

FUNDACAO UNIVERSIDADE DO MARANHAO

Termo de Referência 106/2025

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
106/2025	154041-FUNDACAO UNIVERSIDADE DO MARANHAO	MARCOS WINICIOS DOS SANTOS FERREIRA	15/06/2026 11:15 (v 0.18)
Status	ASSINADO		

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Bens de TIC	299/2025	23115.022857/2025-55

1. Condições gerais da contratação

CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Aquisição de solução de Segurança da Informação destinada à ampliação da segurança da rede corporativa da Universidade Federal do Maranhão – UFMA, compreendendo solução de Firewall de Próxima Geração (NGFW), gerenciamento centralizado de políticas de segurança, gerenciamento e correlação de logs, licenciamento, repasse de conhecimento, garantia, manutenção e suporte técnico por 60 (sessenta) meses, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

Item	Especificação	CATMAT	Métrica ou Unidade de Medida	Cód. PMC-TIC	Quantidade	Valor Unitário	Valor Total
1	Solução de Segurança Firewall NGFW – Alta Capacidade (FortiGate 1801F ou equivalente), incluindo Licenciamento UTP, Garantia e Suporte por 60 (sessenta) meses.	609340	Unidade	Não se aplica	01	R \$ 1.802.590,00	R \$ 1.802.590,00
2	Solução de Segurança Firewall NGFW – Média Capacidade (FortiGate 100F ou equivalente), incluindo Licenciamento UTP, Garantia e Suporte por 60 (sessenta) meses.	607833	Unidade	Não se aplica	10	R \$ 107.450,00	R \$ 1.074.500,00

3	Appliance Físico de Gerenciamento de Logs e Relatórios (FortiAnalyzer-300G ou equivalente), incluindo Licenciamento e Suporte por 60 (sessenta) meses.	21202	Unidade	Não se aplica	01	R \$ 278.850,00	R \$ 278.850,00
4	Appliance Virtual de Gerenciamento Centralizado de Políticas (FortiManager VM ou equivalente – licença para 10 devices/vdoms), incluindo FortiCare Premium por 60 (sessenta) meses.	21202	Unidade	Não se aplica	01	R \$ 44.500,00	R \$ 44.500,00

VALOR TOTAL ESTIMADO DA CONTRATAÇÃO: R\$ 3.200.440,00

Classificação do objeto quanto à heterogeneidade ou complexidade

1.2. Os bens objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar.

Classificação do objeto como bem de luxo

1.3. O objeto desta contratação não se enquadra como bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

Classificação do objeto quanto ao modelo de execução

1.4. O fornecimento dos bens é enquadrado como não continuado, uma vez que seu objeto consiste na aquisição de equipamentos, licenças e serviços correlatos de implantação, treinamento, garantia e suporte técnico, não caracterizando prestação continuada de serviços, conforme justificativa constante do Estudo Técnico Preliminar.

Prazo de vigência

1.5. O prazo de vigência da contratação é de 12 (doze) meses contados da assinatura do contrato ou instrumento hábil que o substitua, na forma do artigo 105 da Lei nº 14.133, de 2021.

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

2. Descrição da solução

DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

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

2.2. A solução de TIC consiste na aquisição de solução integrada de Segurança da Informação para proteção da infraestrutura tecnológica da Universidade Federal do Maranhão – UFMA, composta por Firewall de Próxima Geração (NGFW) de alta capacidade para proteção do ambiente central, Firewalls NGFW de média capacidade para atendimento das unidades descentralizadas, solução de gerenciamento centralizado de políticas de segurança, solução de gerenciamento, correlação e retenção de logs, licenciamento de funcionalidades de segurança, garantia, manutenção, suporte técnico especializado e repasse de conhecimento.

A solução deverá prover mecanismos avançados de proteção contra ameaças cibernéticas, controle de aplicações, inspeção de tráfego, prevenção e detecção de intrusões, filtragem de conteúdo, análise de ameaças, geração de relatórios gerenciais, correlação de eventos de segurança e gerenciamento centralizado dos ativos de segurança da informação da instituição.

Compõem a solução os seguintes itens:

I – 01 (uma) Solução de Segurança Firewall NGFW de Alta Capacidade (FortiGate 1801F ou equivalente), incluindo licenciamento UTP, garantia e suporte técnico por 60 (sessenta) meses;

II – 10 (dez) Soluções de Segurança Firewall NGFW de Média Capacidade (FortiGate 100F ou equivalente), incluindo licenciamento UTP, garantia e suporte técnico por 60 (sessenta) meses;

III – 01 (um) Appliance Físico de Gerenciamento de Logs e Relatórios (FortiAnalyzer-300G ou equivalente), incluindo licenciamento, garantia e suporte técnico por 60 (sessenta) meses;

IV – 01 (um) Appliance Virtual de Gerenciamento Centralizado de Políticas (FortiManager VM ou equivalente, licença para 10 devices/vdoms), incluindo FortiCare Premium por 60 (sessenta) meses.

As especificações técnicas detalhadas dos equipamentos, licenças, funcionalidades, requisitos de desempenho, garantia, suporte técnico e demais características da solução constam do ANEXO I deste Termo de Referência.

Considerando o ciclo de vida do objeto, a solução contempla fornecimento, implantação, configuração, operação assistida, transferência de conhecimento, garantia do fabricante, atualização de versões, suporte técnico especializado e substituição de componentes defeituosos durante todo o período contratual, assegurando a continuidade operacional, a disponibilidade dos serviços institucionais e a proteção dos ativos de informação da UFMA.

A solução objeto desta contratação é classificada como Solução de Tecnologia da Informação e Comunicação (TIC), enquadrada na categoria de Infraestrutura de TIC – Segurança de Redes, em conformidade com a Instrução Normativa SGD/ME nº 94/2022, observando as diretrizes da Lei nº 14.133/2021, do Estudo Técnico Preliminar e do Mapa de Riscos elaborados para a contratação.

3. Fundamentação e descrição da necessidade

FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1. A presente contratação justifica-se pela necessidade de ampliar e modernizar a infraestrutura de segurança da informação da Universidade Federal do Maranhão – UFMA, visando proteger os ativos de tecnologia da informação, os sistemas institucionais, os dados acadêmicos e administrativos e os serviços digitais disponibilizados à comunidade universitária.

A solução atualmente utilizada encontra-se próxima do limite de sua capacidade operacional, diante do crescimento da infraestrutura tecnológica da instituição, da ampliação do número de usuários, da expansão dos serviços digitais e do aumento constante das ameaças cibernéticas. Tal cenário demanda a adoção de mecanismos avançados de proteção, monitoramento, controle de tráfego, prevenção de intrusões, inspeção de aplicações, análise de comportamento e gerenciamento centralizado da segurança da rede.

A contratação contempla solução de Firewall de Próxima Geração (NGFW), gerenciamento centralizado de políticas de segurança, gerenciamento e correlação de logs, licenciamento, garantia, suporte técnico e transferência de conhecimento, possibilitando maior controle sobre os ambientes computacionais da UFMA, aumento da disponibilidade dos serviços institucionais e fortalecimento da capacidade de resposta a incidentes de segurança.

Os quantitativos definidos foram estabelecidos com base na arquitetura tecnológica atualmente utilizada pela UFMA, considerando a necessidade de proteção da infraestrutura central e das unidades descentralizadas, conforme detalhamento constante do Estudo Técnico Preliminar.

- 3.2. O objeto da contratação está previsto no Plano de Contratações Anual – PCA 2024, conforme consta das informações básicas deste Termo de Referência.
- 3.3. O objeto da contratação também está alinhado com os objetivos estratégicos institucionais e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2022-2027 da Universidade Federal do Maranhão – UFMA, conforme demonstrado abaixo.

ALINHAMENTO AOS PLANOS ESTRATÉGICOS

ID	Objetivos Estratégicos
TI-8	Intensificar ações relacionadas à segurança, privacidade e normatizações.

ALINHAMENTO AO PDTIC 2022-2027

ID	Ação do PDTIC	ID	Meta do PDTIC associada
AC.TI-178	Solução de firewall para atender as unidades fora da sede.	TI-8	Intensificar ações relacionadas à segurança, privacidade e normatizações.

4. Requisitos da contratação

Requisitos de Negócio

- 4.1. A presente contratação orienta-se pelos seguintes requisitos de negócio:
- 4.1.1. Disponibilizar solução integrada de Segurança da Informação capaz de ampliar a proteção da infraestrutura de TIC da UFMA contra ameaças cibernéticas, acessos indevidos, códigos maliciosos, ataques de rede e demais incidentes de segurança.
- 4.1.2. Garantir a proteção do tráfego de dados entre a sede e os campi da UFMA, assegurando a disponibilidade, integridade, confidencialidade e autenticidade das informações institucionais.
- 4.1.3. Possibilitar a centralização da administração, monitoramento, auditoria, correlação de eventos e gerenciamento das políticas de segurança dos ambientes protegidos pela solução.
- 4.1.4. Prover mecanismos de prevenção, detecção, análise e resposta a incidentes de segurança da informação, reduzindo riscos operacionais e fortalecendo a continuidade dos serviços institucionais.
- 4.1.5. Atender às necessidades institucionais identificadas no Estudo Técnico Preliminar e às diretrizes estabelecidas no Plano Diretor de Tecnologia da Informação e Comunicação da UFMA, especialmente quanto à ampliação da segurança dos ambientes computacionais da Instituição.

