TERMO DE REFERÊNCIA

1	**OBJETO:**
1.1	Registro de Preços para eventual aquisição de "Solução de Segurança de Rede" composta por Equipamentos com garantia técnica *on-site* pelo período mínimo de 60 (sessenta) meses, instalação e Serviço de Treinamento..
2	**JUSTIFICATIVAS DA AQUISIÇÃO:**
2.1	Além da sede da PGJ-MA e das Promotorias de Justiça da Capital, o Ministério Público do Estado do Maranhão - MPMA possui vários órgãos setoriais e Promotorias de Justiça na Capital e no Interior do Estado, as quais necessitam de conexão segura à internet e aos sistemas internos do MPMA, tais como DIGIDOC, SIMP, GESP, Ponto Eletrônico, Servidores de Arquivos, Servidores de Videoconferência, Servidores de Backup, Servidores de Videomonitoramento, e vários outros sistemas críticos para o funcionamento apropriado das atividades jurisdicionais.
2.3	A cada dia, vemos uma onda crescente de notícias sobre crimes cibernéticos e novos tipos de ataques e invasões no ambiente virtual.
2.4	Os ataques ao ambiente tecnológico estão cada vez mais sofisticados, o que pode acabar por impactar na disponibilidade dos serviços prestados à sociedade. Esses ataques ocorrem constantemente e, principalmente, em momentos críticos para o Ministério Público, para o Brasil e para a população em geral, quando da publicação externa de sistemas importantes para a sociedade.
2.4	O número de tentativas de invasões somente no período de pandemia no Brasil, em 2020, cresceu cerca de 860%, reafirmando essa onda de notícias.
2.5	Nos últimos meses houve um crescimento substancial de ataques cibernéticos tendo como alvo órgãos públicos brasileiros, a saber: **Superior Tribunal de Justiça**: STJ é alvo de ataque de hacker e Polícia Federal investiga o sistema (https://agenciabrasil.ebc.com.br/justica/noticia/2020-11/stj-e-alvo-de-ataque-de-hacker-e-policia-federal-investiga-o-sistema) **Tribunal Superior Eleitoral**: Ataque hacker ao TSE também acessou dados de 2020 do tribunal) (https://noticias.uol.com.br/eleicoes/2020/11/19/ataque-hacker-ao-tse-tambem-acessou-dados-de-2020-do-tribunal.htm?cmpid=copiaecola) **Tribunal de Justiça do Rio Grande do Sul**: Sistemas do TJ-RS continuam fora do ar após ataque hacker (https://www.conjur.com.br/2021-mai-04/sistemas-tj-rs-continuam-fora-ar-ataque-hacker) **Supremo Tribunal Federal:** STF trabalha para liberar acesso externo ao site ainda na manhã desta sexta (7/5)

TERMO DE REFERÊNCIA

	https://www.conjur.com.br/2021-mai-07/stf-trabalha-liberar-acesso-externo-site-ainda-nesta-sexta
2.6	A necessidade de priorizar investimentos na área de segurança da informação, principalmente no tocante à proteção dos dados institucionais, cujo valor é imensurável, bem como o impacto do comprometimento ou perda da massa de dados dos sistemas institucionais, isto é, não manter os dados seguros pode trazer perda de produtividade e prejuízos inimagináveis, podendo até causar a paralisação de todas as atividades do MPMA.
2.7	Uma invasão e/ou o comprometimento dos recursos e dados de TI podem ocorrer por meio de um acesso externo (a partir da Internet), mas também por meio de uma disseminação interna (a partir da rede de computadores do MPMA).
2.8	O MPMA não possui, atualmente, equipamentos próprios de segurança de rede (firewalls). Os 2 (dois) únicos equipamentos atuais em uso são itens de um contrato de circuitos de dados com vigência até setembro de 2021.
2.9	A aquisição uma solução de firewall proverá uma barreira de segurança para proteger a infraestrutura de comunicação de dados do MPMA e seus ativos contra acessos indevidos. Utilizando controle de tráfego de dados e regras de filtragem dos mesmos. Desta forma, é possível permitir somente a transmissão e a recepção de dados autorizados, evitando tentativas de acessos indevidos às informações.
2.10	Melhorar, por conseguinte, os serviços prestados à sociedade, visto que a melhoria da infraestrutura de comunicação de dados proporcionará uma significativa melhoria na entrega dos serviços e informações demandados pela sociedade, alavancando o alcance das políticas sociais, tornando a Instituição cada vez mais resolutiva e mais próxima do cidadão maranhense.
2.11	Com a finalidade de renovar o parque de equipamentos e infraestrutura de telecomunicações, a CMTI/PGJ-MA incluiu no PDTI 2017-2021 ações que visam a modernização de todo o ambiente de telecomunicações, destacando-se: "Renovar Parque de Soluções de Conectividade e Comunicação" e "Padronizar Infraestrutura de Rede Elétrica e Lógica".
2.12	Dentre as diversas ações promovidas pela PGJ-MA, relacionadas com a infraestrutura tecnológica, inclui-se a modernização da rede. A esse macrodesafio foram estabelecidos os seguintes indicadores: a) Índice de Atualização do Parque (IAP), cuja meta é "Atingir 100% de Atualização até 31/12/2021"; b) Índice de Padronização das Redes Elétrica e Lógica (IPREL), cuja meta é "Padronizar 100% das redes até dez 2020".
2.13	Portanto, a pretendida contratação, além de contribuir para o atingimento dos indicadores ora mencionados, contribuirá para o cumprimento das aquisições previstas no Plano Diretor de Tecnologia da Informação – PDTI – 2017-2021.
2.14	A título de informação, registra-se que o PDTI tem dentre as diversas finalidades, diagnosticar os equipamentos e as instalações necessárias que deverão ser adquiridas pela PGJ-MA, em determinado período de tempo.
2.15	Importante lembrar, também, que a aquisição de equipamentos de rede, está alinhada ao negócio da PGJ-MA, bem como às iniciativas "Adequar as instalações e equipamentos à demanda das unidades" e "implantar o processo judicial eletrônico - PJe", vinculadas ao macrodesafio acima citado.
2.16	Pela imprevisibilidade da ocorrência desta demanda, em quantidades exatamente definidas, não se sabe ao certo qual será a efetiva necessidade da Administração, em qual período ela se dará, quais unidades e

