preços.

ALINHAMENTO AO PDTIC 2019_2022			
ID	**Necessidades do PDTIC**	**ID**	**Objetivos estratégicos de TIC**
N2	Oferta e manutenção de infraestrutura de TIC visando aumentar a confiabilidade e a disponibilidade alinhada à expansão da UnB;	OETIC7, OETIC8, OETIC9, OETIC12, OETIC15.	• Promover atualização tecnológica dos sistemas e da infraestrutura de TIC da UnB; • Garantir a conectividade, qualidade e segurança dos serviços de TICs; • Garantir a transparência e a segurança da informação e comunicação; • Atender à legislação pertinente à área de TI; • Garantir o efetivo atendimento às demandas de TIC e melhorar a disponibilidade dos sistemas e serviços de TIC" (sic);
N3	Desenvolvimento de mecanismos de Segurança da Informação e Comunicação.	OETIC7, OETIC8, OETIC9, OETIC12, OETIC15.	• Promover atualização tecnológica dos sistemas e da infraestrutura de TIC da UnB; • Garantir a conectividade, qualidade e segurança dos serviços de TICs; • Garantir a transparência e a segurança da informação e comunicação; • Atender à legislação pertinente à área de TI; • Garantir o efetivo atendimento às demandas de TIC e melhorar a disponibilidade dos sistemas e serviços de TIC" (sic);

ALINHAMENTO AO PAC_2021	
Item	**Descrição**
1	Segundo processo SEI nº 23106.017186/2021-96, DOD (6604977), informamos que a referida contratação de TI está presente no PAC 2021. Item no PAC: 10752.

3.3. Estimativa da demanda

3.3.1. Considerando os dados de abril de 2019, obtidos da solução atual de antivírus – a qual contempla o ambiente administrativo da universidade – em que constava o total de 2635 (dois mil e seiscentos e trinta e cinco) estações de trabalho gerenciadas e 919 (novecentos e dezenove) estações de trabalho não gerenciadas, totalizando 3.554 (três mil quinhentos e cinquenta e quatro) unidades.

3.3.2. Considerando o quantitativo de estações ingressas no Active Directory da Microsoft, as quais possuem em torno de 2000 (duas mil) estações de trabalho, conforme levantamento realizado em junho de 2021, sendo o restante dos equipamentos não ingressos no referido serviço de diretório, o que não exclui a necessidade de manutenções e instalações em modo stand-alone. A variação do número de estações fora do domínio se dá devido ao momento atual da universidade, que vem passando pela redução do trabalho na modalidade presencial devido às medidas de isolamento social demandadas para combate à epidemia do Covid-19. Com o gradativo retorno ao trabalho em modalidade presencial, estes números tendem a retornar aos indicativos mencionados no parágrafo anterior.

3.3.3. A Secretaria de Tecnologia da Informação, assumindo que terá um crescimento de 5% a 10% ao ano na quantidade de estações de trabalho gerenciadas ou controladas pela solução corporativa de antivírus, justifica a necessidade de adquirir o quantitativo de licenças solicitadas no processo de aquisição.

3.4. Parcelamento da Solução de TIC

3.4.1. Não haverá parcelamento do objeto, uma vez que este objeto é único para solução apresentada.

3.4.2. O não parcelamento se justifica no fato de que a solução de segurança para estações de trabalho e servidores, o software servidor de gerenciamento centralizado, o suporte técnico e o treinamento são serviços complementares, interdependentes e customizados entre si para garantir a compatibilidade com os produtos do respectivo fabricante da solução fornecida, e que sendo realizados de forma desconectada pode gerar à Universidade de Brasília o paradoxo de conflito de garantias entre fornecedores.

3.5. Resultados e Benefícios a Serem Alcançados

3.5.1. A Universidade de Brasília tem o objetivo de contratar uma solução corporativa de antivírus multiplataforma com gerenciamento centralizado, para atender as necessidades de proteção contra códigos maliciosos na rede computacional administrativa da universidade; com isso, a solução contratada deve atingir os seguintes resultados:

3.5.1.1. Atender todas as especificações técnicas;

3.5.1.2. Ser uma alternativa de baixo custo, porém vantajosa à Universidade de Brasília, compondo seu catálogo de serviços;

3.5.1.3. Fazer com que a Secretaria de Tecnologia da Informação possa ter a capacidade de atender às necessidades técnicas de segurança de forma direta para a rede computacional administrativa e de forma indireta para o ambiente da REDUnB, dando proteção no tráfego de informações e retenção de dados;

3.5.1.4. Aumentar a confiabilidade direta dos usuários que utilizam os serviços da rede computacional administrativa e de forma indireta dos usuários dos outros recursos computacionais da Universidade de Brasília.

3.6. **Da Justificativa para Utilização do Registro de Preços**

3.6.1. A contratação para fornecimento da solução antivírus, objeto do termo de referência, por meio do sistema de registro de preços justifica-se em razão da solução proposta será implantada de forma escalonada durante o ano de 2022, com isso as requisições serão parceladas visando atender as unidades da UnB ao longo do ano, de forma parcelada, o que justifica a realização do Registro de Preços, o qual terá vigência de 12 (doze) meses para atender à estas demandas.

3.6.2. 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, define as hipóteses sobre sua admissão pela Administração Pública em especial o inciso II do Art. 3º o qual abarca a justificativa.

"Art. 3º O Sistema de Registro de Preços poderá ser adotado nas seguintes hipóteses:

[...]

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;

3.6.3. Marçal Justen Filho, em sua obra "Comentários à Lei de Licitações e Contratos Administrativos" (12ª edição, editora Dialética, 2008, página 180), assim comenta o Sistema de Registro de Preços:

> *"No Sistema de Registro de Preços, a principal diferença reside no objeto da licitação. Usualmente, a licitação destina-se a selecionar um fornecedor e uma proposta para uma contratação específica, a ser efetivada posteriormente pela Administração. No Registro de Preços, a licitação destina-se a selecionar fornecedor e proposta para contratações não específicas, seriadas, que poderão ser realizadas durante um certo período, por repetidas vezes. A proposta selecionada fica a disposição da Administração que, se e quando desejar adquirir, se valerá dos preços registrados, tantas vezes quantas o desejar (dentro dos limites estabelecidos no ato convocatório)".*

3.6.4. Além disso, a existência de preços registrados não obriga a Administração a firmar as contratações que deles poderão advir, ficando facultada a realização de licitação específica para aquisição, sendo assegurada ao beneficiário do registro a preferência de fornecimento em igualdade de condições.

3.7. **Da adesão de órgãos não participantes**

3.7.1. Não será concedida a adesão de órgãos não participantes em conformidade com o disposto no §10 do art. 22 do Decreto nº 7.892, de 23/01/2013, alterado pelo Decreto nº 9.488, de 30/08/2018.

> § 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: (Incluído pelo Decreto nº 9.488, de 2018) (Vigência)
>
> I - gerenciada pelo Ministério do Planejamento, Desenvolvimento e Gestão; ou (Incluído pelo Decreto nº 9.488, de 2018) (Vigência)
>
> 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. (Incluído pelo Decreto nº 9.488, de 2018) (Vigência)

4. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio

4.1.1. A empresa contratada deverá fazer a instalação e configuração da solução adotada nas instalações e infraestrutura da contratante, compreendendo a instalação de servidores para o gerenciamento centralizado em ambiente virtualizado (console de gerenciamento) e também a instalação e configuração (deployment) dos clientes (endpoints) para servidores e estações de trabalho já disponíveis na solução atual (em produção), bem como a adaptação e/ou transferência das tarefas e políticas em uso da solução anterior, tomadas as devidas providências para mitigar e minimizar eventuais impactos no ambiente administrativo da REDUnB.

4.1.2. As licenças a ativar em endpoints e servidores de gerência deverão ser flutuantes, ou seja, quando um equipamento (computador / estação de trabalho ou servidor) for substituído ou formatado, a licença deverá ser realocada a outro equipamento ou associada novamente à máquina antiga, conforme o caso.

4.1.3. A solução deverá ser implantada na localização determinada pela Secretaria de Tecnologia da Informação da Universidade de Brasília, em ambiente virtualizado, sendo que na gerência da solução implantada devem ser ativadas todas as licenças adquiridas.

4.1.4. Em resumo a solução corporativa de antivírus a ser contratada, bem como os serviços atrelados a esta solução, devem ser entregues de modo a prover segurança na camada de usuário, mitigando riscos capazes de impactar a produtividade nas atividades laborais dos colaboradores da Universidade de Brasília e degradar o desempenho dos sistemas e do ambiente administrativo da REDUnB.

4.1.5. A CONTRATADA deverá designar preposto para o acompanhamento e para garantir os serviços de acordo com as necessidades da CONTRATANTE;

4.1.6. A CONTRATADA deverá disponibilizar os recursos necessários a execução dos serviços;

4.1.7. Todo o material necessário para a instalação será fornecido pela CONTRATADA.

4.2. Requisitos de Capacitação

4.2.1. Deverá ser fornecida uma atividade de capacitação para os profissionais da contratante com a finalidade de transferência tecnológica e de conhecimento da solução, da contratada para a contratante, com carga horário mínima de 30 horas, para 10 participantes;

4.2.2. As atividades deverão ser realizadas e ministradas pela empresa contratada, fornecendo aos participantes a capacitação do fabricante para a solução apresentada em proposta, cujos instrutores detenham os certificados oficiais do fabricante para o respectivo produto;

4.2.3. As atividades devem abordar todos os recursos e características disponíveis para a solução contratada, bem como apresentação para solução de problemas referentes à sua administração e gerenciamento;

4.2.4. As atividades devem contemplar, por parte da empresa contratada, o fornecimento ou criação de uma estrutura própria para tal evento, bem como sua estrutura necessária (redes, máquinas virtuais etc), em um arranjo de hardware e/ou software separado do ambiente de produção da contratante, com o intuito de se evitar impactos negativos para o funcionamento da solução contratada;

4.2.5. As atividades deverão ser fornecidas preferencialmente em modalidade presencial, podendo ser em ambiente externo à empresa contratante ou em suas próprias instalações (in company), respeitados os pontos referentes ao ambiente de treinamento descrito no item 5.2.4; caso ainda persistam as regras de isolamento social decorrentes dos efeitos da pandemia de COVID-19, o treinamento poderá ser realizado em modalidade virtual, em ambiente remoto fornecido pela contratada; ambos os cenários (presencial ou remoto) deverão seguir as recomendações descritas no item 5.2.4.

