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	24/02/2026 15:16 (v 0.9)

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

1.1 Aquisição de soluções de Segurança da Informação com o propósito de ampliar a segurança da rede da UFMA, incluindo repasse de conhecimento, manutenção e suporte técnico por 60 (sessenta) meses de acordo com as condições e especificações constantes neste Termo de Referência termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

ITEM	ESPECIFICAÇÃO	CATMAT	UNIDADE DE MEDIDA	QTD	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	01	R$ 552.370,00	R$ 552.370,00
2	Solução de Segurança Firewall NGFW – Média Capacidade (**FortiGate 100F** ou equivalente), incluindo Licenciamento UTP, Garantia e Suporte por 60 (sessenta) meses.	607833	Unidade	10	R$ 67.000,00	R$ 670.000,00
3	Appliance Físico de Gerenciamento de Logs e Relatórios (**FortiAnalyzer-300G** ou equivalente), incluindo Licenciamento e Suporte por 60 (sessenta) meses.	21202	Unidade	01	R$ 505.536,00	R$ 505.536,00

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	01	R$ 57.665,50	R$ 57.665,50
					VALOR TOTAL	**R$ 1.785.571,50**

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

1.3. Os bens objetos desta contratação são caracterizados como comuns, conforme justificativa constante no Estudo Técnico Preliminar (ETP).

1.4. O prazo de vigência da contratação é de 60 meses, contados da data de assinatura dos referidos contratos, na forma do *artigo 105 da Lei n° 14.133, de 2021*.

1.5. A prestação dos serviços não gera vínculo empregatício entre os empregados da CONTRATADA e a Administração CONTRATANTE, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

1.6. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

1.7. Quanto ao Orçamento e Pesquisa de Preços certifica-se que:

I - Ratificação da Pesquisa: O orçamento estimado para esta contratação encontra-se devidamente detalhado no Relatório de Pesquisa de Preços nº 230/2025, o qual já contempla a revisão técnica e a ratificação dos valores de mercado para a solução de Firewall;

II - Metodologia e Memória de Cálculo: Conforme registrado no referido Relatório, a metodologia utilizada baseou-se na Mediana de preços, utilizando-se de memória de cálculo transparente e fundamentada na IN SEGES/ME nº 65/2021, garantindo a eliminação de distorções por valores inexequíveis ou excessivos;

III - Fontes Priorizadas e Análise Crítica: A instrução processual priorizou o Painel de Preços e contratações públicas similares, acompanhada de análise crítica que atestou a compatibilidade entre as especificações técnicas da solução NGFW e os preços praticados, assegurando a robustez da estimativa de R$ 1.785.571,50.

1.8. No que tange ao Mapa de Riscos informa-se que:

I - Existência e Completude: O Mapa de Riscos nº 156/2025, já acostado aos autos, apresenta-se em sua versão completa, tendo sido elaborado de acordo com as etapas de planejamento da IN 94/2022;

II - Atualização e Marcos Recomendados: O documento foi devidamente atualizado para refletir o cenário atual da contratação, contemplando os riscos de planejamento, seleção do fornecedor e gestão contratual, bem como as respectivas ações preventivas e de contingência, observando todos os marcos recomendados pela legislação vigente.

2. Descrição da solução

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. As especificações técnicas dos equipamentos constam no ANEXO I deste Termo de Referência.

2.3. 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 estrita observância ao Art. 2º, inciso II, da Instrução Normativa SGD/ME nº 94/2022 e aos ditames da Lei nº 14.133/2021, demonstrando total compatibilidade com o planejamento contido no Estudo Técnico Preliminar (ETP) e no Mapa de Riscos.

3. Fundamentação e descrição da necessidade

3.1. A fundamentação da contratação e de seus quantitativos encontram-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

3.2. O objeto da contratação está previsto no Plano de Contratações Anual 2025, conforme consta das informações básicas deste Termo de Referência.

DFD ASSOCIADO	DESCRIÇÃO DO OBJETO	NÚMERO DA CONTRATAÇÃO
42/2024	Solução de Firewall para atender as necessidades da UFMA	154041-171/2025

3.3. O objeto da contratação também está alinhado com os objetivos estratégicos e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2022-2027, conforme demonstrado abaixo:

ID	DESCRIÇÃO DO OBJETIVO ESTRATÉGICO
TI-8	Intensificar ações relacionadas a segurança, privacidade e normatizações.

ID	DESCRIÇÃO DA AÇÃO
AC.TI-178	Solução de firewall para atender as unidades fora da sede.

4. Requisitos da contratação

Requisitos de Negócio:

4.1. A solução deverá permitir a segurança dos dados pessoais e institucionais por ela utilizados.

4.2. A contratada deverá garantir a disponibilidade, integridade e confidencialidade da solução.

4.3. A solução deverá possuir suporte técnico especializado.

4.4. A solução deverá estar sempre atualizada, em sua última versão disponível, durante a vigência do contrato.

4.5. A prestação dos serviços não gerará vínculo empregatício entre os empregados da Contratada e a Administração, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

4.6. Todos os dados e ativos processuais produzidos em decorrência do uso da solução serão de inteira propriedade da UFMA.

Requisitos de Capacitação

4.7. Deve ser fornecido treinamento que ofereça os conhecimentos necessários e suficientes para a instalação, administração, configuração, otimização, resolução de problemas e utilização do equipamento, com carga horária mínima de 20 horas, para a equipe de 6 pessoas responsáveis pela operação do serviço, além da possibilidade de participação de ouvintes.