TERMO DE REFERÊNCIA

	Promotorias de Justiça a Administração pretende atender, e também com o fito de se evitar fracionamento indevido de despesas, optou-se por adotar o sistema de registro de preços, no qual é feita apenas uma estimativa de possíveis aquisições que possam ser realizadas, não obrigando esta Instituição a fazê-lo, conforme disposto no(s) item(ns) do Art 3º III, do Ato Regulamentar Nº 11/2014-GPGJ e do artigo 3º do Decreto nº 7.892, de 23 de janeiro de 2013, este in verbis: *"Art. 3º O Sistema de Registro de Preços poderá ser adotado nas seguintes hipóteses:* *I - quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes;* *II - quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;* *III - (...)* *IV - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração."*
2.17	Por se tratar de um registro de preços, o quantitativo definido não significa, necessariamente, que serão adquiridos na sua totalidade. Porém, é importante que se tenha esse quantitativo para atendimento da demanda atual e reserva técnica. Tal quantitativo também será passível de adesões por parte de outros órgãos, além do fato do registro de preços não requerer obrigatoriedade de dotação orçamentária, nem de aquisição integral do quantitativo definido, podendo ser adquirido de acordo com a necessidade, aliada à disponibilidade de orçamento.
2.18	**Justificativa quanto ao enquadramento dos serviços na categoria de Serviços Comuns:**
2.18.1	A Lei nº 10.520/2002 institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, a modalidade de licitação denominada "Pregão" para aquisição de bens e serviços comuns, e considera tais bens e serviços como sendo aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo Edital, por meio de especificações usuais no mercado. Assim sendo, uma vez que o objeto da contratação do presente TERMO DE REFERÊNCIA pode ser objetivamente definido e mensurado por meio de especificações usuais no mercado, pode-se concluir que se trata de serviços comuns.
2.18.2	O Tribunal de Contas da União – TCU, por meio do Acórdão n° 2.471/2008-Plenário, em seu item 9.2, recomenda que a Administração Pública Direta, Autárquica e Fundacional utilize a modalidade de licitação do tipo "Pregão", para contratar bens e serviços de informática considerados comuns. Entende o TCU, conforme item 9.2.2 do referido Acórdão, que devido à padronização existente no mercado, os bens e serviços de Tecnologia da Informação geralmente atendem a protocolos, métodos e técnicas pré-estabelecidos e conhecidos e a padrões de desempenho e qualidade que podem ser objetivamente definidos por meio de especificações usuais no mercado.
2.18.3	Dessa forma, os serviços descritos nesta contratação podem ser definidos por padrões usuais de mercado, atendendo a padrões, protocolos, normas, métodos e técnicas pré-estabelecidos e conhecidos e a padrões de desempenho e qualidade, estando caracterizados como serviços comuns. Sendo assim, recomenda-se modalidade de licitação do tipo "Pregão", com julgamento pelo critério "Menor Preço" para provimento de todos os itens da solução (Decreto n° 5.450/2005, Art. 4°).
2.19	**Justificativa para o não parcelamento em itens:**
2.19.1	Embora o corolário da segregação da contratação em itens seja a obrigatoriedade de aplicação da regra do

	parcelamento, contida no art. 23, § 1º, da Lei 8666/1993, a Comissão de Planejamento da Contratação, constatou que, no aspecto técnico, há uma interdependência entre os itens requisitados, que necessitam de total integração e compatibilidade entre si, de modo que não podem ser adquiridos de forma segregada, onde a melhor opção é que todos os equipamentos, licenças, materiais e acessórios sejam do mesmo FABRICANTE, e isto inviabiliza qualquer tentativa de parcelamento, sob pena de prejudicar a eficácia da Contratação.
2.19.2	A centralização da responsabilização em uma única empresa CONTRATADA, por tratar-se de uma solução de alta disponibilidade e desempenho, além da abrangência de distribuição dos equipamentos, se mostra mais adequada, não apenas sob o prisma dos requisitos de interoperabilidade e do acompanhamento de problemas e soluções, mas sobremaneira para facilitar a verificação das causas e atribuição de responsabilidade, de modo a aumentar o controle sobre a execução do objeto licitado e para minimizar reposições em caso de defeitos durante a garantia técnica, por exemplo.
2.19.3	Em sendo assim, considerando as implicações que envolvem a pretendida aquisição, bem como as razões técnicas e de logística apresentadas, a Contratação de uma única empresa para o fornecimento e do equipamento e realização do treinamento se mostra o mais adequado.
3	**DO PRAZO, LOCAL E CONDIÇÕES DE ENTREGA DO OBJETO:**
3.1	O prazo para entrega do objeto do contrato será de, no máximo, 45 (quarenta e cinco) dias consecutivos, contados a partir do recebimento da nota de empenho pela CONTRATADA.
3.2	Os equipamentos, licenças, materiais e acessórios deverão ser entregues no *Data Center* do Prédio-sede da Procuradoria-Geral de Justiça do Maranhão – PGJ-MA, Pavimento Térreo, na Avenida Professor Carlos Cunha, nº 3261, Jaracati, CEP: 65076-820 – São Luís – Maranhão, no horário das 08:00h às 15:00h, em dias úteis, de segunda-feira a sexta-feira e deverá ser agendada com antecedência mínima de 24 (vinte e quatro) horas, sob o risco de não ser autorizada.
3.3	O fornecimento do objeto será feito de acordo com a necessidade da CONTRATANTE, pelo prazo de validade da Ata de Registro de Preços gerada.
3.4	O serviço de Instalação deverá ser iniciado no prazo máximo de 30 (trinta) dias consecutivos, a contar da data de recebimento da formalização, por parte da CONTRATADA, comunicando a finalização da entrega de todos os equipamentos, licenças, materiais e acessórios no local determinado, a ser encaminhada pela CONTRATANTE por meio eletrônico (e-mail institucional).
3.5	O serviço de Treinamento deverá ser iniciado no prazo máximo de 30 (trinta) dias corridos, a contar da data de recebimento da Ordem de Serviço específica, a ser encaminhada pela CONTRATANTE por meio eletrônico (e-mail institucional).
3.6	Eventual pedido de prorrogação de prazo de entrega deverá ser encaminhado para o endereço de e-mail cmti@mpma.mp.br.
3.7	Serão injustificados os atrasos não comunicados tempestivamente ou indevidamente fundamentados, e a aceitação da justificativa ficará a critério do CONTRATANTE.
3.8	Deverão estar incluídos nos preços unitários todos os impostos, taxas, fretes e encargos sociais, obrigações trabalhistas, previdenciárias, fiscais e comerciais, assim como despesas com transportes, os quais serão de responsabilidade da CONTRATADA.
4	**DAS CONDIÇÕES E PRAZOS DE RECEBIMENTO DO OBJETO:**
4.1	**Recebimento dos equipamentos, licenças, materiais e acessórios:**