4.3. Requisitos Legais

4.3.1. Lei nº 8.666/1993: Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências;

4.3.2. 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;

4.3.3. Decreto nº 7.174/2010: Regulamenta a contratação de bens e serviços de informática e automação pela Administração Pública Federal;

4.3.4. Decreto nº 8.184, de 17 de janeiro de 2014, que estabelece a aplicação de margem de preferência em licitações realizadas no âmbito da administração pública federal para aquisição de equipamentos de tecnologia da informação e comunicação, para fins do disposto no art. 3º da Lei nº 8.666, de 21 de junho de 1993;

4.3.5. Decreto nº 10.024, de 20 de Agosto de 2019, que Regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal;

4.3.6. Instrução Normativa SGD/ME nº 01/2019 e suas alterações: Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Poder Executivo Federal;

4.3.7. Instrução Normativa SEGES nº 05/2017: Dispõe sobre os procedimentos administrativos básicos para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral;

4.3.8. Instrução Normativa nº 01, de 19 de janeiro de 2010 - Art. 5º: Institui, aos órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional, critérios de sustentabilidade ambiental;

4.3.9. Instrução Normativa nº 73/2020-SEGES/ME, de 5 de agosto de 2020, que dispõe sobre os procedimentos administrativos básicos para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral;

4.3.10. Decreto nº 7.746/2012: Estabelece critérios, práticas e diretrizes gerais para a promoção do desenvolvimento nacional sustentável por meio das contratações realizadas pela administração pública federal direta, autárquica e fundacional e pelas empresas estatais dependentes, e institui a Comissão Interministerial de Sustentabilidade na Administração Pública – CISAP;

4.3.11. 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;

4.3.12. Decreto nº 9.507, de 21 de Setembro de 2018, que Dispõe sobre a execução indireta, mediante contratação, de serviços da administração pública federal direta, autárquica e fundacional e das empresas públicas e das sociedades de economia mista controladas pela União;

4.3.13. Lei nº 13.709, DE 14 DE Agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

4.4. Requisitos de Manutenção

4.4.1. A abertura de chamados ocorrerá via ligação telefônica gratuita (0800), chamado telefônico local, portal web (site) e/ou e-mail específico.

4.4.2. Os atendimentos para aberturas de chamados deverão estar disponíveis 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano.

4.4.3. Após os atendimentos, os tempos máximos de espera (TME) e de reparo ou resolução (TMR) deverão seguir os seguintes critérios:

4.4.3.1. Para chamados ou solicitações com níveis de severidade que representem falhas mínimas que prejudicam o desempenho, mas não irão produzir paralização do serviço (severidade baixa) os indicadores TME e TMR deverão ser de 16 e 24 horas, respectivamente;

4.4.3.2. Para chamados ou solicitações com níveis de severidade que representem incidentes capazes de causar a paralisação do serviço (severidade média) os indicadores TME e TMR deverão ser de 8 e 12 horas, respectivamente;

4.4.3.3. Para chamados ou solicitações com níveis de severidade que representem incidentes críticos, ou que possam tornar inoperante o serviço e provocar outros danos (severidade alta) os indicadores TME e TMR deverão ser de 4 e 6 horas, respectivamente;

4.4.3.4. O tempo máximo de espera (TME) deve ser de até 4 (quatro) horas para as ordens de serviço devidamente registradas, contadas a partir da abertura do chamado. O Tempo máximo de Reparo (TMR) de até 8 (oito) horas.

4.4.4. A CONTRATADA deverá realizar o atendimento do chamado de suporte técnico por telefone ou por e-mail ou sistema on-line que deverá ser informado à CONTRATANTE.

4.4.4.1. Caso seja por telefone a CONTRATADA deverá informar o número e os procedimentos necessários para utilização;

4.4.4.2. Caso seja por e-mail a CONTRATADA deverá informar a conta de e-mail e os procedimentos necessários para utilização;

4.4.4.3. Caso seja por sistema on-line a CONTRATADA deverá liberar acesso aos servidores designados pela UnB e informar os procedimentos necessários para utilização.

4.4.5. O atendimento do chamado de suporte técnico deverá ser realizado, salvo solicitação em contrário, nos dias de expediente da CONTRATANTE, das 07:00 às 12:00 e das 14:00 às 19:00, de segunda-feira a sexta-feira, sempre por profissionais com os conhecimentos necessários para a solução do problema.

4.4.6. A CONTRATADA não poderá recusar-se em executar o suporte técnico solicitado.

4.5. Requisitos Temporais

4.5.1. O prazo de entrega da solução corporativa de antivírus multiplataforma com gerência centralizada é de 30 a 60 dias, sendo 30 dias para a apresentação formal da contratada, incluindo a execução das atividades de entrega e implantação, e em sequencia o prazo de 45 dias para o início das atividades de transferência tecnológica e de conhecimento da solução;

4.5.2. Para fins de início dos prazos será utilizado como referência o dia da assinatura do contrato;

4.6. Requisitos de Segurança

4.6.1. A CONTRATADA deverá seguir todas as normas de segurança vigentes nos sistemas da CONTRATANTE e suas dependências.

4.6.2. Cada profissional da CONTRATADA deverá assinar Termo de Compromisso declarando total obediência às normas de segurança vigentes ou que venham a ser implantadas, a qualquer tempo nas dependências da CONTRATANTE, ANEXO III - TERMO DE CONFIDENCIALIDADE, SIGILO E COMPROMISSO.

4.6.3. Além disso, cada profissional da CONTRATADA deverá assinar termo declarando estar ciente de que a estrutura informatizada disponibilizada pela CONTRATANTE não poderá ser utilizada para fins particulares e que a navegação em sítios da Internet e as correspondências em meio eletrônico utilizando endereços da CONTRATANTE ou acessada à partir dos seus equipamentos, poderão ser auditadas.

4.7. Requisitos Sociais, Ambientais e Culturais

4.7.1. A CONTRATADA deverá atender, no que couber, os critérios de sustentabilidade ambiental previstos na Instrução Normativa nº 01, de 19 de janeiro de 2010, da Secretaria de Logística e Tecnologia da Informação, do Ministério do Planejamento, Orçamento e Gestão - SLTI/MPOG, e do Decreto nº 7.746, de 05 de junho de 2012.

4.7.2. Os serviços prestados pela CONTRATADA deverão pautar-se sempre

no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e material consumidos, bem como a geração excessiva de resíduos, a fim de atender às diretrizes de responsabilidade ambiental adotadas pelo CONTRATANTE.

4.7.3. A CONTRATADA deverá instruir os seus empregados quanto à necessidade de racionalização de recursos no desempenho de suas atribuições, bem como das diretrizes de responsabilidade ambiental adotadas pelo CONTRATANTE.

4.8. **Requisitos de Arquitetura tecnológica**

4.8.1. Deve possuir suporte às arquiteturas 32-bits e 64-bits;

4.8.2. Deve possuir capacidade de instalação e pleno funcionamento dos módulos solicitados em estações de trabalho com no mínimo 3GB de memória RAM;

4.8.3. Deve suportar as seguintes plataformas Microsoft (clientes/desktops):

4.8.3.1. Windows 10 e superiores;

4.8.3.2. Windows 8.1;

4.8.3.3. Desejável suporte ao Windows 8;

4.8.3.4. Desejável suporte ao Windows 7;

4.8.4. Deve suportar as seguintes plataformas Microsoft (servidores):

4.8.4.1. Windows Server 2019 e superiores;

4.8.4.2. Windows Server 2016;

4.8.4.3. Windows Server 2012 R2;

4.8.4.4. Windows Server 2012;

4.8.4.5. Windows Storage Server 2012;

4.8.4.6. Desejável suporte ao Windows Server 2008 R2 nas versões Standard, Datacenter, Enterprise ou Web;

4.8.4.7. Desejável suporte ao Windows Server 2003 em todas as suas versões.

4.8.5. Deve inclusive suportar o modo Server Core;

4.8.6. Deve suportar, pelo menos a função de antivírus, nas seguintes distribuições de Linux:

4.8.6.1. Red Hat 6 e superiores, 32 e/ou 64bits;

4.8.6.2. SUSE Server 12 e superiores, 64bits (desejável suporte também para versões desktop, bem como versões com 32 bits);

4.8.6.3. Ubuntu 16.04 e superiores, 64bits (desejável suporte também para versões desktop, bem como versões com 32 bits);

4.8.6.4. CentOS 6.x e superiores, 64bits (desejável suporte também para versões com 32 bits);

4.8.6.5. Debian 9 e superiores, 64bits (desejável suporte também para versões com 32 bits);

4.8.7. Deve suportar a instalação de agente e endpoint nos sistemas operacionais acima virtualizados nas seguintes plataformas:

4.8.7.1. AWS;

4.8.7.2. Azure;

4.8.7.3. GCP;

4.8.7.4. Citrix XenApp;

4.8.7.5. Citrix XenDesktop;

4.8.7.6. Citrix XenServer;

4.8.7.7. Microsoft Hyper-V 2012 R2 e superiores;

4.8.7.8. Vmware ESXi;

4.8.7.9. Vmware Player;

4.8.7.10. Vmware vSphere;

4.8.7.11. Vmware Workstation;

4.8.7.12. OpenStack

4.8.8. Toda a proteção deverá ser realizada através de um único agente de proteção com as funcionalidades descritas neste termo, não sendo aceitos plug-ins ou softwares adicionais para a composição do pacote;

4.8.9. O agente único deve compreender, no mínimo, as seguintes funcionalidades:

4.8.9.1. Módulo antimalware;

4.8.9.2. Módulo de proteção contra ameaças avançadas;

4.8.9.3. Desejável módulo de proteção de dados;

4.8.9.4. Desejável módulo para resposta à incidentes;

4.8.9.5. Desejável módulo de inteligência integrada contra ameaças;

4.8.9.6. Módulo para controle de dispositivos removíveis;

4.8.10. Todas as funcionalidades deverão ser geridas por uma console única com as capacidades mínimas de:

4.8.10.1. Relatórios;

4.8.10.2. Dashboards;

4.8.10.3. Políticas;

4.8.10.4. Configuração;

4.8.10.5. Instalação/Desinstalação;

4.8.10.6. Integração com produtos de terceiros;

4.8.11. O cliente deve ser capaz de operar em modo autônomo (self-managed) e permitir que as configurações sejam aplicadas diretamente no cliente.