Requisitos de Capacitação

- 4.2. Será necessário treinamento à equipe que atuará com a solução. O treinamento deverá ser de no mínimo 20 (vinte) horas de duração.
- 4.2.1. O treinamento deverá contemplar, no mínimo, instalação, configuração, administração, operação, monitoramento, geração de relatórios, análise de logs, gerenciamento centralizado, configuração de VPNs, aplicação de políticas de segurança, atualização da solução, procedimentos de contingência, troubleshooting e demais funcionalidades necessárias à plena utilização da solução contratada.

Requisitos Legais

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

Requisitos de Manutenção

4.5. Devido às características da solução, há necessidade de realização de manutenções corretivas, preventivas, adaptativas e evolutivas pela Contratada, visando à manutenção da disponibilidade da solução.

4.5.1. A solução deverá contemplar suporte técnico especializado, garantia do fabricante, atualização de software, firmware, assinaturas de segurança, bases de inteligência de ameaças e substituição de componentes defeituosos durante todo o período contratual de 60 (sessenta) meses.

Requisitos Temporais

4.6. A entrega dos equipamentos deverá ser efetivada no prazo máximo de 45 (quarenta e cinco) dias corridos, a contar do recebimento da Ordem de Fornecimento de Bens (OFB), emitida pela Contratante, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante.

4.6.1. A implantação da solução deverá ser concluída em até 60 (sessenta) dias corridos após o recebimento definitivo dos equipamentos, observando cronograma previamente aprovado pela Contratante.

Requisitos de Segurança e Privacidade

4.7. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação da Contratante, e às demais normas aplicáveis à segurança da informação.

4.7.1. A solução deverá assegurar a confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade das informações processadas, observando os requisitos da Lei Geral de Proteção de Dados Pessoais (LGPD) e das normas institucionais de segurança da informação da UFMA.

Requisitos Sociais, Ambientais e Culturais

4.8. Os equipamentos devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais:

4.8.1. Os equipamentos fornecidos deverão observar, quando aplicável, critérios de sustentabilidade ambiental, eficiência energética, logística reversa e descarte ambientalmente adequado de resíduos eletroeletrônicos, em conformidade com a legislação vigente.

Requisitos da Arquitetura Tecnológica

4.9. Os equipamentos deverão observar integralmente os requisitos de arquitetura tecnológica descritos a seguir:

4.9.1. A solução deverá ser composta por plataforma integrada de Firewall de Próxima Geração (NGFW), gerenciamento centralizado de políticas de segurança, gerenciamento e correlação de logs, recursos de alta disponibilidade, atualização contínua de assinaturas e inteligência de ameaças, observando integralmente as especificações técnicas constantes do Anexo I deste Termo de Referência.

Requisitos de Projeto e de Implementação

4.10. Os equipamentos deverão observar integralmente os requisitos de projeto e de implementação descritos a seguir:

4.10.1. A Contratada deverá elaborar Plano de Projeto contendo cronograma de execução, estratégia de implantação, plano de migração, plano de testes, plano de transferência de conhecimento e documentação técnica necessária à implementação da solução, submetendo-o previamente à aprovação da Contratante.

Requisitos de Implantação

4.11. Os equipamentos deverão observar integralmente os requisitos de implantação, instalação e fornecimento descritos a seguir:

4.11.1. A implantação deverá contemplar a instalação física dos equipamentos, configuração dos componentes da solução, integração entre os equipamentos de firewall, gerenciamento centralizado e análise de logs, realização de testes operacionais, validação da solução pela Contratante, transferência de conhecimento e entrega da documentação técnica necessária à operação e sustentação do ambiente.

Requisitos de Garantia, Manutenção e Assistência Técnica

4.12. O prazo de garantia contratual dos bens, complementar à garantia legal, será de, no mínimo, 60 (sessenta) meses, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

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

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

4.15. A garantia abrange a realização de manutenção corretiva, preventiva, adaptativa e evolutiva dos equipamentos e softwares fornecidos, incluindo atualizações de firmware, assinaturas de segurança, bases de inteligência de ameaças, correções de vulnerabilidades e demais componentes necessários ao pleno funcionamento da solução.

4.16. Entende-se por manutenção corretiva aquela destinada a corrigir defeitos, falhas ou indisponibilidades apresentadas pelos equipamentos, softwares ou licenças da solução, compreendendo substituição de peças, ajustes, reparos, correções e demais procedimentos necessários ao restabelecimento das condições normais de operação.

4.17. As peças que apresentarem vício ou defeito durante o período de vigência da garantia deverão ser substituídas por outras novas, originais e de primeiro uso, com características técnicas e desempenho iguais ou superiores às originalmente fornecidas.

4.18. Uma vez notificado, o Contratado deverá iniciar o atendimento técnico em até 4 (quatro) horas para chamados críticos e adotar as providências necessárias à solução do problema, observados os níveis mínimos de serviço definidos neste Termo de Referência.

4.19. Na hipótese de necessidade de substituição de equipamento defeituoso, esta deverá ocorrer em prazo compatível com os níveis de serviço estabelecidos, sem prejuízo à continuidade dos serviços institucionais da Contratante.

4.20. Caso a indisponibilidade ultrapasse os prazos acordados para atendimento e solução, o Contratado deverá disponibilizar equipamento equivalente ou superior para utilização provisória pela Contratante, sem custos adicionais.

4.21. Os custos referentes ao transporte, remoção, substituição, reinstalação e demais procedimentos necessários à execução da garantia serão de responsabilidade exclusiva do Contratado.

4.22. O suporte técnico deverá ser prestado diretamente pelo fabricante ou por rede de assistência técnica autorizada, contemplando atendimento remoto e presencial quando necessário.

4.23. Durante toda a vigência contratual, a solução deverá permanecer coberta por licenciamento válido, assinaturas de segurança, atualizações de software, atualizações de firmware e suporte técnico especializado.

4.24. A garantia legal ou contratual do objeto possui vigência própria e desvinculada da vigência contratual, permitindo eventual aplicação das penalidades cabíveis em caso de descumprimento de suas condições.

Requisitos de Experiência Profissional

4.25. Os serviços de implantação, configuração, migração, treinamento, suporte técnico, garantia e manutenção deverão ser executados por profissionais devidamente capacitados para atuação em soluções de Segurança da Informação e redes corporativas.

4.26. Os profissionais envolvidos na implantação e suporte da solução deverão possuir qualificação técnica compatível com os produtos ofertados, incluindo conhecimento em NGFW, VPN, gerenciamento centralizado, análise de logs, monitoramento e resposta a incidentes de segurança.

Requisitos de Formação da Equipe

4.27. Os serviços deverão ser prestados por técnicos devidamente capacitados, de acordo com os critérios estabelecidos a seguir:

4.27.1. A equipe responsável pela implantação e suporte deverá possuir treinamento oficial do fabricante ou certificação técnica compatível com os produtos ofertados.

4.27.2. A Contratada deverá assegurar a disponibilidade de profissionais aptos a executar atividades de instalação, configuração, troubleshooting, atualização e sustentação da solução durante toda a vigência contratual.

Requisitos de Metodologia de Trabalho

4.28. O fornecimento dos equipamentos está condicionado ao recebimento, pelo Contratado, da Ordem de Fornecimento de Bens (OFB) emitida pela Contratante.

4.29. A OFB indicará o tipo de equipamento, a quantidade e a localidade na qual os equipamentos deverão ser entregues.

4.30. O Contratado deverá disponibilizar central de atendimento para abertura, acompanhamento e encerramento de chamados técnicos, com funcionamento 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, por meio eletrônico e telefônico.

4.31. O andamento da entrega, implantação e suporte da solução deverá ser acompanhado pelo Contratado, que dará ciência à Contratante acerca de ocorrências relevantes e das medidas adotadas.

4.32. A Contratada deverá disponibilizar mecanismos para acompanhamento dos chamados técnicos, contemplando histórico de atendimento, classificação de severidade, tempos de resposta e tempos de solução.

Requisitos de Segurança da Informação e Privacidade

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

4.33.1. Garantir a confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade das informações acessadas ou tratadas em decorrência da execução contratual.

4.33.2. Observar integralmente as disposições da Lei nº 13.709/2018 (LGPD), bem como as normas e políticas de segurança da informação vigentes na UFMA.

4.33.3. Não divulgar, compartilhar ou utilizar informações da Contratante para finalidade diversa da execução contratual.

Outros Requisitos Aplicáveis

4.34. Todos os componentes necessários ao pleno funcionamento da solução deverão ser fornecidos pela Contratada, incluindo equipamentos, licenças, assinaturas, softwares, documentação técnica, treinamento, suporte e demais serviços necessários à operacionalização da solução.

Sustentabilidade

4.35. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos:

4.35.1. Os equipamentos deverão observar, quando aplicável, requisitos de eficiência energética e boas práticas ambientais adotadas pelo fabricante.

4.35.2. A Contratada deverá observar a legislação ambiental vigente quanto à destinação adequada de componentes eletrônicos eventualmente substituídos; e

4.35.3. A Contratada deverá adotar práticas que reduzam impactos ambientais durante a execução contratual, observando as diretrizes do Guia Nacional de Contratações Sustentáveis.

Indicação de marcas ou modelos

4.36. Na presente contratação será admitida a indicação de marcas, modelos ou características técnicas equivalentes às soluções de referência constantes do Estudo Técnico Preliminar, exclusivamente para fins de definição do padrão mínimo de desempenho, compatibilidade, capacidade, integração, segurança, suporte e operacionalidade exigidos pela Administração, observando-se o disposto no art. 41 da Lei nº 14.133/2021.