4.8. O treinamento deverá contemplar, no mínimo, os seguintes tópicos:

- Funcionalidades básicas do equipamento: senha de administração, hora e data, schedules e etc.;
- Procedimento de registro e ativação de licenças;
- Procedimento de atualização de software;
- Zonas de segurança e objetos;

- Interfaces físicas, interfaces virtuais (VLANs) e roteamento interno;
- NAT;
- Serviços de segurança como IPS e Anti-Malware;
- Regras de firewall;
- VPN;
- Regras de aplicação, incluindo visibilidade das mesmas;
- Geração de relatórios diversos da plataforma;
- Monitoramento da plataforma; e
- Demais funcionalidades existentes no firewall que não estão contempladas acima.

4.9. O Treinamento poderá ser realizado através de ferramentas de videoconferência ou presencialmente. Para melhor didática, a empresa fornecedora deverá disponibilizar um ambiente online (laboratório) para simular o uso dos equipamentos de firewall.

4.10. O ambiente tecnológico a ser utilizado durante a capacitação fica sob responsabilidade da contratada, podendo a UFMA auxiliar no que for possível.

4.11. A carga horária 20h poderá ser estendida conforme o necessário para que os capacitados recebam todo o treinamento necessário e suficiente para operar a solução.

4.12. Os materiais didáticos (apostila, slides, livros, etc.), sejam eles impressos ou digitais, deverão ser providos pela empresa fornecedora e disponibilizados para consulta posterior.

4.13. Para consulta posterior, deverá ser fornecido no mínimo 3 tipos de materiais (Ex: apostila + slide ou slide + livro ou apostila + slide + livro).

4.14. Exige-se que o instrutor tenha domínio técnico pleno da solução e possuir certificado fornecido por centro de treinamento oficial do Fabricante que o credencie a ministrar treinamentos na solução.

4.15. A contratada deverá emitir certificado ao final da capacitação indicando a carga horária, nome do participante, tópicos abordados no curso, bem como outras informações apropriadas.

Requisitos Legais

4.16. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD /ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis;

4.17. A contratada deverá observar e cumprir o Decreto Nº 9.637, de 26 de dezembro de 2018, da Presidência da República, que institui a Política Nacional de Segurança da Informação.

4.18. A contratada deverá observar e cumprir a Instrução Normativa GSI/PR Nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

4.19. A contratada deverá observar e cumprir a Política de Segurança da Informação da UFMA.

4.20. Esta contratação observa rigorosamente as vedações e diretrizes estabelecidas na Instrução Normativa SGD/ME nº 94/2022, garantindo que:

> **I - Não Ingerência:** É expressamente vedada qualquer ingerência da UFMA na gestão de pessoal da futura contratada, sendo proibido exercer poder de mando sobre seus empregados, direcionar a contratação de pessoas específicas ou interferir em questões remuneratórias e de benefícios (Art. 44, §3º);
>
> **II - Gestão por Resultados:** A fiscalização do contrato será baseada na entrega dos resultados e na conformidade técnica do Firewall, e não pelo controle de frequência ou subordinação dos funcionários da empresa detentora da solução;
>
> **III - Unicidade do Objeto:** Justifica-se o não parcelamento do objeto (hardware e licenças) em itens distintos, uma vez que a solução de segurança requer integridade e compatibilidade tecnológica absoluta entre os componentes para garantir a eficácia da proteção contra ameaças, sob pena de perda de garantia e suporte do fabricante (Art. 13, VI);
>
> **IV - Artefatos de Planejamento:** O processo encontra-se devidamente instruído com todos os artefatos exigidos (DOD, ETP, Mapa de Riscos e Termo de Referência), assegurando a rastreabilidade e a transparência de todas as etapas do planejamento.

4.21. No que tange ao atendimento das Portarias da Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI), certifica-se que:

I - Inexistência de Modelo Padronizado: Esta contratação não se enquadra em nenhum dos modelos de contratação obrigatórios ou catálogos de soluções padronizadas instituídos pelas portarias vigentes da SGD/MGI (tais como a Portaria nº 1.070 /2023, Portaria nº 750/2023 ou Portaria nº 5.950/2023);

II - Justificativa de Não Incidência: As referidas normas tratam de serviços de operação de infraestrutura (NOC/Service Desk), desenvolvimento de software e computação em nuvem, respectivamente. O objeto desta demanda é a aquisição de solução de hardware com licenciamento integrado (Appliance), categoria para a qual a SGD ainda não publicou modelo de Termo de Referência ou de execução obrigatória;

III - Autonomia de Especificação: Diante da ausência de padronização por parte do órgão central (SGD), a especificação técnica foi elaborada de forma autônoma pela equipe de planejamento da UFMA, visando atender às necessidades específicas de segurança de rede da Instituição, mantendo a aderência aos princípios gerais da IN SGD/ME nº 94/2022.

4.22. Em relação à consulta aos Catálogos de Soluções de TIC e ao Preço Máximo de Compra (PMC-TIC), estabelece-se que:

I - Ausência de Padronização: Após consulta realizada ao Portal de Compras do Governo Federal, certifica-se que o objeto desta contratação (Firewall/NGFW) não se encontra listado nos Catálogos de Soluções de TIC padronizadas pela Secretaria de Governo Digital (SGD/MGI);

II - Inaplicabilidade do PMC-TIC: Diante da inexistência de item padronizado para esta solução, não há incidência de Preço Máximo de Compra (PMC-TIC) específico, sendo o valor estimado da contratação balizado exclusivamente pela pesquisa de preços de mercado detalhada no Relatório nº 230/2025, em conformidade com a IN SEGES/ME nº 65/2021.