4.8.12. O cliente deve ser capaz de atualizar as definições para detecção de ameaças, seus patches e hotfixes a partir de um servidor definido pelo administrador ou diretamente nos servidores do fabricante.

4.8.13. A solução de prevenção deve ser colaborativa, ou seja, os módulos exigidos devem ser capazes de trocarem informações para uma análise mais inteligente;

4.8.14. A solução deve possuir múltiplas camadas de proteção, não serão aceitas soluções baseadas apenas em assinaturas;

4.8.15. A solução deve conter módulo capaz de proteger contra botnets, negação de serviço, executáveis não confiáveis e conexões web maliciosas;

4.8.16. A solução deve conter módulo capaz de garantir uma navegação web segura, prevenindo contra sites maliciosos, downloads de ameaças e garantir a política de acesso (Permitir/Negar)

4.8.17. A plataforma deverá permitir automação de tarefas como: agendar tarefas como varreduras (scans), envio de relatórios, atualizações, atribuição de política e iniciar uma ativação de um agente;

4.8.18. Desejável que a solução de segurança para desktops e servidores possa se conectar a módulos de correlação e investigação em nuvem;

4.8.19. Requisitos de Proteção da Solução:

4.8.20. Características da prevenção contra exploração

4.8.20.1. Deve ser possível selecionar, no mínimo, dois modos de proteção (Padrão/Máximo).

4.8.20.2. Deve ser possível ativar/desativar a proteção contra escalonamento de privilégios genéricos.

4.8.20.3. Deve ser possível ativar/desativar a prevenção de execução de dados do Windows.

4.8.20.4. Deve ser possível selecionar dentre as ações de apenas bloquear ou apenas relatar ou bloquear e relatar;

4.8.20.5. Deve ser possível bloquear contra falsificação de IP (IP Spoofing)

4.8.20.6. Deve ser possível incluir exclusões por:

1. Processo;
2. Nome;
3. Caminho do Arquivo;
4. Hash MD5;
5. Módulo chamador:
    1. Nome;
    2. Caminho;
    3. Hash MD5;
    4. Signatário Digital.

4.8.20.7. É desejável que a solução tenha a capacidade de bloquear exploits que trabalham em nível de "shell code" e suas variantes, assim como, implementar a funcionalidade de "virtual patching" ou qualquer outra técnica para blindagem para aplicações, sistemas e sistemas operacionais

contra exploração de vulnerabilidades conhecidas;

4.8.21. Características da Proteção de acesso

4.8.21.1. Deve fornecer regras de proteção de maneira nativa, ou seja, pré-definida pelo fabricante da solução, no mínimo, para:

1. Acesso remoto a pastas locais;
2. Alteração de políticas de direitos dos usuários;
3. Alterar os registros de extensão dos arquivos;
4. Criação de novos arquivos na pasta Arquivo de Programas;
5. Criação de novos executáveis na pasta Windows;
6. Criar/Modificar remotamente arquivos Portable Executable, INI, PIF e as localizações do sistema;
7. Criar ou Modificar remotamente arquivos ou pastas;
8. Desativar o editor de registro e o gerenciador de tarefas;
9. Executar arquivos das pastas do usuário;
10. Execução de scripts pelo host de script do Windows;
11. Instalar objetos de ajuda a navegação ou extensões de shell;
12. Instalar novos CLSIDs, APPIDs e TYPELIBs;
13. Modificar configurações de rede;
14. Modificar configurações do Internet Explorer;
15. Modificar processos principais do Windows:
    1. Navegadores iniciando programas da pasta de downloads;
    2. Registrar programas para execução automática;
16. As regras especificadas devem permitir o:
    1. Bloqueio, ou
    2. Evento de Informação, ou
    3. Bloqueio e Evento de Informação;
17. Deve permitir ao administrador criar regras customizadas com no mínimo os seguintes parâmetros:
    1. Processos:
        1. Nome do processo;
        2. Hash MD5;
        3. Assinatura Digital;
    2. Usuário
    3. Arquivos:
        1. Criação;
        2. Deletar;
        3. Executar;
        4. Alteração de permissão;
        5. Leitura;
        6. Renomear;
        7. Escrever;
    4. Chave de Registro:
        1. Escrever;
        2. Criar;
        3. Deletar;
        4. Ler;
        5. Enumerar;
        6. Carregar;
        7. Substituir;
        8. Restaurar;
    5. Alterar permissão;
    6. Valor de Registro:
        1. Ler;
        2. Criar;
        3. Deletar;

7. Processo:
    1. Qualquer acesso;
    2. Criar thread;
    3. Modificar;
    4. Terminar;
    5. Executar;

18. Deve permitir a configuração de exclusões;

4.8.22. Características da varredura ao acessar

4.8.22.1. A Varredura deve ser passível de habilitação/desativação por opção do administrador;

4.8.22.2. Deve iniciar a proteção durante a inicialização do sistema operacional;

4.8.22.3. Deve ser capaz de realizar análise no setor de boot;

4.8.22.4. O administrador da solução deve especificar o tempo máximo de análise para um único arquivo;

4.8.22.5. Deve analisar os processos durante inicialização do serviço e na atualização de conteúdo;

4.8.22.6. Deve possibilitar ao administrador a análise de instaladores confiáveis;

4.8.22.7. Deve realizar análise durante cópia entre pastas locais;

4.8.22.8. A solução deve possuir conexão com Centro de Inteligência do fabricante, passível de ativação ou desativação por parte do administrador;

4.8.22.9. Deve permitir a configuração do nível de agressividade da análise entre:

1. Muito Baixo;
2. Baixo;
3. Médio;
4. Alto;
5. Muito Alto

4.8.22.10. Deve possibilitar aplicar as configurações a todos os processos do sistema operacional ou a uma lista específica criada pelo administrador;

4.8.22.11. Deve realizar varredura quando o processo:

1. Ler o disco;
2. Gravar no disco;
3. Deixar a solução decidir;

4.8.22.12. Deve possibilitar análise em:

1. Unidades de Rede;
2. Arquivos abertos para backup;
3. Arquivos compactados, por exemplo .jar, .zip e outros;
4. Arquivos codificados (MIME);

4.8.22.13. Deve detectar programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas;

4.8.22.14. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:

1. Limpar o arquivo;
2. Excluir o arquivo;
3. Negar acesso ao arquivo;

4.8.22.15. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:

1. Limpar o arquivo;
2. Excluir o arquivo;
3. Permitir acesso ao arquivo;
4. Negar acesso ao arquivo;

4.8.22.16. Deve possibilitar ao administrador a gestão de uma lista de exclusões;

4.8.22.17. Deve possuir módulo capaz de interceptar scripts (Javascript e VBScript) destinados ao Windows Host Scripting e analisá-lo para indicar se é malicioso ou não;

4.8.22.18. Deve permitir a criação de listas de exclusão de URL's que não sofrerão interceptação e análise de scripts;

4.8.22.19. Ao detectar uma ameaça o agente deverá emitir uma notificação ao usuário com uma mensagem a ser customizada pelo administrador da solução.

4.8.23. Características Varredura sob demanda

4.8.23.1. Deve ser possível realizar varreduras agendadas com periodicidade diária ou semanal.

4.8.23.2. Deve permitir a criação de repetição da tarefa.

4.8.23.3. Deve permitir definir a hora da execução da tarefa de análise;

4.8.23.4. Deve permitir a criação da tarefa de varredura de maneira aleatória;

4.8.23.5. Deve permitir a realização de varreduras agendadas após logon do usuário ou durante inicialização do sistema operacional.