Da vedação de utilização de marca/produto na execução do serviço

4.37. Não serão aceitos equipamentos, softwares, licenças ou componentes que:

4.37.1. Não possuam suporte técnico oficial do fabricante durante todo o período contratual;

4.37.2. Estejam descontinuados, em fim de vida (End of Sale - EOS), fim de suporte (End of Support - EOS/EOL) ou com previsão formal de descontinuidade durante a vigência contratual; e

4.37.3. Não atendam integralmente aos requisitos técnicos mínimos estabelecidos neste Termo de Referência e respectivos anexos.

Da exigência de carta de solidariedade

4.38. Não será exigida carta de solidariedade do fabricante para esta contratação.

Subcontratação

4.39. Não será admitida a subcontratação do objeto contratual.

Da exigência de amostra

4.40. Não será exigida apresentação de amostras para a presente contratação, considerando que a avaliação da solução será realizada mediante análise documental das especificações técnicas, catálogos oficiais dos fabricantes, datasheets, manuais, certificações e demais documentos comprobatórios exigidos no Termo de Referência.

4.41. A comprovação do atendimento aos requisitos técnicos mínimos ocorrerá durante a fase de julgamento das propostas e habilitação técnica, mediante apresentação da documentação exigida pela Administração.

4.42. A Administração poderá realizar diligências para validação das informações apresentadas pelos licitantes, inclusive junto aos fabricantes das soluções ofertadas.

4.43. A Administração poderá solicitar documentação complementar, esclarecimentos técnicos ou demonstração das funcionalidades da solução ofertada, quando julgar necessário para comprovação do atendimento dos requisitos técnicos estabelecidos neste Termo de Referência.

4.44. O não atendimento às diligências solicitadas pela Administração ou a comprovação de incompatibilidade da solução ofertada com os requisitos mínimos estabelecidos implicará a desclassificação da proposta.

4.45. A documentação técnica apresentada deverá demonstrar de forma clara, objetiva e inequívoca o atendimento às especificações constantes deste Termo de Referência.

4.46. Os resultados das análises técnicas e diligências realizadas serão registrados nos autos do processo administrativo correspondente.

4.47. Caso a documentação apresentada pelo licitante provisoriamente classificado em primeiro lugar não comprove o atendimento integral dos requisitos exigidos, será analisada a documentação do licitante subsequente, observada a ordem de classificação.

4.48. Toda documentação técnica apresentada ficará incorporada aos autos do processo para fins de instrução e fiscalização contratual.

4.49. A Administração poderá solicitar esclarecimentos adicionais sempre que julgar necessário à adequada avaliação da solução ofertada.

4.50. Todos os custos relacionados à apresentação de documentação, demonstrações, diligências ou comprovações técnicas correrão por conta exclusiva do licitante, sem qualquer ônus para a Administração.

Garantia da Contratação

4.51. Não haverá exigência de garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, considerando que o objeto consiste no fornecimento de solução integrada de segurança da informação, com pagamento condicionado ao efetivo recebimento dos bens e serviços, suporte técnico continuado, garantia do fabricante e mecanismos de fiscalização contratual suficientes para resguardar os interesses da Administração, conforme justificativa constante do Estudo Técnico Preliminar.

Informações relevantes para o dimensionamento e apresentação da proposta

4.52. A demanda da Universidade Federal do Maranhão fundamenta-se na necessidade de ampliação, modernização e fortalecimento dos mecanismos de proteção da infraestrutura tecnológica institucional, observando as seguintes características:

4.52.1. Fornecimento de solução integrada de Segurança da Informação composta por equipamentos Firewall de Próxima Geração (NGFW), plataforma de gerenciamento centralizado, solução de gerenciamento e correlação de logs, licenciamento, assinaturas de segurança, suporte técnico especializado e garantia do fabricante;

4.52.2. Implantação, configuração, integração, migração, testes, transferência de conhecimento, treinamento operacional e documentação técnica necessários à entrada em produção da solução no ambiente computacional da Universidade Federal do Maranhão; e

4.52.3. Prestação de serviços continuados de suporte técnico, manutenção corretiva, preventiva, adaptativa e evolutiva, incluindo atualizações de software, firmware, assinaturas de segurança, inteligência de ameaças e substituição de componentes defeituosos durante toda a vigência contratual.

Reserva de cotas para microempresas e empresas de pequeno porte

4.53. Não se aplica a reserva de cotas para microempresas e empresas de pequeno porte, uma vez que o objeto constitui solução tecnológica integrada e indivisível, composta por equipamentos, licenças e serviços tecnicamente interdependentes, cujo parcelamento poderá comprometer a compatibilidade, a interoperabilidade, a segurança, a garantia e a adequada execução da solução contratada.

Margem de Preferência

4.54. Não se aplica margem de preferência à presente contratação, observando-se os princípios da isonomia, da competitividade, da economicidade e da seleção da proposta apta a gerar o resultado mais vantajoso para a Administração.

4.55. As propostas deverão contemplar todos os equipamentos, licenças, assinaturas, serviços de implantação, suporte técnico, garantia, treinamento, documentação técnica e demais elementos necessários ao pleno funcionamento da solução, conforme especificações, requisitos e condições estabelecidos neste Termo de Referência e seus anexos.

5. Papéis e responsabilidades

PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da CONTRATANTE:

- 5.1.1. Nomear Gestor do Contrato, Fiscal Técnico, Fiscal Requisitante e Fiscal Administrativo para acompanhar e fiscalizar a execução contratual, nos termos da Lei nº 14.133/2021 e da IN SGD/ME nº 94/2022.
- 5.1.2. Encaminhar formalmente as demandas por meio de Ordem de Fornecimento de Bens (OFB) ou instrumento equivalente, observados os critérios estabelecidos neste Termo de Referência.
- 5.1.3. Receber provisória e definitivamente os bens e serviços fornecidos pela Contratada, após a verificação de conformidade com as especificações técnicas estabelecidas.
- 5.1.4. Fiscalizar a execução contratual sob os aspectos técnicos, administrativos e operacionais, podendo solicitar correções, adequações e esclarecimentos sempre que necessário.
- 5.1.5. Comunicar formalmente à Contratada quaisquer ocorrências, falhas, inconformidades ou irregularidades identificadas durante a execução do contrato.
- 5.1.6. Aplicar as sanções administrativas e contratuais cabíveis nos casos de descumprimento das obrigações assumidas pela Contratada.
- 5.1.7. Liquidar as despesas e efetuar os pagamentos devidos nos prazos estabelecidos contratualmente.
- 5.1.8. Exigir o cumprimento integral das especificações técnicas, dos níveis mínimos de serviço e das demais condições estabelecidas neste Termo de Referência.
- 5.1.9. Avaliar os relatórios, evidências técnicas, documentações, entregas e resultados apresentados pela Contratada.
- 5.1.10. Verificar o cumprimento dos Acordos de Nível de Serviço (ANS), quando aplicáveis, promovendo as medidas administrativas cabíveis em caso de descumprimento.
- 5.1.11. Emitir registros, pareceres e relatórios relacionados ao acompanhamento e fiscalização da execução contratual.
- 5.1.12. Exigir que os produtos, equipamentos, licenças, assinaturas e serviços fornecidos atendam integralmente às especificações previstas neste Termo de Referência.

5.2. São obrigações da CONTRATADA:

- 5.2.1. Indicar formalmente preposto apto a representá-la perante a Contratante, respondendo pela fiel execução contratual durante toda a vigência do contrato.
- 5.2.2. Atender prontamente às solicitações, orientações e determinações da equipe de fiscalização da Contratante.
- 5.2.3. Fornecer todos os equipamentos, licenças, assinaturas, serviços, documentação e demais componentes necessários à completa execução do objeto contratado.
- 5.2.4. Reparar, corrigir, remover, substituir ou refazer, às suas expensas, quaisquer bens ou serviços que apresentem falhas, defeitos ou desconformidades.
- 5.2.5. Reparar quaisquer danos causados à Administração ou a terceiros em decorrência de ação ou omissão de seus empregados, prepostos ou representantes.
- 5.2.6. Propiciar todos os meios necessários ao exercício das atividades de fiscalização contratual pela Contratante.
- 5.2.7. Manter, durante toda a execução contratual, as condições de habilitação e qualificação exigidas no certame.

- 5.2.8. Disponibilizar equipe técnica devidamente qualificada, certificada e capacitada para execução dos serviços previstos neste Termo de Referência.
- 5.2.9. Garantir a prestação dos serviços de suporte técnico, manutenção corretiva, preventiva, adaptativa e evolutiva durante toda a vigência contratual.
- 5.2.10. Executar o objeto em conformidade com a Lei nº 13.709/2018 (LGPD), adotando medidas adequadas para proteção dos dados e informações tratados durante a execução contratual.
- 5.2.11. Manter sigilo e confidencialidade sobre todas as informações, documentos, dados, configurações e ambientes tecnológicos aos quais tiver acesso em razão da execução contratual.
- 5.2.12. Não divulgar, reproduzir ou utilizar informações da Contratante para finalidades diversas da execução do contrato, sem autorização formal.
- 5.2.13. Assumir integral responsabilidade pelos encargos trabalhistas, previdenciários, fiscais, comerciais e demais obrigações decorrentes da execução contratual.
- 5.2.14. Fornecer às suas expensas todas as ferramentas, softwares, equipamentos, instrumentos, transporte e recursos necessários à execução dos serviços.
- 5.2.15. Garantir que os produtos, softwares, licenças e soluções fornecidos não violem direitos autorais, patentes, marcas, propriedade intelectual ou quaisquer direitos de terceiros.
- 5.2.16. Disponibilizar atualizações de software, firmware, assinaturas de segurança, inteligência de ameaças e demais componentes necessários ao correto funcionamento da solução durante toda a vigência contratual.
- 5.2.17. Realizar a transferência de conhecimento e a capacitação da equipe técnica da Contratante, conforme previsto neste Termo de Referência.
- 5.2.18. Fornecer toda a documentação técnica necessária à administração, operação, manutenção e sustentação da solução implantada.
- 5.2.19. Observar integralmente as normas de segurança da informação, controles de acesso e procedimentos internos adotados pela UFMA durante a execução contratual.