Requisitos de Manutenção

4.23. Todos os equipamentos que compõem a solução devem acompanhar extensão de garantia de suporte e manutenção de software e hardware, com substituição de peças e/ou equipamentos, por um período de 60 meses.

4.24. O modelo dos equipamentos não pode estar prestes a ser descontinuado para o serviço de suporte pelo fabricante, ou seja, não pode estar no final de seu “ciclo de vida”, durante a vigência do contrato.

4.25. A empresa fornecedora deverá fornecer os softwares e suas atualizações, firmwares, sistema operacional, durante toda a vigência da garantia, através de meio eletrônico ou magnético sem ônus adicionais.

4.26. A contratada deverá disponibilizar canal de comunicação (telefone, e-mail ou sistema de chamados), para abertura e gerenciamento de chamados técnicos 24x7.

4.27. Dada a necessidade de reposição de peça/equipamento, a CONTRATADA deverá preparar ou realizar a substituição, reconfiguração (importação de arquivos de backup), no datacenter da AGETIC/UFMA, em até 1 (um) dia útil.

4.28. Os chamados técnicos serão classificados de acordo com a severidade devendo atender aos respectivos prazos de solução definidos abaixo:

- SEVERIDADE BAIXA – prazo máximo de 48 horas para solução: correção de falha que não impede a continuidade da maior parte dos negócios e solicitações de informações sobre os produtos, incluindo configuração e instalação;
- SEVERIDADE MÉDIA – prazo máximo de 24 horas para solução: problemas que causem impactos significativos nos negócios, incluindo degradação de desempenho;
- SEVERIDADE ALTA – prazo máximo de 04 horas para solução: problemas que causem a interrupção parcial ou total dos serviços.

4.29. Quaisquer peças, componentes ou outros materiais que substituírem os defeituosos deverão ser originais do fabricante e de qualidade e características técnicas iguais ou superiores aos existentes no equipamento, sem ônus para a UFMA.

4.30. Em caso da impossibilidade em solucionar o problema nos prazos estipulados, a CONTRATADA compromete-se a substituir urgentemente o equipamento defeituoso, até o término do reparo do mesmo, por outro equivalente ou superior, de sua propriedade, a fim de proporcionar a operacionalização do equipamento e a continuidade da rotina de trabalho dos usuários.

4.31. Todas as despesas relacionadas com a eventual substituição dos equipamentos, no local de instalação AGETIC/UFMA), ocorrerão por conta da contratada e/ou do fabricante.

4.32. A CONTRATADA não poderá cobrar valores adicionais, tais como custos de deslocamento, alimentação, transporte, alojamento, trabalho aos sábados, domingos e feriados ou em horário noturno, bem como qualquer outro valor adicional.

4.33. A CONTRATADA e/ou fabricante deverá providenciar o deslocamento do equipamento, quando necessário, bem como seu retorno ao local de origem, sendo considerado, para todos os efeitos, durante este período, como fiel depositário do mesmo.

Requisitos Temporais

4.34. A resolução de problemas deverá ser atendida conforme estabelecido neste Termo de Referência.

4.35. As datas de realização do treinamento serão acordadas através de reunião do gestor do contrato com o preposto da CONTRATADA, após a assinatura do contrato e mediante a abertura de ordem de serviço pela contratante.

Requisitos de Segurança e Privacidade

4.36. A contratada deverá observar e cumprir a Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº13.709/2018).

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

4.38. A contratada deverá coibir o vazamento de dados e fraudes digitais.

4.39. Em conformidade com o disposto na NC 14/IN01/DSIC/GSIPR, os dados e informações do contratante devem residir exclusivamente em território nacional, incluindo replicação e cópias de segurança (backups), de modo que a Contratante disponha de todas as garantias da legislação brasileira enquanto tomador do serviço e responsável pela guarda das informações armazenadas em nuvem.

Requisitos Sociais, Ambientais e Culturais

4.40. Os serviços prestados pela Contratada deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e materiais consumidos bem como a geração excessiva de resíduos, a fim de atender às diretrizes de responsabilidade ambiental adotadas pela contratante.

Requisitos da Arquitetura Tecnológica

4.41. A alta disponibilidade informada acima deverá suportar os modos ativo-ativo e ativo-passivo, com sincronização, em tempo real, de configuração e de estados das sessões. No caso de falha de um dos equipamentos do cluster, não deverá haver perda das configurações e nem das sessões já estabelecidas e a transição entre os equipamentos deverá acontecer de forma transparente para o usuário.

4.42. A solução deverá incluir as funcionalidades mínimas de um Firewall de nova geração:

- Funcionalidades de um firewall tradicional;
- IPS integrado;
- Controle de aplicação; e
- Outras características elencadas no ANEXO I - Especificações Técnicas da solução de TIC.

Requisitos de Projeto e de Implementação

4.43. A contratada deverá realizar o planejamento das atividades a serem executadas, através da elaboração de um cronograma e um plano de projeto e implementação, em consonância com as disposições constantes neste Termo de Referência.

4.44. Reunião para detalhamento de todos os parâmetros de configuração da solução de segurança da informação.

4.45. Definição do plano de testes, em conjunto com o corpo responsável da UFMA, de cada etapa para migração dos serviços.

4.46. Definição de cronograma de implementação do projeto com o planejamento de migração para não afetar a operação da rede atual.