4.8.23.6. Deve permitir escolher (um ou mais) alvos da varredura, dentre eles:

1. Os locais da varredura:
    1. Memória para rootkits;
    2. Processos em execução;
    3. Arquivos registrados;
    4. Meu computador;
    5. Todas as unidades locais;
    6. Todas as unidades fixas;
    7. Todas as unidades removíveis;
    8. Todas as unidades mapeadas;
    9. Pasta inicial;
    10. Pasta de perfil do usuário;
    11. Pasta Windows;
    12. Pasta de arquivos de programas;
    13. Pasta temporária;
    14. Lixeira;
    15. Arquivo ou pasta especificada pelo administrador;
    16. Setor de inicialização (boot);
    17. Arquivos compactados;
    18. Arquivos MIME;
2. Os tipos de arquivos que serão analisados;
3. Opções adicionais, como por exemplo, detecção de programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas.
4. Áreas de exclusão que não deverão ser varridas;

4.8.23.7. Deve permitir a integração com o Centro de Inteligência do fabricante durante a varredura agendada.

4.8.23.8. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:

1. Limpar o arquivo;
2. Excluir o arquivo;
3. Negar acesso ao arquivo;

4.8.23.9. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:

1. Limpar o arquivo;
2. Excluir o arquivo;
3. Permitir acesso ao arquivo;
4. Negar acesso ao arquivo;

4.8.23.10. Para minimizar o impacto ao usuário, a solução deve permitir:

1. Utilização de cache, ou seja, arquivos que já foram analisados e não tiveram seu conteúdo alterado não serão novamente analisados;
2. Iniciar a varredura apenas quando o sistema estiver ocioso;
3. Permitir ao usuário retomar varreduras pausadas;

4.8.23.11. Deve permitir ao administrador inserir uma conta de domínio para realizar a análise de dispositivos de rede;

4.8.24. Características módulo de ameaças avançadas

4.8.24.1. A solução deve permitir o confinamento dinâmico de aplicativos e arquivos executáveis com indícios maliciosos (ransomware);

4.8.24.2. A solução deve ser capaz de avaliar aplicações desconhecidas e potencialmente maliciosas executando-as em ambiente controlado;

4.8.24.3. Deve permitir a indicação de aplicações confiáveis para que não caiam no filtro de confinamento dinâmico;

4.8.24.4. Não deve requerer conexão com centro de inteligência do fabricante para que a proteção seja ativada ou executada;

4.8.24.5. Solução deve manter um cache de reputação local com informações de aplicações - conhecidas, desconhecidas e maliciosas;

4.8.24.6. Dentre os comportamentos maliciosos, deve ser capaz de:

1. Bloquear acesso local a partir de cookies;
2. Bloquear a criação de arquivos a partir de arquivos com extensão .bat, .exe, html, hpg, jpg, bmp, job e .vbs;
3. Bloquear a criação de arquivos em qualquer local de rede;
4. Bloquear a criação de novos CLSIDs, APPIDs e TYPELIBs;
5. Bloquear a criação de threads em outro processo;
6. Bloquear a desativação de executáveis críticos do sistema operacional
7. Bloquear a leitura / exclusão / gravação de arquivos visados por ransomwares;
8. Bloquear a gravação e leitura na memória de outro processo;
9. Bloqueio de modificação da política de firewall do Windows;
10. Bloqueio de modificação da pasta de tarefas do Windows;
11. Bloqueio de modificação de arquivos críticos do Windows e Locais do Registro;
12. Bloqueio de modificação de arquivos executáveis portáteis;
13. Bloqueio de modificação de bit de atributo oculto;
14. Bloqueio de modificação de bit de atributo somente leitura;
15. Bloqueio de modificação de entradas de registro de DLL AppInit;
16. Bloqueio de modificação de locais do registro de inicialização;
17. Bloqueio de modificação de pastas de dados de usuários;
18. Bloqueio de modificação do local do Registro de Serviços;
19. Bloqueio de Suspensão de um processo;
20. Bloqueio de Término de outro processo;

4.8.24.7. Dos comportamentos observados, deve ser possível bloquear

ou apenas informar caso o mesmo ocorra;

4.8.24.8. Deve ser capaz de informar ao usuário as ameaças encontradas através de mensagem customizada;

4.8.24.9. O modo de ativação do confinamento dinâmico para quaisquer arquivos desconhecidos acessados pelo sistema operacional e nunca antes visto pela solução;

4.8.24.10. Deve ser possível atribuir a regra conforme política equilibrada, visando maior segurança ou produtividade do usuário;

4.8.24.11. A proteção deve estar contida no mesmo agente de proteção, não requerendo outro software ou aplicação adicional na estação de trabalho para a execução e ativação da proteção;

4.8.24.12. Deve possuir capacidade de inspecionar arquivos suspeitos e detectar comportamentos maliciosos utilizando técnicas de "machine-learning";

4.8.25. Módulo para controle de dispositivos removíveis

4.8.25.1. Controlar o modo como os usuários copiam dados em drives USB, iPods, CDs regraváveis e DVDs, disquetes, dispositivos Bluetooth e IrDA, dispositivos de leitura de imagens, portas COM e LPT e outros;

4.8.25.2. Especificar quais dispositivos podem ou não ser usados por qualquer parâmetro de dispositivo, inclusive códigos de produtos, códigos de fornecedor, números de série, classes de dispositivos, nomes de dispositivos;

4.8.25.3. Coletar dados de incidentes tais como dispositivo, data/hora, evidências de dados e outros, para reação, investigação e auditoria;

4.8.25.4. Permitir regra de reação para unidades de mídia removível (ex.: pendrive) com as opções de bloqueio total, somente leitura e monitoramento;

4.8.25.5. Monitorar automaticamente o uso e bloquear todas as tentativas de uso dos dispositivos ou transferência de dados contrários às políticas definidas;

4.8.25.6. Integração com a ferramenta de gerenciamento centralizado para a coleta de dados essenciais de uso, tais como dispositivo, data/hora e evidências de dados;

4.8.25.7. Integração com estrutura de Active Directory para criação de regras baseadas em usuários ou grupos de usuários;

4.8.25.8. Bloquear a remoção do agente da estação mediante senha fornecida pelo administrador;

4.8.26. Características do módulo de gerenciamento centralizado

4.8.26.1. Deve suportar a instalação nos seguintes sistemas operacionais:

1. Windows Server 2019 e superiores;
2. Windows Server 2016 e superiores;
3. Desejável a instalação e execução em Windows Server 2012 Release 2 e superiores;
4. Desejável a instalação e execução em Windows Server 2012;
5. Desejável a instalação e execução em Windows Server 2008 Service Pack 2 (SP2) Standard, Enterprise ou Datacenter;
6. Desejável a instalação e execução em Windows Server 2008 R2 Standard, Enterprise ou Datacenter;
7. Desejável o fornecimento de um appliance pela Contratada, ou seja, um arquivo para instalação virtual ou hardware que contemple os requisitos listados neste Termo de Referência;

4.8.26.2. A arquitetura dos Sistemas Operacionais deve ser 64-bits;

4.8.26.3. Deve suportar a instalação em cluster Microsoft;

4.8.26.4. Deve suportar Ipv4 e Ipv6;

4.8.26.5. Deve suportar a virtualização do sistema operacional com base nos seguintes hypervisors:

1. Vmware ESX
2. Citrix Xen Server
3. Microsoft Hyper-V

4.8.26.6. Deve possuir suporte a base de dados:

1. SQL Server 2012 ou superior;
2. Desejável suporte a MySQL versões Standard ou Enterprise 5.7 ou superior, 32 ou 64 bits;
3. Desejável suporte a MariaDB Server 10.3 32 ou 64 bits;

4.8.26.7. A console de gerência deve ser acessada via WEB;

4.8.26.8. Deve possuir compatibilidade com os seguintes browsers:

1. Google Chrome;
2. Firefox;
3. Internet Explorer 7 ou superior;
4. Safari 6.0 ou superior;
5. Microsoft Edge;

4.8.26.9. Deve ser possível segregar a instalação da solução em:

1. Servidor Console Central
2. Servidor Base de Dados
3. Servidor de Interação com os Agentes
4. Agentes Distribuidores de Vacina

4.8.26.10. Deve suportar o uso do SQL Server em ambientes SAN;

4.8.26.11. Permitir a instalação dos Módulos da Solução a partir de um único servidor;

4.8.26.12. Permitir a alteração das configurações Módulos da Solução nos clientes de maneira remota;

4.8.26.13. Possuir a integração com o gerenciamento da solução de segurança de estações de trabalho e servidores, deste mesmo fabricante a fim de prover uma única console de gerenciamento centralizado de todas as soluções de segurança que possam ser utilizadas pela CONTRATANTE nesta contratação presente ou futura;

1. Permitir a atualização incremental da lista de definições de vírus nos clientes, a partir de um único ponto da rede local.

4.8.26.14. Visualização das características básicas de hardware das máquinas;

4.8.26.15. Integração e Importação automática da estrutura de domínios do Active Directory já existentes na rede local;

4.8.26.16. Permitir a criação de tarefas de atualização, verificação de vírus e upgrades em períodos de tempo pré-determinados, na inicialização do Sistema Operacional ou no logon na rede;

4.8.26.17. Permitir o armazenamento das informações coletadas nos clientes em um banco de dados centralizado;

4.8.26.18. Permitir diferentes níveis de administração do servidor, de maneira independente do login da rede;

4.8.26.19. Suporte a múltiplos usuários, com diferentes níveis de acesso e permissões aos produtos gerenciados;

4.8.26.20. Criação de grupos de máquinas baseadas em regras definidas em função do número IP do cliente;

4.8.26.21. Permitir a criação de grupos virtuais através de marcadores;

4.8.26.22. Permitir aplicar as marcações nos sistemas por vários critérios incluindo: produtos instalados, versão de sistema operacional, quantidade de memória, dentre outros;

4.8.26.23. Forçar a configuração determinada no servidor para os clientes;

4.8.26.24. Caso o cliente altere a configuração, a mesma deverá retornar ao padrão estabelecido no servidor, quando a mesma for verificada pelo agente.