6. Modelo de execução do contrato

MODELO DE EXECUÇÃO DO CONTRATO

Rotinas de Execução

Do Encaminhamento Formal de Demandas

- 6.1. O Gestor do Contrato emitirá a Ordem de Fornecimento de Bens (OFB) para a entrega dos equipamentos, licenças e serviços previstos neste Termo de Referência.
- 6.2. O Contratado deverá fornecer os equipamentos, licenças e serviços observando integralmente as especificações técnicas, quantitativos e demais condições definidas na OFB.
- 6.3. O recebimento provisório e definitivo dos bens e serviços será realizado conforme critérios estabelecidos em tópico próprio deste Termo de Referência.
- 6.3.1. Após a assinatura do contrato, será realizada reunião inicial entre as partes para alinhamento dos procedimentos operacionais, cronograma de execução, definição dos canais de comunicação e apresentação dos responsáveis pela execução contratual.
- 6.3.2. Na reunião inicial, a Contratada deverá apresentar o preposto responsável pela execução contratual, bem como os documentos comprobatórios de suporte, garantia e demais requisitos exigidos neste Termo de Referência.

Forma de execução e acompanhamento do contrato

Condições de Entrega

6.4. O prazo de entrega dos equipamentos, licenças e demais componentes da solução será de até 45 (quarenta e cinco) dias corridos, contados do recebimento da Nota de Empenho ou da Ordem de Fornecimento de Bens (OFB), em remessa única.

6.5. A implantação, configuração, integração, migração e entrada em operação da solução deverá ser concluída em até 60 (sessenta) dias corridos após o recebimento definitivo dos equipamentos.

6.6. Caso não seja possível cumprir os prazos estabelecidos, a Contratada deverá comunicar formalmente as razões do atraso com antecedência mínima de 05 (cinco) dias úteis, para análise e deliberação da Contratante, ressalvados os casos fortuitos ou de força maior devidamente comprovados.

6.7. Os equipamentos deverão ser entregues no Almoxarifado Central da Universidade Federal do Maranhão – UFMA, localizado na Avenida dos Portugueses nº 1966, Cidade Universitária Dom Delgado, Vila Bacanga, São Luís /MA, CEP 65080-805.

6.8. A instalação, configuração e implantação da solução deverão ser realizadas nas dependências da Agência de Inovação, Empreendedorismo, Pesquisa, Pós-Graduação e Internacionalização e da Superintendência de Tecnologia da Informação da UFMA, ou em outro local indicado pela Contratante.

6.9. As entregas deverão ocorrer em dias úteis, no horário de funcionamento da Contratante, mediante agendamento prévio com antecedência mínima de 24 (vinte e quatro) horas.

Formas de Transferência de Conhecimento

6.10. A transferência de conhecimento deverá ser realizada observando-se os seguintes requisitos:

6.10.1. Capacitação teórica e prática da equipe técnica da UFMA quanto à administração, operação, monitoramento, troubleshooting e manutenção da solução implantada;

6.10.2. Apresentação das configurações implementadas, topologia lógica, políticas de segurança, procedimentos operacionais e melhores práticas de utilização da solução; e

6.10.3. Entrega da documentação técnica completa, incluindo diagramas, relatórios, manuais, procedimentos operacionais e demais artefatos produzidos durante a implantação.

Procedimentos de Transição e Finalização do Contrato

6.11. Os procedimentos de transição e encerramento contratual compreenderão:

6.11.1. Entrega da documentação técnica atualizada da solução;

6.11.2. Transferência de informações necessárias à continuidade operacional da solução pela equipe da Contratante; e

6.11.3. Encerramento formal das atividades mediante emissão do termo de aceite definitivo pela Contratante.

Quantidade mínima de bens ou serviços para comparação e controle

6.12. Cada Ordem de Fornecimento de Bens conterá a descrição dos itens, quantitativos, local de entrega e prazos de execução.

6.13. O fornecimento deverá contemplar integralmente todos os equipamentos, licenças, subscrições, serviços especializados, implantação, treinamento, garantia e suporte técnico previstos neste Termo de Referência.

Mecanismos Formais de Comunicação

6.14. São definidos como mecanismos formais de comunicação entre a Contratante e a Contratada:

- I) Ordem de Fornecimento de Bens – OFB;
- II) Ata de Reunião;
- III) Ofício;
- IV) Sistema de abertura de chamados da Contratada;
- V) Correio eletrônico institucional (e-mail);
- VI) Sistema Eletrônico de Informações – SEI, quando aplicável; e
- VII) Outros meios formais definidos pela Contratante durante a execução contratual.

Formas de Pagamento

6.15. Os critérios de medição, aceite e pagamento serão tratados em tópico próprio do Modelo de Gestão do Contrato.

Manutenção de Sigilo e Normas de Segurança

6.16. A Contratada deverá manter sigilo absoluto sobre quaisquer informações, dados, documentos, configurações, credenciais, registros, arquivos, equipamentos ou ambientes tecnológicos aos quais tiver acesso em razão da execução contratual.

6.17. A Contratada deverá observar integralmente a Política de Segurança da Informação da UFMA, a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018) e demais normativos aplicáveis.

6.18. O Termo de Compromisso de Manutenção de Sigilo e o Termo de Ciência deverão ser assinados pelo representante legal da Contratada e pelos profissionais diretamente envolvidos na execução contratual, conforme modelos constantes dos anexos deste Termo de Referência.

6.19. É vedada a divulgação, reprodução, compartilhamento ou utilização de quaisquer informações obtidas em decorrência da execução contratual sem autorização formal da Contratante.

6.20. A Contratada responderá civil, administrativa e penalmente por quaisquer danos decorrentes da violação das obrigações de sigilo e segurança da informação previstas neste Termo de Referência.

7. Modelo de gestão do contrato

MODELO DE GESTÃO DO CONTRATO

7.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

7.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

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

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

Reunião Inicial

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

7.6. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até 10 (dez) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

7.7. A pauta desta reunião observará, pelo menos:

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

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

7.7.3. Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

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

7.7.5. Apresentação das declarações, certificações ou documentos oficiais do fabricante, comprovando que os equipamentos, licenças, subscrições, suporte técnico e garantia ofertados atendem às exigências estabelecidas neste Termo de Referência.

Fiscalização

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

Fiscalização Técnica

7.9. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

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

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

7.12. O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

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

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

Fiscalização Administrativa

7.15. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

7.16. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência.

7.17. Além do disposto acima, a fiscalização contratual obedecerá às seguintes rotinas:

7.17.1. Verificar o cumprimento dos prazos de entrega, instalação, configuração, migração, implantação, treinamento, transferência de conhecimento e demais obrigações previstas neste Termo de Referência;

7.17.2. Acompanhar a prestação dos serviços de suporte técnico especializado, garantia do fabricante, manutenção corretiva, atualização de software, firmware, assinaturas de segurança e demais serviços contratados; e

7.17.3. Verificar a conformidade dos equipamentos, licenças, subscrições, documentação técnica, relatórios, entregáveis e níveis mínimos de serviço contratados, registrando eventuais inconformidades para adoção das medidas cabíveis.

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

Gestor do Contrato

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

7.19.1. Coordenar a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da Administração.

7.19.2. Acompanhar os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior aquelas que ultrapassarem a sua competência.

7.19.3. Acompanhar a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotar os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

7.19.4. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo Contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

7.19.5. Tomar providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso.

7.19.6. Elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.

7.19.7. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

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

Critérios de Aceitação

7.21. A avaliação da qualidade dos bens, licenças, serviços de implantação, suporte técnico e demais entregáveis, para fins de aceitação, consistirá na verificação dos critérios relacionados a seguir:

7.22. Todos os equipamentos fornecidos deverão ser novos (incluindo todas as peças e componentes presentes nos produtos), de primeiro uso, sem sinais de utilização anterior, não reconicionados, remanufaturados ou reutilizados, e em fase regular de comercialização pelo fabricante, não sendo aceitos produtos classificados como End of Sale (EOS), End of Support (EOS/EOL) ou equivalentes.

7.23. Todos os componentes dos equipamentos, softwares, licenças e funcionalidades fornecidas deverão ser plenamente compatíveis entre si e com a solução ofertada, vedada a utilização de adaptações, procedimentos improvisados ou quaisquer mecanismos que comprometam a estabilidade, segurança, desempenho ou suporte da solução.

7.24. Os equipamentos deverão ser entregues devidamente acondicionados, lacrados pelo fabricante e acompanhados dos respectivos acessórios, cabos, fontes, licenças, manuais e demais componentes necessários ao pleno funcionamento da solução.

7.25. O número de série dos equipamentos deverá ser único e válido junto ao fabricante, permitindo a identificação da garantia, do suporte técnico e da procedência dos produtos fornecidos.