4.47. Deverá ser executado por profissionais devidamente capacitados, com certificação do fabricante.

Requisitos de Implantação

4.48. A contratada deverá realizar o planejamento das atividades a serem executadas, bem como cronograma detalhado, devendo ser entregue em um Plano de Projeto, elaborado em consonância com as disposições constantes neste Termo de Referência.

4.49. O Plano de Projeto deverá ser entregue antes da execução das atividades, validado e aprovado previamente pelo Gestor do Contrato.

4.50. A implantação da solução no ambiente da UFMA deve obedecer a gestão de mudança e liberação que são realizadas na AGETIC.

4.51. Os serviços serão executados conforme o acordado no Plano de Projeto, que deverão conter as atividades necessárias para entrega e perfeito funcionamento do objeto contratado.

4.52. Deverá ocorrer uma reunião de início de Projeto para alinhamento dos serviços a serem executados, agendada previamente entre as partes, através de e-mail ou telefone, em até 15 (quinze) dias após a assinatura do contrato.

4.53. Deverá ocorrer uma reunião para apresentação e validação do Plano de Projeto.

4.54. Em caráter excepcional e a critério da UFMA, as atividades poderão ser realizadas em dias e horários distintos do estabelecido, definidos em comum acordo com a contratada.

Requisitos de Garantia, Manutenção e Assistência Técnica

4.55. A contratada deverá disponibilizar canal de comunicação (telefone, e-mail ou sistema de chamados), para abertura e gerenciamento de chamados técnicos 24x7.

4.56. A contratada deverá possibilitar que as novas atualizações da solução sejam utilizadas pela UFMA durante o período de vigência do contrato.

Requisitos de Experiência Profissional

4.57. Apresentar uma lista com o nome de cada profissional que será utilizado na execução dos serviços, ficando a critério da UFMA a aprovação dos profissionais listados, bem como solicitar a substituição de qualquer profissional que julgar não possuir a capacitação necessária para execução dos serviços.

4.58. Os profissionais deverão possuir certificado fornecido por centro de treinamento oficial do Fabricante que o credencie na implantação da solução contratada.

Requisitos de Formação da Equipe

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

Requisitos de Metodologia de Trabalho

4.60. A UFMA encaminhará Ordem de Serviço/Fornecimento solicitando a implantação da solução adquirida.

4.61. A solução deverá ser implantada no prazo estabelecido neste Termo de Referência.

4.62. A CONTRATADA, com apoio da UFMA, no que couber, realizará a implantação e a configuração dos equipamentos.

4.63. Sendo atendido pela contratada o demandado na Ordem de Serviço/Fornecimento, a UFMA procederá com o recebimento provisório e em seguida após análise dos serviços e bens fornecidos será elaborado o termo de recebimento definitivo e o processo de pagamento.

4.64. A implantação da solução poderá ser realizada em fases e de acordo com a necessidade da UFMA.

4.65. O pagamento será efetuado conforme a implantação da solução contratada e entrega dos equipamentos.

Requisitos de Segurança da Informação e Privacidade

4.66. A contratada deverá observar a Lei Geral de Proteção de Dados Pessoais -LGPD (Lei nº 13.709/2018).

4.67. A contratada deverá observar a ABNT NBR ISO/IEC 27001:2013. Tecnologia da Informação - Técnicas de Segurança.

4.68. A contratada deverá observar a ABNT NBR ISO/IEC 27005:2011. Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

4.69. A contratada deverá observar a ABNT NBR ISO/IEC 27701:2019. Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27000.

4.70. A contratada deverá observar Guia de Boas Práticas da LGPD – CCGD (Comitê Central de Governança de Dados).

Sustentabilidade

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

4.72. Usar equipamentos homologados pela Anatel e/ou ABNT, no que diz respeito a normas ambientais.

4.73. Fornecer aos empregados os equipamentos de segurança que se fizerem necessários, para a execução dos serviços de instalação da Solução.

4.74. Respeitar as Normas Brasileiras - NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos, incluindo práticas de logística reversa, conforme o caso.

4.75. Dar preferência ao uso de bens constituídos por material reciclado, atóxico, biodegradável, conforme ABNT NBR - 15448-1 e 15448-2.

4.76. Acondicionar os bens preferencialmente em embalagem individual adequada, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento.

4.77. Que os bens não contenham substâncias perigosas em concentração acima das recomendadas pelas normas técnicas.

4.78. Todos os documentos ou artefatos gerados pela contratada, salvo manifestação explícita deverão ser entregues em formato digital.

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

- Instrução Normativa SLTI/MPOG nº 1, de 19 de janeiro de 2010, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências.
- Decreto nº 9.373, de 11 de maio de 2018, dispõe sobre a alienação, a cessão, a transferência, a destinação e a disposição final ambientalmente adequada de bens móveis no âmbito da administração pública federal direta, autárquica e fundacional.
- Resolução Conama n° 401, de 4 de novembro de 2008, que estabelece os limites máximos de chumbo, cádmio e mercúrio para pilhas e baterias comercializadas no território nacional e os critérios padrões para o seu gerenciamento ambientalmente adequado, e dá outras providências.
- Art. 33, inciso VI, da Lei Federal nº 12.305/2010, que dispõe sobre a Política Nacional de Resíduos Sólidos, de abrangência nacional, determina que os fabricantes, importadores, distribuidores e comerciantes de produtos eletroeletrônicos e seus componentes são obrigados a estruturar e implementar sistemas de logística reversa, mediante retorno dos produtos e embalagens após o uso pelo consumidor, de forma independente do serviço público de limpeza urbana e de manejo dos resíduos sólidos.
- Guia Nacional de Licitações Sustentáveis– DECOR/CGU/AGU, quando da aquisição de bens, serão exigidos os seguintes critérios de sustentabilidade:

    a) Que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação.