4.8.26.25. A comunicação entre as máquinas clientes e o servidor de gerenciamento deve ser segura usando protocolo de autenticação HTTPS;

4.8.26.26. Forçar a instalação dos Módulos da Solução nos clientes;

4.8.26.27. Caso o cliente desinstale os Módulos da Solução, os mesmos deverão ser reinstalados, quando o agente verificar o ocorrido;

4.8.26.28. A solução deverá ser capaz de desinstalar versões antigas e soluções de antivírus (agentes e endpoints) de terceiros;

1. O módulo de gestão deverá realizar a gestão, de no mínimo, as seguintes soluções propostas neste termo de referência:
    1. Solução para proteção de estações de trabalho e servidores;
    2. Desejável solução para resposta a incidentes;
    3. Desejável Solução para proteção de servidores críticos;
    4. Deve ser possível realizar a customização dos relatórios gráficos gerados;
    5. Exportação dos relatórios para os seguintes formatos: HTML, CSV, PDF, XML;
    6. Geração de relatórios que contenham as seguintes informações:
        1. Máquinas com a lista de definições de vírus desatualizada;
        2. Qual a versão do software (inclusive versão gerenciada pela nuvem) instalado em cada máquina;
        3. Os vírus que mais foram detectados;
        4. As máquinas que mais sofreram infecções em um determinado período de tempo;
        5. Os usuários que mais sofreram infecções em um determinado período de tempo;
    7. Gerenciamento de todos os módulos da suíte.
    8. A solução de gestão deve possuir dashboards no gerenciamento da solução;
    9. Estes dashboards devem conter no mínimo todos os seguintes relatórios de fácil visualização:
        1. Relatório dos últimos 30 dias da detecção de códigos maliciosos;
        2. Top 10 Computadores com Infecções;
    10. Gerenciar a atualização do antivírus em computadores portáteis (notebooks), automaticamente, mediante conexão em rede local ou remota (VPN);
    11. Suportar o uso de múltiplos repositórios para atualização de produtos e arquivo de vacina com replicação seletiva;
    12. Ter a capacidade de gerar registros/logs para auditoria
    13. A solução de gerenciamento deve ter a capacidade de atribuir etiquetas as máquinas, facilitando assim a distribuição automática dentro dos grupos hierárquicos na estrutura de gerenciamento.
    14. A solução de gerenciamento deve permitir acesso a sua console via web.

4.9. Requisitos de Implantação

4.9.1. A contratada deverá efetuar os serviços de instalação, configuração, teste e disponibilização (customização) da solução corporativa de antivírus no ambiente físico da Universidade de Brasília.

4.9.2. Os serviços de instalação, configuração e implantação da solução corporativa de antivírus deverão ser efetuados de forma a não comprometer o funcionamento dos serviços, recursos ou equipamentos atualmente em operação.

4.9.3. Os serviços e entregas da solução corporativa de antivírus deverão ser iniciados e executados somente após prévio agendamento com a Universidade de Brasília.

4.9.4. Para a execução destes serviços, fica estabelecido o horário de funcionamento da Universidade de Brasília, das 07h às 20h, de segunda a sexta-feira. Caso haja a necessidade de execução dos serviços durante finais de semana ou mesmo em horários distintos ao estabelecido, será necessária prévia

negociação com a área responsável.

4.9.5. Em caso de ocorrerem situações sanitárias que venham a demandar o isolamento e distanciamento social dos integrantes da STI, contratante e contratada deverão elaborar estratégias para implantar a solução por meio remoto, respeitando as eventuais limitações e necessidades de ambas as partes, e levando em consideração também as resoluções administrativas.

4.9.6. A Contratada deverá implantar a versão estável mais recente dos módulos e de seus agentes nas estações de trabalho e na rede.

4.9.7. A Contratada deverá instalar o Software Servidor de Gerenciamento do Antivírus em sua última versão estável.

4.9.8. Na conclusão de cada uma das etapas deverá ser apresentado um relatório que será aprovado pela a equipe da Universidade de Brasília, que emitirá um termo de aceitação da fase.

4.10. Requisitos de Garantia e Suporte

4.10.1. Esses requisitos são para TODOS os itens deste Termo de Referência.

4.10.2. A garantia, e suporte técnico compreendem o conjunto de serviços técnicos para manter a solução em perfeito funcionamento, com as versões de software plenamente atualizadas, de acordo com as especificações do fabricante, sem qualquer ônus para a UnB;

4.10.3. A garantia e suporte terão um prazo de 36 (trinta e seis) meses para toda a solução adquirida neste termo de referencia e será prestada nas dependências da Universidade de Brasília onde a STI determinar;

4.10.4. A garantia poderá ser prestada pela contratada ou por representante indicada pela contratada ou pelo fabricante da solução, sem prejuízo a responsabilidade integral da contratada quanto aos atendimentos dos níveis de serviço;

4.10.5. Os serviços de garantia serão solicitados mediante abertura de chamado via "on site" do fabricante ou chamada local gratuita ao fabricante ou a empresa autorizada, devendo os serviços estarem disponíveis em tempo integral (24 horas do dia x 7 dias da semana x 365 dias do ano);

4.10.6. O serviço de suporte técnico deverá ser efetuado segundo as melhores práticas do fabricante, visando sempre o máximo desempenho, disponibilidade e segurança, por técnico certificado por este, de modo a garantir total interoperabilidade no ambiente computacional;

4.10.7. É facultada a contratada a execução, ao seu planejamento e disponibilidade, de garantia do tipo preventiva que pela sua natureza reduza a incidência de problemas que possam gerar garantia do tipo corretiva. As manutenções do tipo preventiva e evolutiva não podem gerar custos a contratante;

4.10.8. A contratada deverá responder pela configuração, ativação e implementação de todas as atualizações necessárias ao bom funcionamento dos equipamentos e soluções nas manutenções corretivas, preventivas ou evolutiva solicitadas pelo contratante, sem qualquer ônus para a UnB;

4.10.9. A contratada deverá responder pela correção de problemas na solução pertencente ao ambiente instalado, atendendo integralmente as características e as necessidades da STI e responsabilizando-se por todo o material, equipamentos, acessórios e mão de obra necessária para o seu bom funcionamento, sem qualquer ônus para a UnB;

4.10.10. Chamados relacionados a software poderão ser atendidos, preferencialmente, na modalidade de atendimento remoto, podendo ocorrer a critério da contratada a comutação da modalidade para atendimento presencial, conforme a necessidade, urgência e criticidade da solicitação;

4.10.11. As atividades deverão ser apresentadas e detalhadas por meio de ordens de serviço, previamente ao início das atividades;

4.10.12. Sempre ao final de um atendimento deve ser enviado por meio digital um relatório informando o que foi executado, garantindo assim que a UnB tenha também uma copia em sua posse, não dependendo de algum sistema da CONTRATADA para ter esses relatórios;

4.11. Requisitos de Experiência Profissional

4.11.1. Por tratar-se de um ambiente computacional heterogêneo e com diversas cargas de missão crítica, será necessário a CONTRATADA comprovar as exigências mínimas descritas abaixo, em momento anterior a instalação dos equipamentos, softwares ou a execução dos serviços e atividades de implantação da solução contratada:

4.11.1.1. Ao menos um órgão de estrutura semelhando a da UnB que já tenha sido instalado e configurado os softwares do Edital;

4.11.1.2. No mínimo 2 (dois) técnicos profissionais capacitados e certificados na linha de produtos proposta;

4.11.1.3. Caso o fabricante não possua certificação específica para a linha de produtos, serão aceitos profissionais comprovadamente capacitados e aprovados em treinamento formal do fabricante;

4.11.1.4. A comprovação de que os profissionais compõem o quadro permanente da CONTRATADA se fará mediante a apresentação de cópia da Carteira de Trabalho (CTPS) ou do contrato social da CONTRATADA, no caso de sócio, ou contrato de prestação de serviços pelo prazo de vigência do contrato;

4.11.1.5. Os serviços devem ser realizados por pessoal técnico especializado do fabricante, com habilitação específica na tecnologia envolvida, ou por profissional da CONTRATADA que detenha todas as condições técnicas (teóricas e práticas) necessárias, inclusive o reconhecimento desta condição pelo fabricante da solução;

4.11.1.6. A configuração/instalação do software deverá ser realizada por profissional qualificado/certificado pelo fabricante do software envolvido;

4.11.1.7. As certificações dos funcionários da proponente deverão ser comprovadas mediante apresentação de certificado emitido pelo fabricante do software em questão e registro em carteira de trabalho ou contrato de prestação de serviços entre o profissional e a proponente.

4.12. Requisitos de Metodologia de Trabalho

4.12.1. As atividades de implantação se darão mediante atuação de funcionários da contratada para as atividades de instalação, configuração e testes da solução fornecida, nas dependências da contratante em modalidade presencial ou remota;

4.12.2. As atividades de manutenção corretiva e preventiva, bem como ações de assistência e suporte técnico serão desempenhadas nas dependências da contratante em modalidade presencial ou remota.

4.12.3. O acionamento de possíveis falhas identificadas na execução dos serviços será via central de atendimento por telefone, e-mail, pela web ou por qualquer outro meio definido ou aceito pela CONTRATANTE.

4.12.4. Para efeito de contabilização e medição dos resultados, todos os registros provenientes da CONTRATANTE sobre eventuais não cumprimentos dos níveis de serviço poderão ser feitos de imediato na central de atendimento por meio de solicitação explícita de registro de incidente informando data e horário inicial do incidente, serviço e ativos impactados.

4.13. Requisitos de Segurança da Informação

4.13.1. A CONTRATADA será expressamente responsabilizada quanto à manutenção de sigilo absoluto sobre quaisquer dados, informações, códigos-fonte e artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela CONTRATANTE a tais documentos.

4.13.2. A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto sem autorização por escrito da CONTRATANTE, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos.

4.13.3. Cada profissional da CONTRATADA que desempenhar atividades de implantação, suporte e manutenção deverá assinar termo de responsabilidade e sigilo, comprometendo-se a não divulgar nenhum assunto tratado nas dependências da CONTRATANTE ou a serviço desses, salvo se expressamente autorizado, ANEXO III - TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO.

4.13.4. Serão consideradas como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. Abrange toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE.