7.26. Serão recusados equipamentos, componentes ou acessórios que apresentem sinais de oxidação, avarias, danos físicos, defeitos aparentes, adulterações, ausência de lacres originais ou quaisquer indícios de uso anterior.

7.27. Os produtos ofertados deverão permanecer em linha de fabricação e comercialização na data da apresentação da proposta, não sendo admitidos equipamentos descontinuados ou com previsão formal de encerramento de suporte durante a vigência contratual.

7.28. Todas as licenças, subscrições, assinaturas de segurança, atualizações de software, firmware e demais funcionalidades contratadas deverão estar devidamente registradas em nome da Contratante e habilitadas para uso durante toda a vigência contratual, não sendo admitidas versões de avaliação, demonstração ("trial"), compartilhadas ou qualquer modalidade incompatível com o licenciamento oficial do fabricante.

7.29. A Contratante poderá realizar inspeção total ou por amostragem dos equipamentos, licenças e serviços entregues, registrando em processo administrativo os resultados obtidos para fins de rastreabilidade e fiscalização contratual.

7.30. O recebimento definitivo somente ocorrerá após a verificação do atendimento integral às especificações técnicas, funcionais e operacionais estabelecidas neste Termo de Referência, incluindo a conclusão da implantação, configuração, integração, transferência de conhecimento e validação da solução em ambiente de produção.

7.31. Caso sejam identificadas inconformidades, defeitos, falhas de funcionamento ou descumprimento de requisitos previstos neste Termo de Referência, a Contratada deverá promover as correções necessárias sem qualquer ônus para a Contratante, sujeitando-se às penalidades cabíveis.

Procedimentos de Teste e Inspeção

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

7.32.1. Conferência quantitativa e qualitativa dos equipamentos, licenças, subscrições, acessórios, documentação técnica, garantias e demais componentes entregues, verificando sua conformidade com as especificações constantes deste Termo de Referência e da proposta vencedora;

7.32.2. Realização de testes funcionais para validação das funcionalidades de segurança, gerenciamento centralizado, geração de logs, monitoramento, integração com a infraestrutura da Contratante, atualização de assinaturas, operação dos recursos licenciados e demais requisitos técnicos exigidos; e

7.32.3. Verificação da correta implantação da solução, ativação das garantias e do suporte do fabricante, entrega da documentação técnica, realização da transferência de conhecimento e comprovação da plena operacionalidade da solução em ambiente de produção.

Níveis Mínimos de Serviço Exigidos

7.33. Os níveis mínimos de serviço são indicadores mensuráveis estabelecidos pela Contratante para aferir objetivamente os resultados pretendidos com a contratação. São considerados para a presente contratação os seguintes indicadores:

7.33.1. IAE – INDICADOR DE ATRASO NO FORNECIMENTO DA SOLUÇÃO

Tópico	Descrição
Finalidade	Medir o tempo de atraso na entrega dos equipamentos, licenças, serviços de implantação e demais itens constantes na Ordem de Fornecimento de Bens (OFB).
Meta a cumprir	$IAE \leq 0$. A meta definida visa garantir a entrega dos produtos e serviços constantes nas Ordens de Fornecimento de Bens dentro do prazo previsto.
Instrumento de medição	Ordem de Fornecimento de Bens (OFB), Termo de Recebimento Provisório (TRP) e Termo de Recebimento Definitivo (TRD).
Forma de acompanhamento	A avaliação será realizada mediante comparação entre o prazo previsto na OFB e a data efetiva de entrega e aceite provisório da solução.
Periodicidade	Para cada Ordem de Fornecimento de Bens emitida e encerrada com Termo de Recebimento Definitivo.
Mecanismo de cálculo (métrica)	$IAE = TEX - TEST$. Onde: IAE = Indicador de Atraso na Entrega; TEX = Tempo efetivo de execução da OFB, contado da data de início estabelecida na OFB até a data de aceite provisório da entrega; TEST = Tempo estimado para execução da OFB, conforme prazo estabelecido neste Termo de Referência.
Observações	Obs. 1: Serão utilizados dias corridos na medição. Obs. 2: Os dias com expediente parcial serão considerados normalmente para fins de apuração do indicador.
Início de Vigência	A partir da emissão da Ordem de Fornecimento de Bens (OFB).
Faixas de ajuste no pagamento e sanções	$IAE \leq 0$: pagamento integral da OFB. $1 \leq IAE \leq 30$ dias: glosa de 0,1666% por dia de atraso sobre o valor da OFB. $IAE > 30$ dias: glosa limitada a 10% do valor da OFB, sem prejuízo da aplicação das demais penalidades previstas na Lei nº 14.133/2021 e neste Termo de Referência.

8. Do reajuste

REAJUSTE, INFRAÇÕES E SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NOS PAGAMENTOS

Reajuste

8.1. Os preços inicialmente contratados são fixos e irrealizáveis no prazo de um ano contado da data do orçamento estimado, em 24/03/2026.

8.2. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados mediante a aplicação, pelo Contratante, do Índice de Custos de Tecnologia da Informação – ICTI, mantido pela

Fundação Instituto de Pesquisa Econômica Aplicada – IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

8.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

8.4. No caso de atraso ou não divulgação do(s) índice(s) de reajustamento, o Contratante pagará ao Contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

8.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

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

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

8.8. O reajuste será realizado por apostilamento.

Infrações e sanções administrativas

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

- a) der causa à inexecução parcial do contrato;
- b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
- c) der causa à inexecução total do contrato;
- d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
- e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
- f) praticar ato fraudulento na execução do contrato;
- g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

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

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

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

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

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

8.11.2. Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do item 8.9, sempre que não se justificar a imposição de penalidade mais grave.

8.11.3. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do item 8.9, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave.

8.11.4. Multa:

8.11.4.1. Moratória, para as infrações descritas na alínea “d” do item 8.9, de 0,05% (cinco centésimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 15 (quinze) dias.

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

8.11.4.2.1. O atraso superior a 25 (vinte e cinco) dias para apresentação, suplementação ou reposição da garantia autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei nº 14.133, de 2021.

8.11.4.3. Compensatória, para as infrações descritas nas alíneas “e” a “h” do item 8.9, de 10% (dez por cento) do valor total da contratação.

8.11.4.4. Compensatória, para a inexecução total do contrato prevista na alínea “c” do item 8.9, de 20% (vinte por cento) do valor total da contratação.

8.11.4.5. Compensatória, para a infração descrita na alínea “b” do item 8.9, de 15% (quinze por cento) do valor total da contratação.

8.11.4.6. Compensatória, em substituição à multa moratória para a infração descrita na alínea “d” do item 8.9, de 10% (dez por cento) do valor total da contratação.

8.11.4.7. Compensatória, para a infração descrita na alínea “a” do item 8.9, de 5% (cinco por cento) do valor total da contratação.

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

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

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

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

8.16. A multa poderá ser recolhida administrativamente no prazo máximo de 20 (vinte) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

8.17. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no art. 158 da Lei nº 14.133, de 2021.

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

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

8.18. Na aplicação das sanções serão considerados:

8.18.1. a natureza e a gravidade da infração cometida;

8.18.2. as peculiaridades do caso concreto;

8.18.3. as circunstâncias agravantes ou atenuantes;

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

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

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

8.20. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Termo de Referência ou para provocar confusão patrimonial, observados o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia.

8.21. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no CEIS e no CNEP.

8.21.1. As penalidades serão obrigatoriamente registradas no SICAF.

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

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

9. Critérios de seleção do fornecedor

FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E FORMA DE FORNECIMENTO

Forma de seleção e critério de julgamento da proposta

9.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO.

Forma de fornecimento

9.2. O fornecimento do objeto será integral.

Critérios de aceitabilidade de preços

9.3. O critério de aceitabilidade dos preços observará os valores máximos estimados constantes da pesquisa de preços que integra este Termo de Referência.

Exigências de habilitação

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

Habilitação jurídica

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

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

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

9.8. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

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

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

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

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

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

Habilitação fiscal, social e trabalhista

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

9.15. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social;

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

9.17. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho;

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

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

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

9.21. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar nº 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

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

9.23. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor;

9.24. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos dois últimos exercícios sociais, já exigíveis e apresentados na forma da lei, comprovando índices de Liquidez Geral (LG), Liquidez Corrente (LC) e Solvência Geral (SG) superiores a 1 (um), obtidos mediante as seguintes fórmulas:

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

$SG = \text{Ativo Total} / (\text{Passivo Circulante} + \text{Passivo Não Circulante})$

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

9.25. Caso a empresa interessada apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido patrimônio líquido mínimo correspondente a 10% (dez por cento) do valor total estimado da contratação.

9.26. Os indicadores fixados acima deverão ser atingidos em cada um dos dois últimos exercícios sociais, sob pena de inabilitação;

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

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

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

9.30. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

Qualificação Técnica

9.31. Comprovação de aptidão para o fornecimento de bens e serviços compatíveis com o objeto desta contratação, mediante apresentação de atestado(s) de capacidade técnica emitido(s) por pessoa jurídica de direito público ou privado.

9.31.1. Para fins da comprovação de que trata este subitem, os atestados deverão demonstrar experiência no fornecimento, instalação, configuração e suporte técnico de solução de firewall corporativo de próxima geração (NGFW) ou solução equivalente.

9.31.2. Serão admitidos, para fins de comprovação de quantitativo mínimo exigido, a apresentação e o somatório de diferentes atestados relativos a contratos executados de forma concomitante.