Plano Diretor de Logística Sustentável (PDLS)

4.80. Em relação ao alinhamento com o Plano Diretor de Logística Sustentável, informo que o PDLS da UFMA está em fase de atualização para atendimento das diretrizes da Portaria SEGES/ME nº 8.678, de 19 de julho de 2021, com prazo para conclusão em dezembro de 2024. Por conta disso, foram observadas as diretrizes do Guia Nacional de Contratações Sustentáveis (6ª edição, setembro /2023).

4.81. No que concerne à Sustentabilidade e ao Plano de Logística Sustentável (PLS), a contratação observa os seguintes critérios de práticas ambientais, fundamentados no Guia Nacional de Contratações Sustentáveis:

I - Eficiência Energética: Os equipamentos deverão possuir certificações que atestem o baixo consumo de energia e a eficiência operacional (tais como Energy Star, EPEAT ou equivalentes), visando a redução do impacto ambiental e dos custos operacionais da Universidade;

II - Logística Reversa: A futura contratada deverá responsabilizar-se pelo recolhimento e descarte adequado das baterias e componentes eletrônicos substituídos ou ao final da vida útil do equipamento, conforme as diretrizes da Lei nº 12.305/2010 (Política Nacional de Resíduos Sólidos);

III - Restrição de Substâncias Perigosas: A solução fornecida deverá, preferencialmente, atender à diretriz RoHS (*Restriction of Hazardous Substances*), que limita o uso de substâncias perigosas na fabricação de equipamentos eletrônicos, preservando a saúde dos usuários e facilitando a reciclagem futura;

IV - Competitividade: Tais exigências de sustentabilidade são aplicadas de forma isonômica, não representando barreira indevida à competitividade, visto tratarem-se de padrões mundiais da indústria de hardware de rede e segurança.

Subcontratação

4.82. Não é admitida a subcontratação do objeto contratual.

Garantia da Contratação

4.83. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual de 5% do valor contratual e condições descritas nas cláusulas do contrato.

4.84. Em caso opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.

4.85. A garantia, nas modalidades caução e fiança bancária, deverá ser prestada em até 15 dias após a assinatura do contrato.

4.86. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

5. Papéis e responsabilidades

5.1. São obrigações da CONTRATANTE:

5.1.1. Nomear servidores que integrarão a Equipe de Gestão do Contrato nos termos do art.29 da Instrução Normativa SGD/ME Nº 94 /2022, composta por Gestor do Contrato, Fiscal Técnico, Fiscal Requisitante e Fiscal Administrativo para acompanhar e fiscalizar a execução dos contratos.

5.1.2. Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência, observando-se o disposto no art. 18 a 32 da Instrução Normativa ME Nº 94/2022.

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

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

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

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

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

5.1.8. Comunicar à CONTRATADA toda e quaisquer ocorrências relacionadas com o produto.

5.1.9. Fiscalizar a entrega dos serviços/bens, podendo sustar, recusar, solicitar fazer ou desfazer qualquer entrega ou serviços, no todo ou em parte, que não esteja de acordo com as condições e exigências estabelecidas em cada ordem de serviço ou no Termo de Referência.

5.1.10. Analisar os relatórios de desempenho e os resultados entregues verificando se as exigências, procedimentos e processos definidos e aprovados nas ordens de serviço foram atendidos, assim como se os índices foram alcançados, propondo as glosas e multas cabíveis para cada caso.

5.1.11. Emitir relatórios sobre os atos relativos à execução do Contrato que vier a ser firmado, em especial, quanto ao acompanhamento e fiscalização da execução dos serviços, à exigência de condições estabelecidas e proposta de aplicação de sanções.

5.1.12. Notificar à CONTRATADA eventual irregularidade no cumprimento das obrigações contratuais.

5.1.13. Impor sanções contratuais caso suas demandas de correção de irregularidades, notificadas à CONTRATADA, não sejam corrigidas dentro do prazo estabelecido.

5.1.14. Exigir o cumprimento de todos os compromissos assumidos pela CONTRATADA, de acordo com as especificações do objeto, constantes deste Termo de Referência.

5.1.15. Fiscalizar a execução do objeto, tanto sob o aspecto quantitativo como qualitativo.

5.1.16. Analisar e verificar se os Acordos de Níveis de Serviços contratados foram alcançados e propor as glosas estipuladas para cada caso.

5.2. São obrigações do CONTRATADO:

5.2.1. Indicar formalmente e por escrito, no prazo máximo de 5 (cinco) dias úteis após a assinatura do contrato, junto à contratante, um preposto idôneo com poderes de decisão para representar a contratada, principalmente no tocante à eficiência e agilidade da execução do objeto deste Termo de Referência, e que deverá responder pela fiel execução do contrato.

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

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

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

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

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

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

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

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

5.2.10. Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do contrato, sem prévia autorização da contratante.

5.2.11. Não fazer uso das informações prestadas pela contratante para fins diversos do estrito e absoluto cumprimento do contrato em questão.