TERMO DE REFERÊNCIA

4.1.1	Os equipamentos, licenças, materiais e acessórios serão RECEBIDOS PROVISORIAMENTE mediante Termo Circunstanciado de Recebimento Provisório assinado pelas partes em até 15 (quinze) dias úteis, a contar do primeiro dia útil após o recebimento da formalização, por parte da CONTRATADA, comunicando a finalização da entrega de todos os equipamentos, licenças, materiais e acessórios no local determinado.
4.1.2	O Termo de Recebimento Provisório será certificado pelo fiscal da Ata indicado pela CONTRATANTE, conforme art. 7º, do Ato Regulamentar nº 08/2015.
4.1.3	As especificações serão conferidas através de verificação técnica dos hardwares, manuais técnicos correspondentes às placas lógicas e periféricos e folhetos do FABRICANTE contendo características técnicas.
4.1.4	Caso seja comprovado pela CONTRATANTE que os equipamentos, licenças, materiais e acessórios não tenham sido entregues integralmente, ou eventualmente venham a ser recusados, no todo ou em parte, por apresentarem defeitos ou avarias, ou não atendam às especificações técnicas e requisitos estabelecidos neste TERMO DE REFERÊNCIA, a CONTRATADA terá o prazo de 15 (quinze) dias úteis, contados a partir da assinatura do Relatório de Pendências para concluir as pendências, sem ônus para a CONTRATANTE, sendo interrompido o processo de recebimento provisório até que a CONTRATADA substitua os itens não atendidos conforme especificado.
4.1.5	Os equipamentos, licenças, materiais e acessórios serão RECEBIDOS DEFINITIVAMENTE, mediante Termo Circunstanciado de Recebimento Definitivo, assinado pelas partes, após o decurso do prazo de 15 (quinze) dias úteis de observação ou vistoria de funcionamento contínuo e sem problemas, a contar da emissão do Termo Circunstanciado de Recebimento Provisório, que comprove a inexistência de vícios construtivos aparentes de acordo com o disposto no art. 69, da Lei N.º 8.666/93.
4.1.6	A assinatura do Termo Circunstanciado de Recebimento Definitivo indica que o objeto recebido está conforme o Contrato, ficando a CONTRATADA quitada dos encargos contratuais, porém, permanecendo sua responsabilidade pelo perfeito funcionamento dos equipamentos e manutenção corretiva *on-site* durante o prazo de garantia.
4.1.7	O Termo de Recebimento Definitivo será certificado pelo gestor e pelo fiscal da Ata indicado pela CONTRATANTE, conforme art. 7º, do Ato Reg nº 08/2015.
4.1.8	Os Termos Circunstanciados de Recebimento Provisório e Definitivo dos equipamentos, licenças, materiais e acessórios serão lavrados e assinados pelos Fiscais e pelo Gestor do Contrato indicados pela CONTRATANTE e anexados ao processo de Recebimento Definitivo do Objeto do Contrato.
4.1.9	No ato de entrega do objeto, a CONTRATADA deverá apresentar documento fiscal válido correspondente ao fornecimento.
4.2	**Recebimento do Serviço de Treinamento:**
4.2.1	O serviço de Treinamento será recebido PROVISORIAMENTE, mediante "Termo Circunstanciado de Recebimento Provisório do Serviço de Treinamento", assinado pelas partes, após decorridos 05 (cinco) dias úteis da conclusão efetiva (e sem pendências) do respectivo serviço, se, no mínimo, 80% das avaliações dos servidores participantes indicarem os conceitos B (Bom) e/ou MB (Muito Bom), na avaliação a ser elaborada pela CONTRATADA.
4.2.2	Caso seja comprovado pela CONTRATANTE que o serviço de Treinamento não foi realizado adequada e integralmente, não atenda às especificações técnicas e requisitos estabelecidos neste TERMO DE REFERÊNCIA, ou tenha recebido um índice inferior a 80% de conceitos B (Bom) e/ou MB (Muito Bom), a CONTRATADA terá o prazo de 05 (cinco) dias úteis, contado a partir da emissão do "Relatório de Pendências do Serviço de Treinamento" para realizar, de imediato, todas as correções e ajustes, concluir as

	pendências identificadas pela CONTRATANTE ou, até mesmo, refazer o respectivo serviço.
4.2.3	O serviço de Treinamento será recebido DEFINITIVAMENTE, mediante "Termo Circunstanciado de Recebimento Definitivo do Serviço de Treinamento", assinado pelas partes, após decorridos 10 (dias) dias úteis da emissão do "Termo Circunstanciado de Recebimento Provisório do Serviço de Treinamento", pela equipe da CONTRATANTE, após constatada a inexistência de avaliações de conceito I (Insatisfatório) e/ou - R (Regular), de acordo com o disposto no art. 69, da Lei N.º 8.666/93.
4.2.4	Os Termos Circunstanciados de Recebimento Provisório e Definitivo do serviço de Treinamento serão lavrados e assinados pelos Fiscais e pelo Gestor do Contrato indicados pela CONTRATANTE e anexados ao Conteúdo Programático e à lista de presença e avaliação do Treinamento para compor o processo de Recebimento Definitivo do Objeto do Contrato.
4.3	**Instalação:**
4.3.1	A Instalação da Solução de Segurança será RECEBIDA PROVISORIAMENTE mediante Termo Circunstanciado de Recebimento Provisório assinado pelas partes em até 15 (quinze) dias úteis, a contar do primeiro dia útil após o recebimento da formalização, por parte da CONTRATADA, comunicando a finalização da instalação do Objeto deste Termo de Referência.
4.3.2	O Termo de Recebimento Provisório será certificado pelo fiscal da Ata indicado pela CONTRATANTE, conforme art. 7º, do Ato Regulamentar nº 08/2015.
4.3.3	Caso seja comprovado pela CONTRATANTE que a Instalação dos equipamentos não tenha sido entregue integralmente, ou eventualmente venha a ser recusado, no todo ou em parte, por não atender às especificações técnicas e requisitos estabelecidos neste TERMO DE REFERÊNCIA, a CONTRATADA terá o prazo de 15 (quinze) dias úteis, contados a partir da assinatura do Relatório de Pendências para concluir as pendências, sem ônus para a CONTRATANTE, sendo interrompido o processo de recebimento provisório até que a CONTRATADA substitua os itens não atendidos conforme especificado.
4.3.4	A Instalação da Solução de Segurança será RECEBIDA DEFINITIVAMENTE, mediante Termo Circunstanciado de Recebimento Definitivo, assinado pelas partes, após o decurso do prazo de 30 (trinta) dias úteis de observação ou vistoria de funcionamento contínuo e sem problemas, a contar da emissão do Termo Circunstanciado de Recebimento Provisório, que comprove a inexistência de vícios construtivos aparentes de acordo com o disposto no art. 69, da Lei N.º 8.666/93.
4.4	À CONTRATANTE resguarda-se o direito de não receber o objeto cuja qualidade ou resultado final seja comprovadamente insatisfatório.
4.5	A Administração rejeitará, no todo ou em parte, a entrega dos bens e serviços em desacordo com as especificações técnicas exigidas neste TERMO DE REFERÊNCIA
4.7	O prazo de vigência da Ata de Registro de Preços será de 12 (doze) meses, contados a partir da data de publicação no diário oficial.
5	**DA GARANTIA:**
5.1	Todos os itens que compõem o objeto deste TERMO DE REFERÊNCIA deverão possuir garantia mínima de 60 (sessenta) meses com atendimento técnico nas dependências do Prédio Sede da Procuradoria-Geral de Justiça do Estado do Maranhão, a contar da data do recebimento definitivo do objeto.
5.2	A garantia deverá cobrir todos os defeitos e vícios de fabricação, mediante substituição dos produtos danificados, em até dias 15 (quinze) dias corridos, a contar da comunicação da fiscalização.
5.3	A CONTRATADA será responsável pelos vícios e danos decorrentes do objeto, de acordo com os artigos