9.31.3. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

9.31.4. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual do contratante e local em que foi executado o objeto contratado, dentre outros documentos.

Disposições gerais sobre habilitação

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

9.33. Na hipótese de o fornecedor ser empresa estrangeira que não funcione no País, para assinatura do contrato ou do aceite do instrumento equivalente, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados ou consularizados, conforme legislação aplicável.

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

9.35. Se o fornecedor for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica e documentos que, comprovadamente, sejam emitidos somente em nome da matriz.

9.36. Serão aceitos registros de CNPJ de fornecedor matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

10. Estimativas do valor da contratação

Valor (R\$): 3.200.440,00

10.1. O custo estimado total da contratação, que corresponde ao valor máximo aceitável, é de **R\$ 3.200.440,00 (três milhões, duzentos mil, quatrocentos e quarenta reais)**, conforme custos unitários apostos na tabela do item 1.1.

11. Adequação orçamentária

ADEQUAÇÃO ORÇAMENTÁRIA

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

11.2. A contratação será atendida pela seguinte dotação orçamentária:

I – Gestão/Unidade: 15258 / Universidade Federal do Maranhão – UFMA (UG 154041);

II – Fonte de Recursos: 1000;

III – Programa de Trabalho: 5113 – Educação Superior;

IV – Ação Orçamentária: 20RK – Funcionamento de Instituições Federais de Ensino Superior;

V – Elemento de Despesa: 4.4.90.52 – Equipamentos e Material Permanente; e

VI – Plano Interno: MEATIG35ATN.

11.3. Caso haja necessidade de complementação, alteração ou atualização das informações orçamentárias durante a execução contratual, estas poderão ser formalizadas por apostilamento, observada a legislação vigente.

11.4. A dotação relativa aos exercícios financeiros subsequentes, quando aplicável, será indicada após aprovação da respectiva Lei Orçamentária Anual e liberação dos créditos correspondentes, mediante apostilamento.

12. Critérios de medição e de pagamento

CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

Recebimento do Objeto

12.1. A solução será recebida provisoriamente, de forma sumária, no ato da entrega, implantação ou disponibilização da solução, juntamente com a Nota Fiscal ou instrumento de cobrança equivalente, pelo(s) responsável(is) pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.

12.2. A solução poderá ser rejeitada, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigida, substituída ou refeita no prazo de 05 (cinco) dias úteis a contar da notificação do Contratado, às suas custas, sem prejuízo da aplicação das penalidades.

12.3. O recebimento definitivo ocorrerá no prazo de até 05 (cinco) dias úteis, contados do recebimento provisório, após a verificação da conformidade da solução, da qualidade dos serviços prestados e do cumprimento integral das exigências contratuais, mediante emissão do respectivo Termo de Recebimento Definitivo.

12.4. Para as contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021, o prazo máximo para o recebimento definitivo será de até 05 (cinco) dias úteis.

12.5. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

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

12.7. O prazo para a solução, pelo Contratado, de inconsistências na execução do objeto ou de saneamento da Nota Fiscal ou instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação da despesa, não será computado para fins do recebimento definitivo.

12.8. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança dos bens e serviços, nem a responsabilidade ético-profissional pela perfeita execução do contrato.

12.9. As atividades de implantação, configuração, parametrização, migração de dados, treinamento, suporte inicial e quaisquer outras necessárias ao pleno funcionamento da solução correrão por conta do Contratado e constituem condição para o recebimento definitivo.

Liquidação

12.10. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de até 10 (dez) dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §3º, da Instrução Normativa SEGES/ME nº 77/2022.

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

12.12. Para fins de liquidação, o setor competente deverá verificar se a Nota Fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

12.12.1. o prazo de validade;

12.12.2. a data da emissão;

12.12.3. os dados do contrato e do órgão contratante;

12.12.4. o período respectivo de execução contratual;

12.12.5. o valor a pagar; e

12.12.6. eventual destaque do valor de retenções tributárias cabíveis.

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

12.14. A Nota Fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

12.15. A Administração deverá realizar consulta ao SICAF para:

12.15.1. verificar a manutenção das condições de habilitação exigidas na contratação;

12.15.2. identificar possível razão que impeça a participação em licitação ou contratação com a Administração Pública, bem como ocorrências impeditivas indiretas.

12.16. Constatando-se, junto ao SICAF, situação de irregularidade do Contratado, será providenciada sua notificação, por escrito, para que, no prazo de 05 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa.

12.17. Não havendo regularização ou sendo a defesa considerada improcedente, o Contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do Contratado, bem como quanto à existência de pagamento a ser efetuado.

12.18. Persistindo a irregularidade, o Contratante deverá adotar as medidas necessárias à rescisão contratual, assegurada ao Contratado a ampla defesa.

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

Prazo de Pagamento

12.20. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

12.21. No caso de atraso pelo Contratante, os valores devidos ao Contratado serão atualizados monetariamente entre o termo final do prazo de pagamento e a data de sua efetiva realização, mediante aplicação do IPCA acumulado do período.

Forma de Pagamento

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

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

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

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

12.26. O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123/2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime, desde que apresente a comprovação legalmente exigida.

Antecipação de Pagamento

12.27. Não será admitida antecipação de pagamento para esta contratação.

Cessão de Crédito

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

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

12.28.2. Sem prejuízo do regular atendimento das obrigações contratuais pelo Contratado, a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário.

12.28.3. O crédito a ser pago ao cessionário será exatamente aquele que seria destinado ao Contratado pela execução do objeto contratual.

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

12.29. O disposto nesta seção não afeta as operações de crédito disciplinadas pela Instrução Normativa SEGES/MGI nº 82, de 21 de fevereiro de 2025.

13. Disposições Finais

DISPOSIÇÕES FINAIS

13.1. As informações contidas neste Termo de Referência não são classificadas como sigilosas, exceto o valor estimado da contratação, que permanecerá sigiloso até o encerramento da fase de lances, nos termos da legislação aplicável.

13.2. Considerando que o objeto será fornecido de forma integral, não se aplica cronograma físico-financeiro específico.

13.3. O pagamento será realizado após a entrega, instalação, configuração, testes, recebimento definitivo da solução e demais condições previstas neste Termo de Referência.

14. Responsáveis

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

BENEDITO MENDES DUTRA NETO

Integrante Requisitante



Assinou eletronicamente em 10/06/2026 às 16:25:29.

LUCIANO MONTEIRO DOS SANTOS

Integrante Técnico



Assinou eletronicamente em 11/06/2026 às 14:37:31.

WAGNER DUARTE DE JESUS

Integrante Técnico



Assinou eletronicamente em 15/06/2026 às 11:15:54.

CLAUDIO SANTANA PEREIRA E SILVA

Integrante Administrativo



Assinou eletronicamente em 11/06/2026 às 10:07:40.

ANILTON BEZERRA MAIA

Autoridade Máxima da Área de TIC



Assinou eletronicamente em 10/06/2026 às 18:04:17.

MARCOS MOURA SILVA

Autoridade Administrativa



Assinou eletronicamente em 11/06/2026 às 14:30:38.

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - Lista de Anexos.pdf (27.69 KB)
- Anexo II - Especificacao Tecnica.pdf.pdf (233.83 KB)
- Anexo III - Termo de Compromisso de Manutencao de Sigilo.pdf.pdf (176.86 KB)
- Anexo IV - Termo de Ciencia.pdf.pdf (116.95 KB)

ANEXO I

ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO DE TIC

1. Informações Gerais

1.1. Abaixo serão detalhadas as especificações técnicas mínimas das soluções a serem implementadas;

1.2. O projeto deverá contemplar serviço de instalação, configuração e treinamento de toda a solução;

1.3. Os equipamentos deverão possuir garantia do fabricante por um período de 60 (sessenta) meses, com disponibilidade para chamada de manutenção no regime 24x7 (24 horas por dia, 7 dias por semana);

1.4. Todas as funcionalidades da solução adquirida deverão ser mantidas, mesmo após o vencimento do prazo de garantia dos equipamentos.

1.5. Os quantitativos gerais do projeto são:

ITEM	DESCRIÇÃO COMPLETA DA SOLUÇÃO	QTD	UNIDADE DE MEDIDA	DURAÇÃO
1	Solução de Segurança Firewall NGFW – Alta Capacidade (FortiGate 1801F ou equivalente), incluindo Licenciamento UTP, Garantia e Suporte	01	Unidade	60 meses
2	Solução de Segurança Firewall NGFW – Média Capacidade (FortiGate 100F ou equivalente), incluindo Licenciamento UTP, Garantia e Suporte	10	Unidade	60 meses
3	Appliance Físico de Gerenciamento de Logs e Relatórios (FortiAnalyzer-300G ou equivalente), incluindo Licenciamento e Suporte	01	Unidade	60 meses
4	Appliance Virtual de Gerenciamento Centralizado de Políticas (FortiManager VM ou equivalente - licença para 10 devices/vdoms), incluindo FortiCare Premium	01	Unidade	60 meses

2. Características Gerais

2.1. O Firewall deverá suportar e estar licenciado para o uso das diversas ferramentas de segurança incluídas em um Next Generation Firewall, como Antivírus, IPS, Filtragem Web, Controle de Aplicações, Proteção contra Botnets, Proteção contra Malwares Avançados e AntiSpam de Gateway;

2.2. O equipamento deverá ser fornecido com licenciamento 24x7, para habilitar todas as funcionalidades por 60 meses, conforme descritas no Termo de Referência.