5.2.12. Cumprir, às suas próprias expensas, todas as cláusulas contratuais que definam suas obrigações.

5.2.13. Assumir a responsabilidade por todos os encargos previdenciários e obrigações sociais previstas na legislação social e trabalhista em vigor, obrigando-se a saldá-las na época própria, vez que os seus empregados não manterão nenhum vínculo empregatício com a CONTRATANTE.

5.2.14. Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados durante a execução deste contrato, ainda que acontecido em dependência da CONTRATANTE.

5.2.15. É de responsabilidade da contratada fornecer a seus técnicos todas as ferramentas, softwares e instrumentos necessários e suficientes para a execução dos serviços, bem como prover e se responsabilizar pela locomoção dos mesmos até a CONTRATANTE.

5.2.16. A empresa a ser contratada deverá garantir que os produtos licenciados para uso não infringem quaisquer patentes, direitos autorais ou trade-secrets, devendo a empresa a ser contratada se responsabilizar por quaisquer despesas relacionadas que ocorram.

5.2.17. O contrato possuirá um gestor e uma equipe de fiscalização (fiscal requisitante, fiscal técnico e fiscal administrativo) formalmente designados, os quais atuarão de acordo com as competências estabelecidas neste Termo de Referência e nos normativos vigentes, de forma não taxativa.

6. Modelo de execução do contrato

Rotinas de Execução
Do Encaminhamento Formal de Demandas

6.1. Após a assinatura do Contrato, o Gestor do contrato deverá convocar a reunião inicial com todos os envolvidos na contratação. A reunião inicial poderá ser realizada de forma presencial ou remota. Na reunião inicial será disponibilizado:

6.1.1. A Carta de apresentação do Preposto, que 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;

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

6.1.3. O representante legal da contratada deverá entregar o Termo de Compromisso (ANEXO II) e o Termo de Ciência (ANEXO III), contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes da instituição;

6.1.4. O representante legal da contratada deverá apresentar o cronograma de execução do projeto;

6.1.5. Serão feitos esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato.

6.2. Prazos, horários de fornecimento de bens ou prestação dos serviços:

6.2.1. O prazo de entrega dos bens é de **45 (quarenta e cinco) dias corridos**, contados a partir do envio da nota de empenho, em **remessa única**;

6.2.2. A instalação da solução demandada deverá estar implantada em até **60 (sessenta) dias**, após o a data de recebimento dos equipamentos;

6.2.3. Os bens deverão ser entregues no Almoxarifado Central situado na sede da CONTRATANTE, no endereço: **Av. dos Portugueses, 1966, Vila Bacanga - Cidade Universitária Dom Delgado, São Luís – MA CEP 65.080-805**, **conforme referência geográfica: https://maps.app.goo.gl/95yU7NbYa8i4ALMW6;**

6.2.4. Os equipamentos deverão ser instalados no seguinte endereço: **Superintendência de Tecnologia da Informação - AGETIC da UFMA, conforme referência geográfica: https://maps.app.goo.gl/g84K9cF13tzdP7v29;**

6.2.5. Os bens deverão ser entregues de segunda-feira a sexta-feira no horário das 08:30h às 12:00h e das 13:00h às 16:30h;

6.2.6. A entrega deverá ser agendada com antecedência mínima de 24 horas.

6.3. Referente à documentação mínima exigida, a Contratada deverá fornecer:

6.3.1. Manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração;

6.3.2. Documentação completa da solução, incluindo especificação do equipamento, características e funcionalidades implementadas, desenho lógico da implantação, comentários e configurações executadas; e

6.3.3. Relatório com o detalhamento do processo realizado ao final da implantação como requisito para o aceite definitivo.

6.4. Formas de transferência de conhecimento:

6.4.1 A fim de promover a transferência de conhecimento, a implantação da solução deverá ocorrer com participação, sempre que possível, dos técnicos da UFMA que atuarão na solução. Durante a implantação da solução a equipe da CONTRATADA deverá repassar as informações para a equipe da UFMA, apresentando as configurações realizadas nos equipamentos, a topologia final e procedimentos executados.

Garantia, manutenção e assistência técnica

6.5. 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).

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

6.7. A garantia abrange a realização da manutenção corretiva dos bens pelo próprio Contratado, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

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

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

6.10. Uma vez notificado, o Contratado realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até 1 (Um) dia útil, contados a partir da data de notificação.

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

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

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

6.14. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade do Contratado.

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

6.16. O atendimento inicial deve ser realizado no prazo máximo de 01 (uma) hora para chamados críticos e demais chamados no prazo máximo de 08 (oito) horas, observando as prioridades de atendimento, durante o período de vigência da garantia.

6.17. Entende-se por chamados críticos aqueles derivados de problemas graves, quando o ambiente está parado ou quando o seu desempenho impede a execução das atividades de negócio.

7. Modelo de gestão do contrato

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

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

7.3. As comunicações entre o órgão ou entidade e a contratada 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.

7.5. Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

Fiscalização

7.6. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput), nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

Fiscalização Técnica

7.7. 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. (Decreto nº 11.246, de 2022, art. 22, VI);

7.7.1. 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. (Lei nº 14.133, de 2021, art. 117, §1º, e Decreto nº 11.246, de 2022, art. 22, II);

7.7.2. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

7.7.3. 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. (Decreto nº 11.246, de 2022, art. 22, IV);

7.7.4. 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. (Decreto nº 11.246, de 2022, art. 22, V);

7.7.5. 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 (Decreto nº 11.246, de 2022, art. 22, VII).