TERMO DE REFERÊNCIA

	12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990).
5.4	A CONTRATADA deverá prover estrutura de Central de Atendimento, gratuita, por meio de linha telefônica, e-mail ou página web, para o acionamento da garantia, devendo funcionar em dias úteis, das 8 às 15 horas e estar em funcionamento a partir da data de entrega dos equipamentos e assim permanecer até o término da garantia dos itens.
6	**DA QUALIFICAÇÃO TÉCNICA**
6.1	**A qualificação técnica deverá ser comprovada pela LICITANTE com a apresentação dos seguintes atestados:**
6.1.1	Atestado de Capacidade Técnica (ACT), em nome da LICITANTE, emitido(s) por pessoa(s) jurídica(s) de direito público ou privado, onde comprove ter prestado os serviços a seguir, sendo aceitos somatórios de atestados de capacidade técnica para comprovação, podendo os mesmos serem de fabricantes diferentes: a) entrega, instalação, configuração e suporte técnico para solução de Next Generation Firewall; b) entrega, instalação, configuração e suporte técnico de solução de proteção contra Ameaças Avançadas de rede para tráfego SMTP e HTTP; c) treinamento oficial ou ministrado por instrutor ou técnico especialista na solução ofertada e que possua certificação do FABRICANTE do Firewall da solução proposta pela LICITANTE.
6.1.2	Atestado(s) que comprove(m), no mínimo, atendimento a 50% dos quantitativos previstos para os itens do objeto.
6.1.3	Atestado de experiência mínima de 2 (dois) anos nas soluções de Next Generation Firewall e de proteção contra Ameaças Avançadas de rede para tráfego SMTP e HTTP, onde será aceito o somatório de atestados de períodos diferentes, não havendo obrigatoriedade do período de dois anos ser ininterrupto.
6.2	Todos os atestados deverão obrigatoriamente ser emitidos por pessoa jurídica de direito público ou privado e conter: a) Razão Social, CNPJ e endereço completo da Empresa Emitente; b) Razão Social da Contratada; c) Número e vigência do contrato, se for o caso; d) Objeto do contrato; e) Declaração de que foram atendidas as expectativas do cliente quanto ao cumprimento de cronogramas pactuados; f) Local e Data de Emissão; g) Identificação do responsável pela emissão do atestado, Cargo, Contato (telefone e correio eletrônico); h) Assinatura do responsável pela emissão do atestado.
6	**DAS OBRIGAÇÕES DA CONTRATADA:**
7.1	Executar o fornecimento do objeto que lhe for adjudicado dentro dos padrões e prazos estabelecidos neste TERMO DE REFERÊNCIA, assim como de acordo com as condições constantes da proposta apresentada durante o processo licitatório.
7.2	Emitir Nota Fiscal/Fatura dos materiais fornecidos no valor pactuado e condições deste TERMO DE REFERÊNCIA, apresentando-a a CONTRATANTE para ateste e pagamento.
7.3	Fornecer pelo prazo de sessenta (sessenta) meses, a contar da data do recebimento definitivo do objeto, suporte técnico informando os procedimentos necessários para abertura de pedido de substituição em caso de problemas dentro do prazo de garantia estipulado.
7.4	Manter durante todo o período de vigência da ata de registro de preços, em compatibilidade com as

	obrigações assumidas, todas as condições de habilitação e qualificação exigidas na Licitação.
7.5	Comunicar à CONTRATANTE, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.
7.6	Comunicar imediatamente à CONTRATANTE a eventual alteração no endereço de sua sede, telefone de contato e e-mail.
7.7	Substituir, às suas expensas, no prazo fixado neste TERMO DE REFERÊNCIA, o objeto com avarias ou defeitos.
7.8	À CONTRATADA é vedado transferir, total ou parcialmente, o objeto da Ata, ficando obrigada perante a PGJ-MA, pelo exato cumprimento das obrigações deste TERMO DE REFERÊNCIA.
7.9	Indicar preposto para representá-la durante a execução da Ata.
7.10	Atender prontamente a quaisquer exigências da Administração, inerentes ao objeto da presente licitação.
7.11	Responsabilizar-se pelas despesas dos tributos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, seguros, deslocamento de pessoal, prestação de garantia e quaisquer outras que incidam ou venham a incidir na execução da Ata.
7.12	O encerramento da vigência contratual não prejudica a manutenção das obrigações das partes, no que se refere aos bens e serviços em garantia, nos termos descritos neste TERMO DE REFERÊNCIA.
8	**DAS OBRIGAÇÕES DA CONTRATANTE:**
8.1	Promover a fiscalização e conferência dos fornecimentos executados pela CONTRATADA e atestar os documentos fiscais pertinentes, quando comprovada a execução total, fiel e correta dos fornecimentos, podendo rejeitar, no todo ou em parte, os objetos entregues fora das especificações deste TERMO DE REFERÊNCIA.
8.2	Comunicar à CONTRATADA toda e qualquer ocorrência relacionada à aquisição ou entrega dos objetos.
8.3	Proceder às advertências, multas e demais comunicações legais pelo descumprimento por parte da CONTRATADA das obrigações assumidas.
8.4	Verificar a regularidade da situação fiscal da CONTRATADA e dos recolhimentos sociais trabalhistas sob sua responsabilidade antes de efetuar os pagamentos devidos.
8.5	Prestar informações e esclarecimentos que venham a ser solicitados pela CONTRATADA.
8.6	Emitir nota de empenho a crédito do fornecedor no valor total correspondente ao material solicitado.
8.7	Enviar a nota de empenho emitida em favor da CONTRATADA.
8.8	Receber o objeto no prazo e condições estabelecidas neste TERMO DE REFERÊNCIA.
8.9	Designar servidores que atuarão como fiscais da Ata de Registro de Preços, que terão a responsabilidade de fiscalizar e acompanhar o cumprimento das obrigações estabelecidas neste TERMO DE REFERÊNCIA.
8.10	Efetuar o pagamento à CONTRATADA no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos.
9	**DAS SANÇÕES ADMINISTRATIVAS:**
9.1	A CONTRATADA será punida com o impedimento de licitar e contratar com a União, Estados, Distrito