4.13.5. As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto.

4.13.6. As obrigações constantes do Termo de Confidencialidade da Informação não serão aplicadas às INFORMAÇÕES que sejam comprovadamente

de domínio público no momento da revelação, tenham sido comprovadas e legitimamente recebidas de terceiros e estranhos, sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

4.13.7. A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

4.13.8. A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção aos empregados que atuarão direta ou indiretamente na execução do CONTRATO sobre a existência deste Termo de Confidencialidade da Informação, bem como da natureza sigilosa das informações.

4.14. **Classificação da Natureza dos Serviços**

4.14.1. A definição de **serviços de execução continuada** informa que são aqueles que se prolongam no tempo e são prestados de maneira permanente, cuja interrupção implicaria possíveis danos e prejuízos à Administração.

4.14.2. Sendo assim, e conforme exposto neste documento, os serviços objeto deste Termo de Referência se **caracterizam como serviços de natureza continuada**, visto que sua interrupção poderia causar danos a instituição, sendo necessários sua execução ao longo de tempo para garantir a proteção e integralidade dos dados forma preventiva, detectando ameaças antes mesmo que elas sejam instaladas e iniciem suas ações, bem como remediando possíveis problemas após a infecção.

5. RESPONSABILIDADES

5.1. Deveres e responsabilidades da CONTRATANTE

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

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

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

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

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

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

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

5.1.8. Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos 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;

5.1.9. Permitir acesso aos profissionais da empresa CONTRATADA às suas dependências, sempre que necessário à execução contratual;

5.1.10. Fornecer à CONTRATADA todo tipo de informação interna essencial à realização dos serviços, atentando ao quesito de segurança e sigilo de dados;

5.1.11. Prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos da empresa CONTRATADA;

5.1.12. Notificar a CONTRATADA, por escrito, em todas as ocorrências atípicas registradas durante a execução do objeto contratado;

5.1.13. Fornecer ou estabelecer em conjunto com o licitante vencedor a agenda de manutenções programadas;

5.1.14. Assistir e homologar os serviços prestados, conforme definido em Contrato;

5.1.15. Rejeitar, no todo ou em parte, a execução do objeto prestado em desacordo com o escopo e especificações técnicas estabelecidas no Termo de Referência;

5.1.16. Fiscalizar toda a execução contratual, como forma de assegurar o cumprimento de todas as condições estabelecidas no Termo de Referência;

5.1.17. Liquidar o empenho e efetuar o pagamento à CONTRATADA de acordo com a forma e prazo estabelecidos, exigindo a apresentação das Notas Fiscais/Faturas e, quando for o caso, de relatórios de execução dos serviços/medições.

5.2. Deveres e responsabilidades da CONTRATADA

5.2.1. Indicar formalmente preposto, que pela natureza do contrato não necessitará permanecer no local da execução do contrato, todavia, que deverá estar apto a representá-la junto à CONTRATANTE, bem como responder pela fiel execução do contrato, no que tange às obrigações da contratada;

5.2.2. 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, ou irregularidade verificada, inclusive resultante de imperfeições técnicas ou de qualidade, respondendo civil e criminalmente, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;

5.2.3. 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;

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

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

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

5.2.7. Cumprir fielmente toda a execução do objeto, conforme os prazos, condições e especificações previamente estabelecidas neste Termo de Referência, mantendo durante toda a execução do contrato as mesmas condições da habilitação;

5.2.8. Comunicar à CONTRATANTE por escrito e em tempo hábil, qualquer anormalidade que esteja impedindo ou dificultando a execução do objeto, prestando os esclarecimentos julgados necessários;

5.2.9. Prover a CONTRATANTE das informações necessárias à execução do objeto;

5.2.10. Responsabilizar- se por todos os tributos, contribuições fiscais e para fiscais que incidam ou venham a incidir, direta ou indiretamente sobre os serviços fornecidos, bem como por quaisquer outros custos inerentes à execução do objeto, apresentando os documentos fiscais em conformidade com a legislação vigente;

5.2.11. Assumir todas as eventuais despesas com transporte, hospedagem e outros custos operacionais decorrentes da execução do objeto, inexistindo qualquer possibilidade de pedido de reembolso à CONTRATANTE;

5.2.12. Manter, durante todo o período de vigência do contrato, todas as condições que ensejaram sua contratação;

5.2.13. Cumprir as atividades inerentes ao objeto contratado, com profissionais devidamente habilitados, treinados e qualificados, assumindo total e exclusiva responsabilidade pelo integral atendimento de toda a legislação aplicável ao serviço de que trata o presente instrumento;

5.2.14. Cumprir e obedecer às normas internas de segurança, de acesso e permanência nas instalações da CONTRATANTE, quando necessária à execução do objeto;

5.2.15. Assumir toda a responsabilidade pelos encargos fiscais, comerciais, previdenciários e trabalhistas resultantes da execução do objeto;

5.2.16. Fornecer novas versões e atualizações do aplicativo se houver, sem custos adicionais à CONTRATANTE;

5.2.17. Fornecer a seus profissionais técnicos todos os recursos materiais necessários à plena execução do objeto seja remota ou presencialmente;

5.2.18. Entregar à CONTRATANTE, às suas expensas, todas as documentações técnicas (relatórios de serviços) gerados em função da execução do contrato;

5.2.19. Responder por eventuais danos patrimoniais de quaisquer naturezas, causados por ação ou omissão de seus profissionais na execução dos serviços, sendo garantida a ampla defesa;

5.2.20. Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando em decorrência da espécie forem vítimas seus empregados ou terceiros na

execução dos serviços ou em conexão com eles, ainda que acontecido nas dependências da CONTRATANTE;

5.2.21. Velar para que todos os privilégios de acesso ao sistema, dados ou informações da CONTRATANTE sejam utilizados exclusivamente na execução dos serviços e pelo período estritamente essencial à realização deles;

5.2.22. Refazer ou corrigir serviços contratados, no todo ou em parte, e às suas expensas, sempre que identificado pela CONTRATANTE ter sido realizado em desacordo com o estabelecido em Contrato ou no Termo de Referência;

5.2.23. Acatar as instruções e observações oriundas das avaliações da CONTRATANTE quanto aos produtos entregues, refazendo, sem ônus, qualquer trabalho não aceito;

5.2.24. Responsabilizar-se pelo sigilo e confidencialidade, por si e seus empregados, dos documentos e/ou informações que lhe chegarem ao conhecimento por força da execução do contrato, e tenham sido definidas como confidenciais, não podendo divulgá-lo, sob qualquer pretexto, conforme as diretrizes estabelecidas pela Política de Segurança da Informação e Comunicações da Universidade;

5.2.25. Manter durante o período de vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação quanto à situação de regularidade da empresa exigidas no ato da contratação;

5.2.26. Disponibilizar uma infraestrutura de atendimento via telefone, para recebimento e registro dos chamados técnicos realizados pela CONTRATANTE, disponibilizando sempre um número de protocolo para controle de atendimento;

5.2.27. Ao final de cada serviço de assistência técnica e atualização de versão, apresentar relatório de visita contendo a data e hora do chamado, do início e do término do atendimento, bem como a identificação da ocorrência e as providências adotadas;

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

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

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

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

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

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

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

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

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

5.3.9. 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;

6. MODELO DE EXECUÇÃO DO CONTRATO

6.1. Rotinas de Execução

6.1.1. A contratante poderá solicitar uma reunião inicial, ou dispensá-la, e caso a reunião seja solicitada deverá obedecer ao seguinte rito:

6.1.1.1. A reunião inicial será o encontro entre representantes das partes que deverá ser realizada após a assinatura do contrato, na qual devem ser apresentados os representantes tanto da contratada quanto da contratante, com o objetivo de alinhar o início da execução do contrato;

6.1.1.2. A contratada deverá apresentar o Preposto, bem como os demais colaboradores necessários para a execução do contrato e a contratante deverá apresentar o Gestor e os fiscais do contrato, sendo estes indispensáveis nessa reunião;

6.1.1.3. A contratante responderá a todas as dúvidas da contratada relativas ao contrato;

6.1.1.4. A reunião acontecerá nas dependências da contratante, conforme agendamento realizado com todos os participantes. Cabe também a contratante facultar, conforme sua própria conveniência, a realização de reunião em ambiente virtual;

6.1.2. Ao final da reunião deverá ser elaborada uma ata que deverá ser aprovada por todos os participantes da reunião;

6.2. Quantidade mínima de bens ou serviços para comparação e controle

6.2.1. O quantitativo mínimo de bens e serviços entregues serão os seguintes:

6.2.1.1. Instalação da console de gerenciamento centralizado;

6.2.1.2. Instalação das licenças disponíveis na quantidade contratada no servidor, em sua totalidade;

6.2.1.3. Realização das atividades de transferência tecnológica e de conhecimento da solução.

6.3. Mecanismos formais de comunicação

6.3.1. Toda a comunicação entre a CONTRATANTE e a CONTRATADA deverá ser sempre formal, exceto em casos que justifiquem outro canal de comunicação;

6.3.2. A comunicação dar-se-á por meio de Ofícios, E-mails, Reuniões mediante elaboração de Ata ou outros que possam ser registrados;

6.3.3. O canal de comunicação entre a CONTRATANTE e a CONTRATADA, para assuntos relacionados à gestão e fiscalização contratual, ocorrerá preferencialmente por meio da figura do PREPOSTO e do Fiscal e Gestor do Contrato. O preposto é o representante da CONTRATADA junto à CONTRATANTE. O preposto poderá ser contatado mesmo fora do horário de expediente, sem ônus extra para a CONTRATANTE.

6.4. Manutenção de Sigilo e Normas de Segurança

6.4.1. 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.

6.4.2. O Termo de Confidencialidade, Sigilo e Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da CONTRATADA, e Termo de Ciência, a ser assinado por todos os empregados da CONTRATADA diretamente envolvidos na contratação, encontra-se no ANEXO III.