Fiscalização Administrativa

7.8. 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 do Contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

7.8.1. 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; (Decreto nº 11.246, de 2022, art. 23, IV).

Gestor do Contrato

7.9. O gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, coordenará 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. (Decreto nº 11.246, de 2022, art. 21, IV).

7.10. O gestor do contrato acompanhará a manutenção das condições de habilitação do Contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

7.11. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

7.12. O gestor do contrato emitirá 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. (Decreto nº 11.246, de 2022, art. 21, VIII).

7.13. O gestor do contrato tomará 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. (Decreto nº 11.246, de 2022, art. 21, X).

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 tempestiva renovação ou prorrogação contratual. (Decreto nº 11.246, de 2022, art. 22, VII).

6.15. O gestor do contrato deverá 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. (Decreto nº 11.246, de 2022, art. 21, VI).

8. Do reajuste

8.1. Será adotado como índice de reajuste do Contrato o Índice de Custos de Tecnologia da Informação – ICTI.

9. Critérios de seleção do fornecedor

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.

9.2. A contratação da Solução de Segurança de TIC (Next Generation Firewall - NGFW) se enquadra na regra geral do art. 47, inciso II, da Lei nº 14.133/21, que determina o **parcelamento** do objeto quando técnica e economicamente vantajoso, visando a ampliação da competitividade e o melhor aproveitamento dos recursos.

Contrariando a regra do parcelamento, a adjudicação será realizada por LOTE ÚNICO, conforme estabelecido no Estudo Técnico Preliminar (ETP), devido à inviabilidade técnica e à desvantagem econômica da separação dos componentes, conforme as justificativas fundamentadas a seguir:

1. Inviabilidade Técnica da Separação (Sistema Integrado): a Solução de Segurança Distribuída e Centralizada não é uma simples soma de equipamentos, mas um **sistema tecnológico intrinsecamente integrado**. O objeto abrange:

    - **Firewalls** de diferentes capacidades para o *datacenter* central e os 10 Campi Regionais.
    - **Gerenciadores Centralizados** de Logs e Políticas.
    - **Licenças de Software** de segurança avançada (como prevenção a ameaças e *sandboxing*).
    - **Serviços** de garantia e suporte.

    O parcelamento desses itens em lotes independentes inviabilizaria a operação, pois exigiria que todos os equipamentos (firewalls) fossem **obrigatoriamente compatíveis** e operáveis sob o **mesmo sistema de gerenciamento centralizado**. Contratar fornecedores diferentes para cada componente criaria o risco de:

    - **Incompatibilidade de Plataformas:** Plataformas de firewall de fornecedores distintos frequentemente não se comunicam ou não podem ser gerenciadas por um único *console* central, comprometendo a **gestão unificada e a uniformidade da política de segurança**.
    - **Perda de Funcionalidades Integradas:** As funcionalidades de segurança de próxima geração (NGFW), como a inteligência de ameaças e o gerenciamento centralizado de logs, dependem da integração nativa entre hardware, software e gerência de um **único fabricante**.
    - **Comprometimento da Alta Disponibilidade (HA):** A exigência de **Alta Disponibilidade (HA) no datacenter central** requer a sincronização perfeita entre os equipamentos, o que é garantido apenas por soluções homologadas do mesmo fornecedor.

    2. Desvantagem Econômica e Operacional do Parcelamento: a divisão do objeto resultaria na perda da economia de escala e geraria um aumento significativo nos custos operacionais e de gestão de riscos:

    - **Risco de Descontinuidade:** Com múltiplos fornecedores, a responsabilidade por falhas de integração ou *bugs* se torna difusa, resultando em longos prazos para a correção de incidentes e comprometendo o requisito de **continuidade dos serviços de segurança**.
    - **Custos de Manutenção Elevados:** Seria necessário manter equipes técnicas com *expertise* em múltiplas plataformas, além de contratos de garantia e suporte com diversos fornecedores, elevando os custos de *Total Cost of Ownership* (TCO).
    - **Complexidade Administrativa:** A gestão de múltiplos contratos de aquisição e serviços diferentes para um único sistema de segurança aumenta exponencialmente a carga administrativa e a burocracia.

Portanto, o não parcelamento e a adjudicação em **Lote Único** se justificam como a opção **tecnicamente mais eficaz e operacionalmente mais eficiente**, sendo a única forma de garantir a integridade, a eficácia e a segurança da informação em toda a UFMA, conforme o art. 47, §1º, da Lei nº 14.133/2021.

Exigências de habilitação

9.3. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

Habilitação jurídica

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

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

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

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

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

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

9.10. F**ilial, 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.

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

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

Habilitação fiscal, social e trabalhista

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

9.14. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

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

9.16. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

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

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

9.19. Caso o fornecedor seja considerado isento dos tributos Estadual ou Municipal 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.

9.20. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

9.21. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;

9.22. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

9.23. Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), comprovados mediante a apresentação pelo licitante de balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais e obtidos pela aplicação das seguintes fórmulas:

I - Liquidez Geral (LG) = (Ativo Circulante + Realizável a Longo Prazo)/(Passivo Circulante + Passivo Não Circulante);
II - Solvência Geral (SG)= (Ativo Total)/(Passivo Circulante +Passivo não Circulante); e
III - Liquidez Corrente (LC) = (Ativo Circulante)/(Passivo Circulante).

9.24. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação capital mínimo OU patrimônio líquido mínimo de 5% do valor total estimado da contratação OU valor total estimado da parcela pertinente.