	Federal ou Municípios e será descredenciada no SICAF, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas neste Termo de Referência e demais cominações legais, nos seguintes casos:
9.1.1	Apresentação de documentação falsa.
9.1.2	Retardamento da entrega do objeto.
9.1.3	Falha no fornecimento do objeto.
9.1.4	Fraude no fornecimento do objeto.
9.1.5	Comportamento inidôneo.
9.1.6	Declaração falsa.
9.1.7	Fraude fiscal.
9.2	Para os fins do item 9.1.5, reputar-se-ão inidôneos atos tais como os descritos nos artigos 92, parágrafo único, 96 e 97, parágrafo único, da Lei n.º 8.666/1993.
9.3	Para as condutas descritas nos itens 9.1.1, 9.1.4, 9.1.5, 9.1.6 e 9.1.7 serão aplicadas multa de no máximo 30% do valor da nota de empenho.
9.4	Para os fins dos itens 9.1.2 e 9.1.3, serão aplicadas multas nas seguintes condições:
9.4.1	1% (um por cento) do valor do CONTRATO, por dia de atraso na entrega, até o máximo de 20% (vinte por cento). O atraso superior a 20 (vinte) dias corridos configura a inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença.
9.4.2	Até o máximo de 20% (vinte por cento) do valor do CONTRATO no caso de inexecução parcial da obrigação assumida.
9.4.3	30% (trinta por cento) do valor do CONTRATO no caso de inexecução total da obrigação assumida.
9.4.4	Após o 30º (trigésimo) dia de atraso, a PGJ-MA poderá cancelar a nota de empenho, caracterizando-se a inexecução total da obrigação assumida.
9.4.5	O valor da multa poderá ser descontado do pagamento a ser efetuado à CONTRATADA.
9.4.6	Se o valor do pagamento for insuficiente, fica a CONTRATADA obrigada a recolher a importância devida no prazo de 15 (quinze) dias, contados da comunicação oficial.
9.4.7	Esgotados os meios administrativos para cobrança do valor devido pelo CONTRATADO à PGJ-MA, este será encaminhado para inscrição em dívida ativa.
9.4.8	Cumulativamente à pena de multa, no caso de inexecução total ou parcial da avença, poderá ser aplicada a pena de impedimento de licitar e contratar com o Estado do Maranhão, pelo prazo de até 05 (cinco) anos.
9.4.9	A aplicação das penalidades será precedida do devido processo legal, garantida a oportunidade de ampla defesa e contraditório por parte da ADJUDICATÁRIA, na forma da lei.
10	**CRITÉRIOS DE ACEITAÇÃO DO OBJETO**
10.1	O OBJETO será considerado aceito somente após a realização de testes de funcionamento de todos os itens que o compõem. Todas as instalações, customizações e configurações serão conferidas pela CONTRATANTE para verificação de atendimento a todas as especificações e condições exigidas neste TERMO DE REFERÊNCIA.

TERMO DE REFERÊNCIA

11	**CRITÉRIOS DE JULGAMENTO DAS PROPOSTAS**
11.1	O critério de julgamento das propostas será pelo MENOR PREÇO GLOBAL ofertado, no qual todos os itens necessários para a correta e eficiente implantação e operacionalização da solução ofertada deverão ser dispostos, quantificados e precificados.
11.2	A CONTRATANTE realizará a análise de conformidade da proposta técnica de cada LICITANTE confrontando os requisitos especificados no TERMO DE REFERÊNCIA com as características da solução ofertada.
12	**FISCALIZAÇÃO E GERENCIAMENTO DO CONTRATO**
12.1	Caberá à equipe de FISCALIZAÇÃO da contratação, a saber: Gestor do CONTRATO (servidor da área requisitante – CMTI – Antonio Alfredo Pires Oliveira); Fiscal Requisitante do CONTRATO (servidor da área requisitante – CMTI – José da Silva Lucena); Fiscal Técnico da CMTI (servidor da área de Tecnologia da Informação - CMTI – Leonardo Dorneles Figueiredo Silva) e Fiscal Administrativo (servidora da área de Tecnologia da Informação - CMTI – Daniela Nascimento Montelo), a GESTÃO e a FISCALIZAÇÃO do CONTRATO, respectivamente, em acordo com a resolução nº 102/2013 do CNMP e do Ato Regulamentar nº 08/2015-GPGJ.
12.2	O acompanhamento e a fiscalização da execução do CONTRATO consistirão na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por um ou mais representantes da CONTRATANTE, especialmente designados, na forma dos Arts. 67 e 73 da Lei nº 8.666/93.
12.3	A FISCALIZAÇÃO de que trata este item não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da CONTRATANTE ou de seus agentes e prepostos, de conformidade com o Art. 70 da Lei nº 8.666/93.
13	**AVALIAÇÃO DO CUSTO:**
13.1	O OBJETO deste TERMO DE REFERÊNCIA, "Solução de Segurança de Rede", é composto pelos seguintes itens: 1) "Equipamentos de Segurança de Rede" e 2) "Serviço de Treinamento" .
13.2	O Custo Estimado Médio Total foi elaborado com base nas propostas em anexo, apresentadas a pedido da CMTI desta PGJ-MA, referentes aos objetos especificados neste TERMO DE REFERÊNCIA.
13.3	O custo estimado total para aquisição do objeto é de R$ 2.795.781,00 (dois milhões, setecentos e noventa e cinco mil, setecentos e oitenta e um reais), conforme demonstrado no quadro a seguir e nos orçamentos anexados:

LOTE ÚNICO - SOLUÇÃO DE SEGURANÇA DE REDE				
ID	**Item**	**Quant.**	**Preço Unitário**	**Preço Total**
1	"Solução de Segurança de Rede"	4	R$ 683.291,83	R$2.733.167,33
2	"Serviço de Treinamento"	1	R$ 62.613,67	R$ 62.613,67
			Custo Estimado Total:	R$ 2.795.781,00