7. MODELO DE GESTÃO DO CONTRATO

7.1. Critérios de Aceitação

7.1.1. A entrega deve ser realizada em remessa (única), no seguinte endereço: Campus Universitário Darcy Ribeiro (UnB – Asa Norte), Prédio da Secretaria de Tecnologia da Informação, CEP 70297-400, Brasília –DF ou, a critério da contratada, poderá ocorrer a disponibilização da solução por meio digital (download, via portal web);

7.1.2. O recebimento da solução com o respectivo serviço de suporte técnico e manutenção deverão ser documentados por meio do Termo de Recebimento Provisório (ANEXO I) pelo Fiscal Técnico do Contrato, após a confirmação de que todos os produtos/serviços contratados foram executados de acordo com todos os critérios estabelecidos neste Termo de Referência.

7.1.3. Para autorização do pagamento da Nota Fiscal referente à prestação dos serviços objeto deste Termo de Referência, o Gestor do Contrato deverá emitir Termo de Recebimento Definitivo (ANEXO II) atestando a entrega da solução ou execução dos serviços de acordo com os critérios estabelecidos neste Termo de Referência.

7.1.4. O recebimento provisório ou definitivo dos serviços não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato.

7.2. Procedimentos de Teste e Inspeção

7.2.1. Da fiscalização do Contrato:

7.2.1.1. Nos termos do art. 67 Lei nº 8.666, de 1993, será designado

representante para acompanhar e fiscalizar a entrega dos itens, objeto deste Termo de Referência, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

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

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

7.2.1.4. Para efeitos desta contratação, serão considerados os atores previstos na Instrução Normativa nº 01 de 04 de abril de 2019 do ME/SGD:

1. Gestor do Contrato: servidor com atribuições gerenciais, preferencialmente da Área Requisitante da solução, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente;

2. Fiscal Técnico do Contrato: servidor representante da Área de TIC, indicado pela autoridade competente dessa área para fiscalizar tecnicamente o contrato;

3. Fiscal Administrativo do Contrato: servidor representante da Área Administrativa, indicado pela autoridade competente dessa área para fiscalizar o contrato quanto aos aspectos administrativos;

4. Fiscal Requisitante do Contrato: servidor representante da Área Requisitante da solução, indicado pela autoridade competente dessa área para fiscalizar o contrato do ponto de vista de negócio e funcional da solução de TIC;

5. Preposto: representante da contratada, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto à contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

7.3. Níveis Mínimos de Serviço Exigidos

7.3.1. Possuir suporte às arquiteturas de 32 e 64 bits;

7.3.2. Possuir suporte às plataformas Microsoft e Linux;

7.3.3. Possuir suporte ao modo Server Core;

7.3.4. Possuir suporte a sistemas virtualizados;

7.3.5. Deve ter um único agente;

7.3.6. Gerenciado por uma console única;

7.3.7. Deve ser capaz de selecionar, no mínimo, dois modos de proteção;

7.3.8. Deve ter recurso para armazenamento de arquivos removidos ou desinfetados para posterior análise, verificação ou restauração (quarentena);

7.3.9. O download das atualizações a partir do servidor centralizado deve ser capaz de buscar em outras bases ou repositórios para se manter atualizado;

7.3.10. Deve emitir relatórios customizáveis pelos usuários;

7.3.11. Deve usar baixo poder computacional do cliente ao fazer instalação nas estações de trabalho ou servidores;

7.3.12. Os processos de proteção em tempo real e varredura contra vírus e outras ameaças escaneamento de vírus não devem impactar no desempenho dos clientes;

7.3.13. As atualizações de software, bibliotecas e definições não devem apresentar impacto para os clientes;

7.3.14. Não deve emitir alertas desnecessário para os usuários.

7.4. **Sanções Administrativas**

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

7.4.1.1. Não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente quando convocado dentro do prazo de validade da proposta;

7.4.1.2. falhar na execução do contrato, pela inexecução, total ou parcial, de quaisquer das obrigações assumidas na contratação;

7.4.1.3. ensejar o retardamento da execução do objeto;

7.4.1.4. fraudar na execução do contrato;

7.4.1.5. comportar-se de modo inidôneo; ou

7.4.1.6. cometer fraude fiscal.

7.4.2. Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

7.4.2.1. **Advertência por escrito**, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;

7.4.2.2. **Multa:**

a) moratória de 0,033 % (zero, virgula zero trinta e três por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

b) compensatória de 10% (dez por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

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

7.4.2.4. **Sanção de impedimento de licitar e contratar com órgãos e entidades da União**, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos.

7.4.2.5. **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;

7.4.3. A Sanção de impedimento de licitar e contratar prevista no subitem "iv" também é aplicável em quaisquer das hipóteses previstas como infração administrativa neste Termo de Referência.

7.4.4. As sanções previstas nos subitens "7.4.2.1.", "7.4.2.3.", "7.4.2.4." e "7.4.2.5." poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

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

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

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

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

7.4.6. 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.

7.4.7. 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.

7.4.7.1. Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 15 (quinze) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

7.4.8. 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.

7.4.9. 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.

7.4.10. 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.

7.4.11. 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.

7.4.12. 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.

7.4.13. As penalidades serão obrigatoriamente registradas no SICAF.

7.5. Do Pagamento

7.5.1. O pagamento da solução com os respectivos serviços de suporte técnico e manutenção e as atividades de transferência tecnológica e de conhecimento será feito em uma única vez;

7.5.2. O pagamento será efetuado pela UnB a partir do décimo dia útil, contados da apresentação da Nota Fiscal/Fatura, contendo o detalhamento do produto entregue e/ou serviços executados e o aceite definitivo pela FUB.

7.5.3. O pagamento somente será autorizado depois de efetuado o "atesto" pelo Gestor do Contrato, condicionado este ato à verificação da conformidade da Nota Fiscal/Fatura apresentada em relação ao produto entregue e/ou serviços efetivamente prestados, devidamente acompanhada das comprovações mencionadas no Anexo XI da IN nº 05 de 2017, publicada em 26 de maio de 2017.

7.5.4. Nos termos do artigo 67 da Instrução Normativa MPOG n° 05, de 2017, será efetuada a retenção do pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a CONTRATADA:

7.5.4.1. Não produziu os resultados acordados;

7.5.4.2. Deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida; e

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

8. ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

8.1. A estimativa de preços para aquisição dos softwares objeto deste Termo de Referência foi elaborada de acordo com a Instrução Normativa SDG/ME nº 73, de 5 de agosto de 2020, e suas atualizações, observando-se, em especial, as disposições do seu art. 5º.

8.2. Para aquisição dos itens a serem licitados a estimativa de preços foi de **R$ 256.000,00 (duzentos e cinquenta e seis mil reais)**, conforme demonstra a tabela abaixo:

Item	Descrição do Bem ou Serviço	Código CATSER	Quantidade	Métrica ou Unidade	Valor Unitário	Valor Total do Item
1	Solução de segurança (software corporativo de antivírus multiplataforma) para estações de trabalho e servidores no ambiente administrativo da REDUnB.	27456	4.000	Licença	R$ 64,00	R$ 256.000,00
Valor Total da Contratação ..... R$ 256.000,00 (duzentos e cinquenta e seis mil reais)						

9. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

9.1. A licitação será por Pregão por Registro de Preços, com isto a fonte de recursos informada no momento da contratação.

Referência	Detalhamento
Fonte de recurso	A licitação será para pregão eletrônico por sistema de registro de preços, sendo a fonte será informada no momento da contratação.
Natureza de Despesa	33.90.40.06 - Serviços de TIC / Locação de Softwares
P.I.	A licitação será para registro de preços, será informado no momento da contratação.
Ação	A licitação será para registro de preços, será informado no momento da contratação.
PTRES	A licitação será para registro de preços, será informado no momento da contratação.
Cronograma físico-financeiro	A licitação será para registro de preços, as aquisições ocorrerão ao longo da vigência da Ata de registro de preços, que será de 12 (doze) meses a partir de sua assinatura.

Impacto econômico-financeiro	O impacto financeiro será distribuído ao longo dos 12 (doze) meses de vigência da Ata, afetando o orçamento destinado a cada unidade de FUB que possui orçamento com detalhamento especifico para atender suas despesas.

10. DA VIGÊNCIA DO CONTRATO

10.1. Para o fiel cumprimento das obrigações, será lavrado Contrato a ser celebrado entre CONTRATANTE e CONTRATADA, com vigência de 36 (trinta e seis) meses, nos termos de inciso IV do art. 57 da Lei nº 8.666/1993, a contar de sua assinatura, podendo ser prorrogado até limite o máximo de60 (sessenta)meses mediante aditamentos ao instrumento original, havendo interesse e manifestação expressa das partes, assim como condições mais vantajosas para a Administração, em obediência aos ditames do inciso II do art. 57, da Lei n.º 8.666/1993.

10.2. A execução do contrato será iniciada a partir da assinatura do contrato pelas partes.

11. DO REAJUSTE DE PREÇOS

11.1. Em caso de reajuste de preços, deverão ser atendidos os critérios definidos pelo artigo 19, inciso XXII da Instrução Normativa nº 3 da SLTI/MPOG, de 15 de outubro de 2009.

11.2. O critério de reajuste de preços, observado o disposto no art. 40, inciso XI da Lei nº 8.666, de 1993, admitindo-se a adoção de índices específicos ou setoriais para as contratações de serviço continuado sem a dedicação exclusiva da mão de obra.

11.3. O preço inicialmente contratado deverá ser reajustado anualmente, a contar da data da proposta comercial, de acordo com a variação do ICTI – Índice de Custo da Tecnologia da Informação, calculado pelo IPEA.