3. Características de Hardware

3.1. Deve suportar, no mínimo, 190 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, considerando pacotes de 512 bytes;

3.2. Deve suportar, no mínimo, 21 Gbps de throughput IPS;

3.3. Deve suportar, no mínimo, 55 Gbps de throughput de VPN IPSec;

3.4. Deve suportar, no mínimo, 10 Gbps de throughput de VPN SSL;

3.5. Deve suportar, no mínimo, 11 Gbps de throughput de Inspeção SSL;

3.6. Deve suportar, no mínimo, 33 Gbps de throughput de Controle de Aplicação;

3.7. Deve suportar, no mínimo, 14.5 Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: firewall, controle de aplicação, IPS e antimalware;

3.8. Suporte a, no mínimo, 11 milhões de conexões simultâneas;

3.9. Deve suportar o gerenciamento de no mínimo 190 Switches do mesmo fabricante por equipamento;

3.10. Suporte a, no mínimo, 700 mil novas conexões por segundo;

3.11. Estar licenciado para, ou suportar sem o uso de licença, 15 mil túneis de VPN IPSEC Site-to-Site simultâneos;

3.12. Estar licenciado para, ou suportar sem o uso de licença, 90 mil túneis de clientes VPN IPSEC simultâneos;

3.13. Estar licenciado para, ou suportar sem o uso de licença, 5 mil clientes de VPN SSL simultâneos;

3.14. Caso seja necessário fornecimento de licenças para prover o uso de VPN para a quantidade de usuários solicitada, a licença deverá operar em caráter perpétuo;

3.15. Possuir ao menos 8 interfaces 1Gbps SFP;

- 3.16. Possuir ao menos 14 interfaces 1Gbps RJ-45;
- 3.17. Possuir ao menos 10 Interfaces SFP28 de até 25Gbps, permitindo também o uso de transceivers 10Gbps SFP+ e Gigabit SFP, com fornecimento de 2 (dois) transceivers SFP + (SR 10GE);
- 3.18. Possuir ao menos 4 Interfaces 40Gbps compatível com transceivers QSFP+;
- 3.19. Deve possuir disco Onboard Storage do tipo Solid State Drive NVMe (SSD) de, no mínimo, 480 (quatrocentos e oitenta) GB de armazenamento do sistema operacional e registro de logs;
- 3.20. Deverá possuir interface USB 3.0 para exportação de backups;
- 3.21. Deverá possuir interface do tipo console para utilização de CLI;
- 3.22. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;
- 3.23. Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;
- 3.24. Possuir no máximo 2 RU de altura e acompanhar kit de instalação em rack;
- 3.25. Deverá possuir fontes de alimentação internas redundantes, do tipo hot-swappable;
- 3.26. O fabricante ofertado deve estar posicionado no quadrante “Leader” do quadrante mágico do Gartner de 2022, na categoria Network Firewalls.

4. Características Gerais de Funcionalidade

- 4.1. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
- 4.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- 4.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
- 4.4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

- 4.5. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
- 4.6. A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede;
- 4.7. Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;
- 4.8. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;
- 4.9. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;
- 4.10. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- 4.11. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
- 4.12. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
- 4.13. Os dispositivos de proteção de rede devem suportar sFlow;
- 4.14. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;
- 4.15. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet lógicas;
- 4.16. Deve suportar NAT dinâmico (Many-to-1);
- 4.17. Deve suportar NAT dinâmico (Many-to-Many);
- 4.18. Deve suportar NAT estático (1-to-1);
- 4.19. Deve suportar NAT estático (Many-to-Many);
- 4.20. Deve suportar NAT estático bidirecional 1-to-1;
- 4.21. Deve suportar Tradução de porta (PAT);
- 4.22. Deve suportar NAT de Origem;
- 4.23. Deve suportar NAT de Destino;
- 4.24. Deve suportar NAT de Origem e NAT de Destino simultaneamente;
- 4.25. Deve poder combinar NAT de origem e NAT de destino na mesma política;

- 4.26. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- 4.27. Deve suportar NAT64 e NAT46;
- 4.28. Deve implementar o protocolo ECMP;
- 4.29. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 4.30. Enviar log para sistemas de monitoração externos, simultaneamente;
- 4.31. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
- 4.32. Proteção anti-spoofing;
- 4.33. Suportar otimização do tráfego entre dois equipamentos;
- 4.34. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 4.35. Para IPv6, deve suportar roteamento estático e dinâmico (RIPng, OSPFv3, BGP4+);
- 4.36. Suportar OSPF graceful restart;
- 4.37. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 4.38. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
- 4.39. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
- 4.40. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
- 4.41. Suporte a configuração de alta disponibilidade (HA) Ativo/Passivo e Ativo/Ativo: Em modo transparente;
- 4.42. Suporte a configuração de alta disponibilidade (HA) Ativo/Passivo e Ativo/Ativo: Em layer 3;
- 4.43. Suporte a configuração de alta disponibilidade (HA) Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;
- 4.44. A configuração em alta disponibilidade (HA) deve sincronizar: Sessões;

- 4.45. A configuração em alta disponibilidade (HA) deve sincronizar: Configurações, incluindo, mas não limitado às políticas de Firewall, NAT, QOS e objetos de rede;
- 4.46. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
- 4.47. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;
- 4.48. O HA deve possibilitar monitoração de falha de link;
- 4.49. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;
- 4.50. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;
- 4.51. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;
- 4.52. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado a exportar configuração dos sistemas virtuais (contextos) por ambas as interfaces;
- 4.53. Controle, inspeção e descryptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
- 4.54. O console de administração deve suportar pelo menos inglês, espanhol e português;
- 4.55. A solução deve oferecer suporte à integração nativa de equipamentos de proteção de e-mail, firewall de aplicativos, proxy, cache e ameaças avançadas;
- 4.56. Deverá ser comprovado que a solução ofertada foi aprovada no conjunto de critérios de avaliação contido nos testes da NSS Labs, da ICSA Labs, ou por meio de certificação similar, que cumpra a mesma finalidade ou que ateste as mesmas funcionalidades.

5. Funcionalidades de Controle por Políticas

- 5.1. Deverá suportar controles por zona de segurança;
- 5.2. Controles de políticas por porta e protocolo;

- 5.3. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- 5.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- 5.5. Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;
- 5.6. Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall;
- 5.7. Ele deve suportar a automação de situações como detecção de equipamentos comprometidos, status do sistema, alterações de configuração, eventos específicos e aplicar uma ação que pode ser notificação, bloqueio de um computador, execução de scripts ou funções em nuvem pública;
- 5.8. Deve suportar o padrão de indústria 'syslog' protocol para armazenamento usando o formato Common Event Format (CEF);
- 5.9. Deve suportar o protocolo padrão da indústria VXLAN;
- 5.10. Deve suportar objetos de endereço IPv4 e IPv6, consolidados na mesma regra/política de firewall;
- 5.11. Deve possuir base com objetos de endereço IP, de serviços da internet como Google e Office 365, atualizados dinamicamente pela solução;
- 5.12. A solução deve oferecer suporte à integração nativa com a solução de sandbox, proteção de e-mail e firewall de aplicativos da Web.

6. Funcionalidades de Controle de Aplicação

- 6.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
- 6.2. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
- 6.3. Reconhecer pelo menos as seguintes aplicações: BitTorrent, gnutella, Skype, facebook, LinkedIn, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

- 6.4. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
- 6.5. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 6.6. Identificar o uso de táticas evasivas via comunicações criptografadas;
- 6.7. Atualizar a base de assinaturas de aplicações automaticamente;
- 6.8. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
- 6.9. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
- 6.10. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
- 6.11. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 6.12. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule etc.) possuindo granularidade de controle/políticas para eles;
- 6.13. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat etc.) possuindo granularidade de controle/políticas para os mesmos;
- 6.14. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
- 6.15. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos;
- 6.16. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol etc.);
- 6.17. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;
- 6.18. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
- 6.19. Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente.

7. Funcionalidades de Prevenção de Ameaças

7.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

7.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

7.3. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

7.4. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

7.5. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

7.6. Deve permitir o bloqueio de vulnerabilidades;

7.7. Deve incluir proteção contra-ataques de negação de serviços;

7.8. Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise de decodificação de protocolo;

7.9. Deverá possuir o seguinte mecanismo de inspeção de IPS: Análise para detecção de anomalias de protocolo;

7.10. Deverá possuir o seguinte mecanismo de inspeção de IPS: IP Defragmentation;

7.11. Deverá possuir o seguinte mecanismo de inspeção de IPS: Remontagem de pacotes de TCP;

7.12. Deverá possuir o seguinte mecanismo de inspeção de IPS: Bloqueio de pacotes malformados;

7.13. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood etc.;

7.14. Detectar e bloquear a origem de portscans;

7.15. Bloquear ataques efetuados por worms conhecidos;

7.16. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

- 7.17. Possuir assinaturas para bloqueio de ataques de buffer overflow;
- 7.18. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- 7.19. Identificar e bloquear comunicação com botnets;
- 7.20. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 7.21. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
- 7.22. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- 7.23. Os eventos devem identificar o país de onde partiu a ameaça;
- 7.24. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
- 7.25. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
- 7.26. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança etc., ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;
- 7.27. Suportar e estar licenciado com proteção contra ataques de dia zero por meio de integração com solução de Sandbox em nuvem, do mesmo fabricante.

8. Funcionalidades de Filtro de URL

- 8.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 8.2. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;
- 8.3. Suportar proxy Web transparente e Explicit Web Proxy;
- 8.4. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

8.5. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

8.6. Possuir pelo menos 60 categorias de URLs;

8.7. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;

8.8. Permitir a customização de página de bloqueio;

8.9. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site).