TERMO DE REFERÊNCIA

14	**ESPECIFICAÇÕES TÉCNICAS MÍNIMAS DO OBJETO:**
14.1	**Especificações do Item 1 - "Solução de Segurança de Rede":**
14.1.1	Deverá possuir funcionalidades de *Next Generation Firewall* (NGFW), ou seja: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.
14.1.2	Deverá ser composto de apenas 1 (um) equipamento appliance físico (não baseado em plataforma PC), contendo hardware, software e firmware especializados.
14.1.3	Deverá realizar análise de conteúdo de aplicações em camada 7.
14.1.4	Deverá suportar gerenciamento via SSH.
14.1.5	Deverá suportar o protocolo de agregação de links 802.3ad (LACP).
14.1.6	Deverá suportar DHCP Relay e DHCP Server.
14.1.7	Deverá suportar sFlow ou Netflow e Jumbo Frames.
14.1.8	Deverá suportar NAT Dinâmico "*Many-to-1*" e "*Many-to-Many*".
14.1.9	Deverá suportar NAT Estático "1-to-1", "*Many-to-Many*" e "bidirecional 1-to-1".
14.1.10	Deverá suportar NAT de Origem e NAT de Destino, inclusive simultaneamente.
14.1.11	Deverá implementar *Network Prefix Translation* (NPTv6) ou NAT66.
14.1.12	Deverá implementar balanceamento de, no mínimo, 2 links de Internet. A solução deverá funcionar de forma transparente, isto é, quando um link ficar indisponível, o acesso à Internet deverá funcionar sem que o administrador do ambiente realize qualquer mudança na solução.
14.1.13	Deverá permitir monitorar via SNMP, através de MIB fornecida pelo Fabricante, no mínimo, os seguintes itens: falhas de hardware, uso de CPU, uso de memória, uso de disco e estatísticas de uso das interfaces de rede.
14.1.14	Deverá possuir proteção anti-spoofing.
14.1.15	Deverá possuir suporte a, no mínimo, 8 milhões de conexões simultâneas.
14.1.16	Deverá possuir suporte a, no mínimo, 180 mil novas conexões por segundo.
14.1.17	Deverá suportar throughput de, no mínimo, 8 Gbps de VPN IPSec.
14.1.18	Deverá estar licenciado para, ou suportar sem o uso de licenças, no mínimo, 2 mil túneis de VPN IPSEC Site-to-Site simultâneos.
14.1.19	Deverá estar licenciado para, ou suportar sem o uso de licença, 2 mil túneis de clientes VPN IPSEC simultâneos.
14.1.20	Deverá suportar throughput de, no mínimo, 7 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, será considerado o de menor valor.
14.1.21	Deverá possuir, pelo menos, 8 interfaces 1000Base-T.

14.1.22	Deverá possuir, pelo menos, 2 interfaces 40Gbps QSFP28 com seus respectivos conectores. Deverão ser fornecidos todos os transceivers/conectores compatíveis com as interfaces QSFP28.
14.1.23	Deverá possuir, pelo menos, 4 interfaces 10GBase-X com conectores SFP+. Deverão ser fornecidos todos os transceivers/conectores compatíveis com as interfaces 10GBase-X.
14.1.24	Deverá possuir fontes redundantes bivolt 100-240 VAC.
14.1.25	Deverá possuir licença perpétua para, ou suportar sem o uso de licenças, armazenamento ilimitado de logs em servidor de backup (ou syslog) externo à solução.
14.1.26	Deverá permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de "*troubleshooting"*.
14.1.27	Deverá suportar configuração de alta disponibilidade nos modos Ativo/Passivo e Ativo/Ativo.
14.1.28	Deverá incluir proteção contra ataques de negação de serviços, possuindo assinaturas específicas para a mitigação de ataques DoS e DDoS.
14.1.29	Deverá possuir os seguintes mecanismos de inspeção de IPS: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes TCP, bloqueio de pacotes malformados.
14.1.30	Deverá ser capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, buffer overflow, ataques por *worms* conhecidos, etc.
14.1.31	Deverá possibilitar a criação de assinaturas de IPS customizadas pela interface gráfica do produto.
14.1.32	Deverá suportar identificação e bloqueio de comunicação com botnets.
14.1.33	Deverá possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas.
14.1.34	Deverá possuir integração com *Microsoft Active Directory* e *LDAP* para identificação de usuários e grupos, permitindo granularidade de controle e de criação de políticas baseadas em usuários e grupos.
14.1.35	Deverá suportar a funcionalidade de *Single Sign-On*, que não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso.
14.1.36	Deverá permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída à internet, para que, antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (*Captive Portal*).
14.1.37	Deverá possuir pelo menos 2 (duas) interfaces Gigabit Ethernet (10/100/1000Base-T), que serão utilizadas como portas WAN, ou seja, como interfaces para rede externa (Multi-Link WAN).
14.1.38	Deverá possuir capacidade de autenticar usuários para administração do Equipamento, através de base de dados local e integrada a servidores TACACS+, LDAP ou RADIUS.
14.1.39	Deverá suportar ações automáticas de envio de *traps* SNMP v2/v3, envio de alertas por e-mail e envio de logs a servidor syslog quando em situações de: HA Failover, Túnel IPSec Up/Down, Interface UP/Down, Appliance em estado inoperante.
14.1.40	Deverá oferecer visualização gráfica, no mínimo, de: aplicações mais utilizadas com respectiva largura de banda; IPs de Destino mais utilizados com respectiva largura de banda, usuários com maior banda utilizada.

14.1.41	No momento da abertura das propostas, todos os componentes de software constantes da Solução deverão possuir EOL (End-of-life) e EOS (End-of-support) não definidos ou anunciados para um prazo superior a sessenta (sessenta) meses.
14.1.42	A solução deverá ser composta de hardware e software licenciado, do mesmo fabricante.
14.1.43	Exceto para as funcionalidades de Antivírus, AntiBot, Controle de Aplicação, Filtro de URL e IPS, todos os demais softwares e componentes da Solução deverão ser fornecidos com licenças perpétuas, isto é, sem prazo de expiração, permitindo o uso continuado da solução baseado nas últimas versões de softwares instalados. Durante todo o prazo da garantia contratual deverão ser fornecidas todas as atualizações de segurança (patches, updates, hotfixes, etc.) para a versão instalada, até seu end-of-life.
14.1.44	A Solução deverá estar licenciada para o funcionamento e atualização, durante todo o período mínimo de 60 (sessenta) meses, a partir do Recebimento Definitivo, de todas as funcionalidades de Antivírus, AntiBot, Controle de Aplicação, Filtro de URL e IPS.
14.1.45	A CONTRATADA deverá disponibilizar, durante todo o período mínimo de 60 (sessenta) meses, a partir do Recebimento Definitivo, a atualização de bases externas de categorização de sites, mensagens, vírus, malware, assinaturas de ataques e vulnerabilidades, bem como dos demais softwares fornecidos e que compõem o equipamento, tão logo ocorra o lançamento de novos softwares em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos softwares fornecidos.
14.1.46	A solução deverá ser licenciada para um número ilimitado de usuários e endereços IP.
14.1.47	Deverá possuir licença perpétua para, ou suportar sem o uso de licenças, a funcionalidade de envio automático de logs para servidor de backup e syslog externo ou similar.
14.1.48	Deverá possuir "Garantia ON-SITE", a ser prestada pelo período de, no mínimo, sessenta (sessenta) meses, a contar do recebimento definitivo do objeto do Contrato, para todos os componentes e peças da solução ofertada, sem nenhum custo adicional para a CONTRATANTE, incluindo substituição de equipamentos, de materiais, de acessórios e correções de defeitos que afetem o desempenho, funcionalidade e/ou configuração dos produtos.
14.1.49	Deverá ser fornecido com kit para instalação em Rack de 19".
14.1.50	**Especificações relacionadas a Controle de Políticas de Firewall:**
14.1.50.1	Deverá suportar controles de políticas por aplicações, por grupos estáticos de aplicações, por grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e por categorias de aplicações.
14.1.50.2	Deverá suportar controles de políticas por usuários, por grupos de usuários, por IPs, por redes, por zonas de segurança, por porta e por protocolos.
14.1.50.3	Deverá suportar inspeção e descriptografia de SSL em tráfego de entrada e saída.
14.1.50.4	Deverá suportar descriptografia de tráfego de entrada e saída em conexões negociadas com TLS 1.2.
14.1.50.5	Deverá permitir o bloqueio de arquivo por sua extensão e por *mime type*.
14.1.50.6	Deverá suportar agendamento de políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
14.1.51	**Especificações relacionadas a Controle de Aplicações:**