11.4. Deverá ser aplicado o índice do mês anterior ao do pagamento da fatura sobre o índice base.

12. DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

12.1. **Regime, tipo e Modalidade da Licitação**

12.1.1. Verifica-se que o objeto pretendido é ofertado por muitos fornecedores no mercado de TIC, e apresentam características padronizadas e usuais. Assim, pode-se concluir que o objeto é comum e, portanto, apresenta-se como melhor opção a utilização da modalidade “Pregão” sendo, preferencialmente, em sua forma eletrônica e do tipo “Menor Preço”;

12.1.2. Com isto, o regime da execução dos contratos será POR MENOR PREÇO DO ITEM, e o tipo e critério de julgamento da licitação é o MENOR PREÇO para a seleção da proposta mais vantajosa, utilizado para compras e serviços de modo geral e para contratação de bens e serviços de informática.

12.1.3. De acordo com o que dispõe o § 1º do Art. 1º do Decreto nº 10.024/2019, esta licitação deve ser realizada na modalidade de Pregão na sua forma eletrônica, com julgamento pelo critério de menor preço por item.

12.1.4. A fundamentação pauta-se na premissa que a contratação de serviços baseia-se em padrões de desempenho e qualidade claramente definidos no Termo de Referência, havendo diversos fornecedores capazes de prestá-los. Caracterizando-se como “serviço comum” conforme Art. 9º, §2º do Decreto 7.174/2010.

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

12.2. **Justificativa para a Aplicação do Direito de Preferência e Margens de Preferência**

12.2.1. Comprovação de aptidão para o fornecimento de bens em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, por meio da apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.

12.2.2. No caso de apresentação de atestado de empresas privadas, não serão considerados aqueles apresentados por empresas participantes do mesmo grupo empresarial da licitante vencedora. Serão consideradas como de mesmo grupo, empresas controladas pela licitante vencedora, ou que tenham pelo menos uma pessoa física ou jurídica que seja sócia da empresa emitente e da licitante vencedora.

12.3. **Critérios de Qualificação Técnica para a Habilitação**

12.3.1. As empresas, cadastradas ou não no SICAF, deverão comprovar, ainda, a qualificação técnica, por meio de:

12.3.1.1. Comprovação de aptidão para o fornecimento dos softwares objeto deste termo de referência em características, quantidades e prazos compatíveis com o objeto, por meio da apresentação de no mínimo um

atestado de capacidade técnica fornecidos por pessoas jurídicas de direito público ou privado para cada item.

12.3.1.2. O atestado deverá comprovar a entrega mínima de 30% (trinta por cento) da quantidade solicitada neste termo de referência para o item que compõe o objeto.

12.3.1.3. Os atestados referir-se-ão a contratos já concluídos ou já decorrido no mínimo um ano do início de sua execução, exceto se houver sido firmado para ser executado em prazo inferior, apenas aceito mediante a apresentação do contrato.

12.3.1.4. Os atestados deverão referir-se as licenças de software, objeto deste Termo de Referência, no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente;

12.3.1.5. O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços.

12.3.1.6. Os documentos exigidos para habilitação relacionados nos subitens acima, deverão ser apresentados em meio digital pelos licitantes, por meio de funcionalidade presente no sistema (upload), no prazo mínimo de até 02 (duas) horas após solicitação do Pregoeiro no sistema eletrônico.

12.3.1.7. Somente mediante autorização do Pregoeiro e em caso de indisponibilidade do sistema, será aceito o envio da documentação por meio do e-mail sti.licitacao@unb.br.

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

13. DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

13.1. A Equipe de Planejamento da Contratação foi instituída e alterada pelos Ato da Secretaria de Tecnologia da Informação nº 018/2021; nº 019/2021; nº 049/2021 e nº 057/2021.

13.2. 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	**INTEGRANTE TÉCNICO**	**INTEGRANTE ADMINISTRATIVO**
Marcos Vinícius Linhares Castro Analista de TI SIAPE 1676387	David de Souza Cid Analista de TI SIAPE 2085504	Wellington Ferreira Chefe da DACTIC SIAPE 1141455

Aprovo,

AUTORIDADE COMPETENTE SECRETÁRIO DE TECNOLOGIA DA INFORMAÇÃO DA UNB Jacir Luiz Bordim SIAPE 14894991

ANEXOS DO TERMO DE REFERÊNCIA

ANEXO I - TERMO DE RECEBIMENTO PROVISÓRIO

IDENTIFICAÇÃO DA ORDEM DE SERVIÇO	
Contrato nº	
Processo nº	
Objeto do Contrato	
Contratada	
Contratante	

ESPECIFICAÇÃO DOS PRODUTOS/SERVIÇOS					
Item	**Descrição de Produtos/Serviços**	**Métrica**	**Valor Unit (R$)**	**Quantidade**	**Valor Total (R$)**
TOTAL					R$ 0,00

DOCUMENTOS ENTREGUES	
Item	**Descrição de Produtos/Serviços**
1	
2	
3	
4	
TOTAL	--

RELATO DE RECEBIMENTO PROVISÓRIO DOS SERVIÇOS
Por este instrumento, atestamos para fins de cumprimento do disposto no artigo 33, inciso I, da Instrução Normativa nº 1/2019 SGD/ME, que os serviços (ou bens), relacionados na O.S. acima identificada, foram recebidos nesta data e serão objeto de avaliação quanto aos aspectos de qualidade, de acordo com os Critérios de Aceitação previamente definidos pelo CONTRATANTE.

DE ACORDO	
_____ FISCAL TÉCNICO DO CONTRATO NOME: SIAPE:	_____ PREPOSTO DO CONTRATO NOME: SIAPE:

Brasília, _____ de _____ de 2021.

ANEXO II - TERMO DE RECEBIMENTO DEFINITIVO – TRD

IDENTIFICAÇÃO DA ORDEM DE SERVIÇO	
Contrato nº	
Processo nº	
Objeto do Contrato	
Contratada	
Contratante	

ESPECIFICAÇÃO DOS PRODUTOS/SERVIÇOS					
Item	**Descrição de Produtos/Serviços**	**Métrica**	**Valor Unit (R$)**	**Quantidade**	**Valor Total (R$)**
TOTAL					R$ 0,00

DOCUMENTOS ENTREGUES	
Item	**Descrição de Produtos/Serviços**
1	
2	
3	
4	
TOTAL	--

RELATO DE RECEBIMENTO DEFINITIVO DOS SERVIÇOS
Por este instrumento, atestamos para fins de cumprimento do disposto no art. 33, inciso VIII, da Instrução Normativa nº 1/2019 SGD/ME, que os serviços e/ou bens integrantes da Ordem de Serviço acima identificada, ou conforme definido no Modelo de Execução do contrato supracitado, atendem às exigências especificadas no Termo de Referência do Contrato acima referenciado. .

FATURAMENTO APURADO

Os serviços foram avaliados por meio da verificação das atividades registradas no Relatório de Atividades fornecido pela Contratada. Não foram registrados incidentes que afete a prestação e aceite desses serviços.

DE ACORDO	
_____ FISCAL TÉCNICO DO CONTRATO NOME: SIAPE:	_____ PREPOSTO DO CONTRATO NOME: SIAPE:

Brasília, _____ de _____ de 2021.

ANEXO III - TERMO DE CONFIDENCIALIDADE, SIGILO E COMPROMISSO

Pelo presente instrumento eu, _____ _____, CPF nº_____, RG nº _____, expedida em _____, órgão expedidor _____, prestador de serviço, ocupante do cargo _____ na empresa _____ _____, que celebrou o Contrato nº XXX/XXXX com a Universidade de Brasília,

DECLARO, para fins de cumprimento de obrigações contratuais e sob pena das sanções administrativas, civis e penais, que tenho pleno conhecimento de minha responsabilidade no que concerne ao sigilo que deve ser mantido sobre os assuntos tratados, as atividades desenvolvidas e as ações realizadas no âmbito da Universidade de Brasília, bem como sobre todas as informações que, por força de minha função ou eventualmente, venham a ser do meu conhecimento, comprometendo-me a guardar o sigilo necessário a que sou obrigado nos termos da legislação vigente.

DECLARO, ainda, nos termos da Política de Segurança da Informação e Comunicações da Universidade de Brasília, estar ciente e CONCORDO com as condições abaixo especificadas, responsabilizando-me por:

1. tratar o(s) ativo(s) de informação como patrimônio da Universidade de Brasília.
2. utilizar as informações em qualquer suporte sob minha custódia e interesse do serviço da Universidade de Brasília.
3. não utilizar ou divulgar em parte ou na totalidade, as informações de propriedade ou custodiadas, sob qualquer forma de armazenamento, pela da Universidade de Brasília sem autorização prévia do gestor ou responsável pela informação.
4. contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.
5. utilizar credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas da Universidade de Brasília.
6. responder perante à Universidade de Brasília, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação.

Brasília-DF, _____de _____de 20____.

_____ Nome do funcionário CARGO / MATRÍCULA CPF

Documento assinado eletronicamente por **Marcos Vinicius Linhares Castro**, **Analista de Tecnologia da Informação da Secretaria de Tecnologia da Informação**, em 03/12/2021, às 18:52, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

Documento assinado eletronicamente por **Wellington Ferreira, Chefe da**

Documento assinado eletronicamente por **Wellington Ferreira**, **Chefe da Divisão de Aquisições e Contratações de TIC da Secretaria de Tecnologia da Informação**, em 03/12/2021, às 19:04, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

Documento assinado eletronicamente por **David de Souza Cid**, **Analista de Tecnologia da Informação da Secretaria de Tecnologia da Informação**, em 06/12/2021, às 08:49, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

Documento assinado eletronicamente por **Francisco Jackson Alves de Freitas**, **Diretor(a) Substituto(a) da Secretaria de Tecnologia da Informação**, em 06/12/2021, às 09:39, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

A autenticidade deste documento pode ser conferida no site http://sei.unb.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7427985** e o código CRC **6EFF2B03**.

Referência: Processo nº 23106.017186/2021-96 SEI nº 7427985