9. Funcionalidades de Identificação de Usuário

9.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;

9.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

9.3. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede etc.;

9.4. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

9.5. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

9.6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

9.7. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

9.8. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

9.9. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso à internet e gerenciamento da solução;

9.10. Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator.

10. Funcionalidades de QoS e Traffic Shaping

10.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, etc.) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

10.2. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;

10.3. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;

10.4. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;

10.5. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

10.6. Suportar a criação de políticas de QoS e Traffic Shaping por porta;

10.7. O QoS deve possibilitar a definição de tráfego com banda garantida;

10.8. O QoS deve possibilitar a definição de tráfego com banda máxima;

10.9. O QoS deve possibilitar a definição de fila de prioridade;

10.10. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

10.11. Suportar modificação de valores DSCP para o Diffserv;

10.12. Suportar priorização de tráfego usando informação de Type of Service;

10.13. Deve suportar QOS (traffic-shapping) em interface agregadas ou redundantes.

11. Funcionalidade de Filtro de Dados

11.1. Permitir a criação de filtros para arquivos e dados pré-definidos;

11.2. Os arquivos devem ser identificados por extensão e tipo;

11.3. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF etc.) identificados sobre aplicações (HTTP, FTP, SMTP etc.);

11.4. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

11.5. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

11.6. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

12. Funcionalidades de ZTNA (Zero Trust Network Access)

12.1. A solução deverá permitir a implementação futura de ZTNA através do licenciamento dos Endpoints, permitindo a ativação das seguintes funcionalidades:

12.1.1. Deverá permitir ao administrador a solicitação enforcement de identificação do usuário no login, de modo que o usuário necessite realizar uma confirmação de identidade através de no mínimo:

12.1.1.1. Informação pessoal do sistema operacional;

12.1.1.2. LinkedIn;

12.1.1.3. Google;

12.1.1.4. Salesforce;

12.1.2. Deverá permitir aplicar perfis de segurança baseado em status de serviços do endpoint, permitindo que seja atribuído um perfil de acesso para os endpoints baseado em no mínimo:

12.1.2.1. DHCP Server: Atribui um perfil de segurança se o endpoint estiver conectado a um servidor DHCP específico;

12.1.2.2. DNS Server: Atribui um perfil de segurança se o endpoint estiver conectado a um servidor DNS específico;

12.1.2.3. Conexão ao Servidor: Atribui um perfil de segurança se o endpoint estiver online e com sua versão atualizada de acordo com o servidor de gerenciamento;

12.1.2.4. Local IP/Subnet: Atribui um perfil de segurança se o endpoint estiver em um range de IPs específico;

12.1.2.5. Default Gateway: Atribui um perfil de segurança se o endpoint estiver enviando informações para um gateway de internet específico, permitindo também a configuração de endereço MAC do Gateway;

12.1.2.6. Ping Server: Atribui um perfil de segurança se o endpoint conseguir enviar um ping para um servidor específico de rede;

12.1.2.7. VPN Tunel: Atribui um perfil de segurança se o endpoint estiver acessando a rede através de um Túnel de VPN, deve ser permitida a escolha de túnel de VPN para cada perfil.

12.1.3. Deve permitir a atribuição de usuários ou grupos de usuários a políticas de acesso.

13. Geolocalização

13.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

13.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

13.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

14. Funcionalidades de VPN

14.1. Suportar VPN Site-to-Site e Cliente-To-Site;

14.2. Suportar IPSec VPN;

14.3. Suportar SSL VPN;

14.4. A VPN IPSec deve suportar Autenticação MD5 e SHA-1;

14.5. A VPN IPsec deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

14.6. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

14.7. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

14.8. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

14.9. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;

14.10. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;

14.11. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

14.12. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

14.13. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

14.14. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

14.15. Deverá manter uma conexão segura com o portal durante a sessão;

14.16. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows 10 (32 e 64 bits) e Mac OS X (v10.10 ou superior);

14.17. Deve suportar Auto Discovery Virtual Private Network (ADVPN);

14.18. Deve suportar agregação de túneis IPsec;

14.19. Deve suportar algoritmo de balanceamento do tipo WRR (Weighted Round Robin) em agregação de túneis IPsec;

14.20. A VPN IPsec deve suportar Forward Error Correction (FEC);

14.21. Deve suportar TLS 1.3 em VPN SSL.

15. Funcionalidades de SD-WAN

15.1. Deve implementar balanceamento de link por hash do IP de origem;

15.2. Deve implementar balanceamento de link por hash do IP de origem e destino;

15.3. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links;

15.4. Deve implementar balanceamento de link por custo configurado do link.

15.5. Deve suportar o balanceamento de, no mínimo, 256 links;

15.6. Deve suportar o balanceamento de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPsec;

15.7. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

- 15.8. Deve gerar log de eventos que registrem alterações no estado dos links do SDWAN, monitorados pela checagem de saúde;
- 15.9. Deve suportar Zero-Touch Provisioning;
- 15.10. Possuir checagem do estado de saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Perda de Pacotes;
- 15.11. Deve ser possível configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link. Estes valores serão utilizados pela solução para decidir qual link será utilizado;
- 15.12. A solução deve permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links;
- 15.13. A checagem de estado de saúde deve suportar teste com Ping, HTTP e DNS;
- 15.14. Suportar UDP Hole Punching em arquitetura ADVPN;
- 15.15. A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoS configurado;
- 15.16. As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de destino e Protocolo;
- 15.17. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD-WAN;
- 15.18. Deve suportar envio de BGP route-map para BGP neighbors, caso a qualidade mínima de um link não seja detectada pela checagem de saúde do link.

ANEXO II

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

Pelo presente instrumento a UNIVERSIDADE FEDERAL DO MARANHÃO (UFMA), sediado em Av. dos Portugueses, 1966 - Vila Bacanga, São Luís - MA, CEP 65080-805, CNPJ nº

06.279.103/0001-19, doravante denominado **CONTRATANTE**, e, de outro lado, a **<NOME DA EMPRESA>**, sediada em **<ENDEREÇO>**, CNPJ nº **<Nº do CNPJ>**, doravante denominada **CONTRATADA**;

CONSIDERANDO que, em razão do **CONTRATO N.º <nº do contrato>** doravante denominado **CONTRATO PRINCIPAL**, a **CONTRATADA** poderá ter acesso a informações sigilosas do **CONTRATANTE**;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação e Privacidade da **CONTRATANTE**;

Resolvem celebrar o presente **TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO**, doravante **TERMO**, vinculado ao **CONTRATO PRINCIPAL**, mediante as seguintes cláusulas e condições abaixo discriminadas.

1 – OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas disponibilizadas pela CONTRATANTE e a observância às normas de segurança da informação e privacidade por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18 de novembro de 2011, Lei nº 13.709, de 14 de agosto de 2018, e os Decretos 7.724, de 16 de maio de 2012, e 7.845, de 14 de novembro de 2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

2 – CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de

UNIVERSIDADE FEDERAL DO MARANHÃO

acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

3 – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá 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: *know-how*, 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 e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

4 – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

- I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;
- II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;
- III – 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.

5 – DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

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

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmos judiciais, inclusive as

UNIVERSIDADE FEDERAL DO MARANHÃO

despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

6 – VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

7 – PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme previsto nos arts. 155 a 163 da Lei nº. 14.133, de 2021.

8 – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

UNIVERSIDADE FEDERAL DO MARANHÃO

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações, conforme definição do item 3 deste documento, disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

9 – FORO

A CONTRATANTE elege o foro da cidade de São Luís - MA, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

10 – ASSINATURAS

UNIVERSIDADE FEDERAL DO MARANHÃO

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

CONTRATADA	CONTRATANTE
<Nome> <Qualificação>	<Nome> Matrícula: xxxxxxxx

TESTEMUNHAS	
<Nome> <Qualificação>	<Nome> <Qualificação>

<Local>, <dia> de <mês> de <ano>.

UNIVERSIDADE FEDERAL DO MARANHÃO

ANEXO II

TERMO DE CIÊNCIA

INTRODUÇÃO

O Termo de Ciência visa obter o comprometimento formal dos empregados da Contratada diretamente envolvidos na contratação quanto ao conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes no órgão/entidade.

No caso de substituição ou inclusão de empregados da contratada, o preposto deverá entregar ao Fiscal Administrativo do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados.

Referência: Art. 18, Inciso V, alínea “b” da IN SGD/ME Nº 94/2022.

1 – IDENTIFICAÇÃO

CONTRATO Nº	xxxx/aaaa		
OBJETO	<objeto do contrato>		
CONTRATADA	<nome da contratada>	CNPJ	xxxxxxxxxxxxx
PREPOSTO	<Nome do Preposto da Contratada>		
GESTOR DO CONTRATO	<Nome do Gestor do Contrato>	MATR	xxxxxxxxxxxxx

2 – CIÊNCIA

Por este instrumento, os funcionários abaixo identificados declaram ter ciência e conhecer o inteiro teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes da Contratante.

Funcionários da Contratada		
Nome	Matrícula	Assinatura
<Nome do(a) Funcionário(a)>	<xxxxxxxxxxx>	

UNIVERSIDADE FEDERAL DO MARANHÃO

<Nome do(a) Funcionário(a)>	<xxxxxxxxxx >	
...	...	...

<Local>, <dia> de <mês> de <ano>.