	Deverá inspecionar *payloads* de pacotes de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo.
	Deverá permitir a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.
	Deverá reconhecer, no mínimo, 2000 aplicações diferentes, incluindo, mas não se limitando 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 e-mail.
	Deverá reconhecer pelo menos as seguintes aplicações: *torrent, skype, facebook, linked-in, twitter, citrix, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, google-docs*.
	Deverá ter a capacidade de identificar aplicações e ataques que utilizam táticas evasivas via comunicações criptografadas.
	Deverá suportar descriptografia SSL a fim de possibilitar a leitura de *payloads* dos pacotes de dados para checagem de assinaturas de aplicações conhecidas pelo fabricante.
	Deverá realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas e validar se o tráfego corresponde com a especificação do protocolo.
	Deverá possuir capacidade para identificar o uso de táticas evasivas via comunicações criptografadas.
	Deverá atualizar a base de assinaturas de aplicações automaticamente.
	Deverá possuir a capacidade de identificar o usuário de rede com integração ao *Microsoft Active Directory*, sem a necessidade de instalação de agentes nas estações dos usuários.
	Deverá suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos.
	Deverá 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.
	Deverá possibilitar a diferenciação e controle de partes das aplicações, como, por exemplo, permitir o Hangouts Chat e bloquear a chamada de vídeo.
	Deverá possibilitar a diferenciação de aplicações *proxies* (*psiphon, freegate*, etc), possuindo granularidade de políticas para os mesmos.
	Deverá possibilitar a criação de grupos dinâmicos de aplicações baseados em características das mesmas.
	Deverá possibilitar a criação de grupos estáticos de aplicações.
14.1.52	**Especificações relacionadas a Prevenção de Ameaças:**
	Deverá possuir módulos de IPS, Antivírus e *Anti-Spyware* integrados no próprio equipamento.
	Deverá incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e *Anti-Spyware*).
	Deverá implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, bloquear, permitir e gerar log.

	As assinaturas deverão poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração.
	Deverá ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes.
	Deverá permitir o bloqueio de *exploits* conhecidos.
14.1.53	**Especificações relacionadas a *QoS*, *Traffic Shaping*, Filtro de Dados e Filtros de URL:**
	Deverá permitir a criação de filtros de URL por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).
	Deverá permitir a criação de filtros de URL por usuários, grupos de usuários, IPs e redes.
	Deverá possuir funcionalidade de criação de políticas baseadas no controle por URL e categoria de URL.
	Deverá possuir pelo menos 40 categorias de URLs.
	Deverá permitir a customização de página de bloqueio de URL.
	Deverá possuir a funcionalidade de apresentar tela de bloqueio mas permitir que o usuário "reporte" possíveis categorizações incorretas do site.
	Deverá suportar a criação de políticas de *Traffic Shaping* por endereço de origem, por endereço de destino, por usuário, por grupo de usuários, por aplicação e por porta.
	O QoS deverá possibilitar a definição de tráfego com banda garantida, banda máxima permitida e com fila de prioridade.
	Deverá suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP e aplicações como *Skype*.
	Deverá permitir a criação de filtros para arquivos e dados pré-definidos.
	Deverá permitir identificação e bloqueio de transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc).
	Deverá suportar identificação de arquivos compactados e aplicação de políticas sobre o conteúdo desses tipos de arquivos.
14.1.54	**Especificações relacionadas a VPN:**
	Deverá suportar VPN Site-To-Site, VPN Client-To-Site, VPN IPSec e VPN SSL.
	A VPN IPSEc deverá suportar: 3DES Encryption; Autenticação MD5; Autenticação SHA-1; Diffie-Hellman; Algoritmo Internet Key Exchange; AES 128 e 256.
	Deverá suportar VPN em IPv4 e IPv6.
	Deverá permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução.
	A VPN SSL deverá suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento, por meio de interface Web ou cliente nativo do sistema operacional.
	Deverá suportar a atribuição de DNS nos clientes remotos de VPN.
	Deverá permitir criar políticas de controle de aplicações, IPS, Antivírus, Antispyware e filtro de URL para

	tráfego dos clientes remotos conectados na VPN SSL.
	Deverá suportar autenticação via Microsoft Active Directory, LDAP e certificado.
	Deverá permitir que a conexão com a VPN seja estabelecida das seguintes formas: a) automaticamente; b) sob demanda do usuário.
	Os agentes ou configuração do cliente nativo do sistema operacional da VPN SSL e IPSEC client-to-site deverão ser compatíveis com pelo menos: Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior).
14.1.55	**Especificações relacionadas ao gerenciamento do equipamento:**
	Deverá possuir capacidade de gerenciamento centralizado simultâneo de todos os equipamentos relacionados ao **Item 1 - "Solução de Segurança de Rede"**
	Deverá ser fornecido no formato de "appliance virtual" compatível com ambiente VMware ESXi 6.0 (ou superior) ou "*appliance* físico".
	Deverá possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos gerenciados.
	Deverá suportar o controle de todas as funcionalidades via interface gráfica.
	Deverá permitir acesso concorrente de administradores.
	Deverá permitir definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações, etc.
	Deverá possuir a funcionalidade de geração de alertas automáticos via e-mail, SNMP e Syslog.
	Deverá possuir funcionalidade de geração de backup e restore das configurações dos equipamentos gerenciados.
	Deverá ser permitido aos administradores se autenticarem na Solução de Gerenciamento através de contas de usuários LOCAIS.
	Deverá ser permitido aos administradores se autenticarem na Solução de Gerenciamento através de base externa LDAP, RADIUS e Certificado Digital.
	Deverá registrar as ações efetuadas por quaisquer usuários.
	Deverá possibilitar a criação e administração de políticas de: firewall, controle de aplicação, IPS, Antivírus, AntiSpyware e Filtro de URL.
	Deverá possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos **"Equipamentos relacionados à Solução de Segurança de Rede"**.
	Deverá possibilitar gerenciamento centralizado das licenças de todos os *appliances* controlados, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta.
	Deverá permitir visualizar informações detalhadas dos dispositivos gerenciados, tais como hostname, serial, IP, modelo, horário do sistema e firmware.
	Deverá permitir criar templates de configurações dos dispositivos gerenciados.
	Deverá permitir configurar e visualizar balanceamento de links nos dispositivos gerenciados de forma centralizada, ou permitir que, através da console centralizada seja possível acessar as configurações de