9.25. 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. (Lei nº 14.133, de 2021, art. 65, §1º).

9.26. O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos. (Lei nº 14.133, de 2021, art. 69, §6º).

Qualificação Técnica

9.27. Efetuada a verificação referente ao cumprimento das condições de participação no certame, a habilitação das licitantes será realizada mediante a apresentação da seguinte documentação complementar:

9.27.1. Atestado de Capacidade Técnica demonstrando que a proponente forneceu equipamentos, para pessoa física ou jurídica de direito público ou privado, e realizou a instalação, configuração e suporte técnico de solução de firewall de próxima geração compatível com o objeto deste termo de referência;

9.27.2. Atestado de Capacidade Técnica demonstrando que a proponente realizou, para pessoa física ou jurídica de direito público ou privado, treinamento da solução de firewall de próxima geração compatível com o objeto deste termo de referência;

9.27.3. Os atestados acima referidos deverão conter identificação do emitente, características e localização da prestação do serviço, local, data da expedição e declaração do emitente do atestado de que o serviço foi realizado a contento.

9.27.4. O atestado deverá ser em nome da LICITANTE, e elaborados em papel timbrado da empresa emitente, contendo os seguintes dados mínimos e obrigatórios:

9.27.4.1. Razão Social, CNPJ e endereço completo da empresa emitente;
9.27.4.2. Razão Social da LICITANTE;
9.27.4.3. Objeto do contrato;
9.27.4.4. Descrição do objeto do contrato: (descrição detalhada dos serviços prestados);
9.27.4.5. Local e Data de emissão do Atestado;
9.27.4.6. Nome, assinatura do signatário, telefone e e-mail de contato da empresa emitente.

9.28. A empresa licitante deverá apresentar atestado(s) que comprove(m), no mínimo, atendimento a 50% dos quantitativos previstos para os itens do objeto;

9.29. Serão aceitos somatórios de atestados de capacidade técnica para comprovação, podendo os mesmos serem de fabricantes distintos.

10. Estimativas do valor da contratação

Valor (R$): 1.785.571,50

10.1. O custo estimado total da contratação é de **R$ 1.785.571,50 (Um milhão, setecentos e oitenta e cinco mil, quinhentos e setenta e um reais e cinquenta centavos)**, conforme custos unitários apostos na tabela do item 1.1.

11. 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 informação orçamentária será apresentada no curso do processo pelo setor competente.

12. Critérios de medição e de pagamento

Recebimento

12.1. Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

12.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 01 (um) dia, a contar da notificação do Contratado, às suas custas, sem prejuízo da aplicação das penalidades.

12.3. O recebimento definitivo ocorrerá no prazo de 05 (cinco) dias, após a data de implantação da solução, sendo o ateste emitido por servidores designados pelo CONTRATANTE, que elaborarão relatório para fins de liberação do pagamento das Notas Fiscais/Faturas.

12.4. Durante a vigência deste contrato, a execução do objeto será acompanhada e fiscalizada pela Equipe de Gestão e Fiscalização Contratual, devidamente designada para esse fim, permitida a assistência de terceiros.

12.5. 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.

12.6. 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.

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

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

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

Liquidação

12.10. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.

> 12.10.1. 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.

12.11. 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:

> 12.11.1. o prazo de validade;
> 12.11.2. a data da emissão;
> 12.11.3. os dados do contrato e do órgão Contratante;
> 12.11.4. o período respectivo de execução do contrato;
> 12.11.5. o valor a pagar; e
> 12.11.6. eventual destaque do valor de retenções tributárias cabíveis.

12.12. 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;

12.13. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado 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.

12.14. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018).

12.15. Constatando-se, junto ao SICAF, a situação de irregularidade do Contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do Contratante.

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

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

12.18. 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

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

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

Forma de pagamento

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

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

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

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

12.24. O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

Cessão de crédito

12.25. É admitida a cessão fiduciária de direitos creditícios com instituição financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020, conforme as regras deste presente tópico.

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

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

12.28. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (Contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração. (INSTRUÇÃO NORMATIVA Nº 53, DE 8 DE JULHO DE 2020 e Anexos).

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

13. 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 05/02/2026 às 12:25:18.

LUCIANO MONTEIRO DOS SANTOS

Integrante Técnico

Assinou eletronicamente em 10/02/2026 às 10:51:01.

WAGNER DUARTE DE JESUS

Integrante Técnico

Assinou eletronicamente em 12/02/2026 às 11:22:47.

CLAUDIO SANTANA PEREIRA E SILVA

Integrante Administrativo

Assinou eletronicamente em 05/02/2026 às 10:16:19.

ANILTON BEZERRA MAIA

Autoridade Máxima da Área de TIC

Assinou eletronicamente em 05/02/2026 às 10:11:14.

MARCOS MOURA SILVA

Autoridade Administrativa

Assinou eletronicamente em 24/02/2026 às 15:16:44.

UNIVERSIDADE FEDERAL DO MARANHÃO

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 descriptografia 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/politicas baseadas em usuários e grupos de usuários;

9.5. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas 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 DCHP 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 throubleshooting;

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 QoE 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.

UNIVERSIDADE FEDERAL DO MARANHÃO

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 n° 06.279.103/0001-19, doravante denominado **CONTRATANTE**, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n° <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

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

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.

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**	xxxxxxxxxxxx
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)>	<xxxxxxxxxx>	

UNIVERSIDADE FEDERAL DO MARANHÃO

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

<Local>, <dia> de <mês> de <ano>.