	balanceamento de links de cada equipamento.
	Deverá suportar receber logs de todos os dispositivos gerenciados.
	Deverá possuir capacidade de gerenciamento, sem custo extra posterior(ex: licenças e/ou outros) para a Contratante, de, no mínimo, 10 TB de logs armazenados localmente e capacidade ilimitada para gerenciamento de logs armazenados em servidores de backup (ou syslog) externos à solução.
	Deverá permitir geração de relatórios em tempo real, para a visualização de tráfego observado, nos formatos: mapas geográficos e tabela.
	Deverá possuir mecanismo para que logs antigos sejam removidos automaticamente.
	Deverá permitir a exportação de relatórios no mínimo em dois dos seguintes formatos: HTML, PDF, XML ou CSV.
	Deverá permitir exportar os logs em CSV.
	Deverá gerar logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.
	Deverá realizar a centralização dos logs de todos os appliances gerenciados, mas também deverá suportar a utilização de um syslog externo ou similar.
	Deverá possuir relatórios pré-definidos.
	Deverá suportar o envio automático de logs para um servidor FTP ou NFS externo à solução.
	Deverá permitir de forma centralizada visualizar os logs recebidos por um ou vários dispositivos externos incluindo a capacidade de uso de filtros nas pesquisas deste log.
	Deve permitir a criação de Dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, origem e destino.
	Deverá possuir um Indicador de Comprometimento que mostre usuários finais com utilização web suspeita, devendo informar, no mínimo: endereço IP do terminal do usuário, hostname, sistema operacional, veredito (classificação geral de ameaça) e número de ameaças detectadas.
	Deverá possuir funcionalidades de geração de relatórios de VPNs.
	Deverá possuir funcionalidades de geração de relatórios de Sistemas de Prevenção de Intrusão (IPS).
14.1.56	**Especificações relacionadas à instalação:**
14.1.56.1	Deverão ser realizados todos os procedimentos necessários à completa instalação dos equipamentos e softwares fornecidos para o ambiente da CONTRATANTE, utilizando-se as melhores práticas definidas pelo fabricante, até o perfeito funcionamento da solução.
14.1.56.2	No decorrer da realização dos serviços a equipe técnica da CONTRATANTE acompanhará todas as atividades para o perfeito funcionamento em relação às ações executadas.
14.1.56.3	Deverá ser entregue, após a realização dos serviços, toda a documentação descrevendo os serviços realizados, procedimentos utilizados, passo-a-passo da instalação e configuração para o ambiente do cliente, informações detalhadas e *know-how* para a perfeita implementação dos produtos (processos, screenshots, customizações, especificações, etc).

TERMO DE REFERÊNCIA

14.1.56.4	A instalação compreende a migração de todas as regras e demais configurações do Firewall atual da CONTRATANTE para a nova SOLUÇÃO contratada.
14.1.56.5	O prazo para a execução completa da instalação é de 15 dias.
14.1.56.6	A CONTRATADA deverá apresentar um PLANO DE IMPLANTAÇÃO, em até 15 (quinze) dias da emissão da Ordem de Serviço pela CONTRATANTE, contendo a documentação detalhada das atividades de entrega, instalação, configuração e testes dos equipamentos e softwares que compõem a solução.
14.1.56.7	Para garantir que a instalação e migração não afetará negativamente o ambiente da CONTRATANTE, os procedimentos e atividades deverão ser realizados por técnicos qualificados pelo fabricante dos produtos envolvidos, comprovado no ato de entrega do PLANO DE IMPLANTAÇÃO.
14.2	**Especificações do Item 2 - "Serviço de Treinamento":**
14.2.1	A CONTRATADA deverá realizar Treinamento Presencial *Hands-On* (Teoria e Prática), nas dependências da CONTRATANTE, capacitando a Equipe Técnica indicada pela CONTRATANTE em tarefas de instalação, configuração, customização, gerenciamento e utilização da solução ofertada.
14.2.2	Deverá ser ministrado por instrutor ou técnico, especialista na solução ofertada e que possua certificação do FABRICANTE dos equipamentos na modalidade de implementador.
14.2.3	Deverá possuir carga horária mínima de 40 horas.
14.2.4	Deverá ser fornecido certificado de participação.
14.2.5	Deverá ser fornecido todo o material didático a ser utilizado durante o Treinamento, em formato digital, incluindo documentações dos produtos que servirão como orientação e referência para os estudos e futuras implementações ou consultas.
14.2.6	A CONTRATADA deverá entregar os certificados e lista de presença do Treinamento no prazo de até 05 (cinco) dias úteis da realização/conclusão do serviço.
14.2.7	Deverá suportar, no mínimo, 20 (vinte) participantes da Equipe Técnica da CONTRATANTE.

Equipe de Planejamento da Contratação			
Gestor do Contrato	**Integrante Requisitante**	**Integrante Técnico**	**Integrante Administrativo**
ANTONIO ALFREDO PIRES OLIVEIRA:1069129 Assinado de forma digital por ANTONIO ALFREDO PIRES OLIVEIRA:1069129 Dados: 2021.10.18 08:43:35 -03'00'	JOSE DA SILVA LUCENA:1071469 Digitally signed by JOSE DA SILVA LUCENA:1071469 DN: C=BR, O=ICP-Brasil, OU=Autoridade Certificadora da Justiça - AC-JUS, OU=05623469000130, OU=Presencial, OU=Cert-JUS Poder Publico - A3, OU=Ministerio Publico do Estado do Maranhao - MPMA, OU=ANALISTA MINISTERIAL, CN=JOSE DA SILVA LUCENA:1071469 Reason: I am approving this document Location: Date: 2021-10-15 12:41:38	LEONARDO DORNELES FIGUEIREDO SILVA:1071397 Assinado de forma digital por LEONARDO DORNELES FIGUEIREDO SILVA:1071397 Dados: 2021.10.15 12:38:10 -03'00'	DANIELA NASCIMENTO MONTELO:1071575 Assinado de forma digital por DANIELA NASCIMENTO MONTELO:1071575 Dados: 2021.10.15 12:37:29 -03'00'
Antonio Alfredo Pires Oliveira	**José da Silva Lucena**	**Leonardo Dorneles Figueiredo Silva**	**Daniela Nascimento Montelo**
Matrícula: 1069129	**Matrícula: 1071469**	**Matrícula: 1071397**	**Matrícula: 1071575**