



FUNDAÇÃO JORGE DUPRAT FIGUEIREDO DE SEGURANÇA E MEDICINA DO TRABALHO
Rua Capote Valente, 710, - Bairro Pinheiros, São Paulo/SP, CEP 05409-002
Telefone: e Fax: @fax_unidade@ - <https://www.gov.br/fundacentro/pt-br>

TERMO DE REFERÊNCIA

Processo nº 47648.001272/2021-18

1. OBJETO DA CONTRATAÇÃO

1.1. Solução de segurança lógica (firewall) com renovação de licenças dos equipamentos da Sede/Centro Técnico Nacional (CTN) e das Unidades Descentralizadas (UD's) da Fundacentro.

2. DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1. ***Bens e serviços que compõem a solução***

2.2. As quantidades e respectivos códigos dos itens a que se referem a presente contratação seguem especificados na tabela a seguir:

Tabela 1 - Escopo da contratação

Item	Descrição do item de serviço (objeto)	CATMAT/CATSER	Quantidade	Unidade de medida
1	Equipamento firewall principal para a Sede/CTN (FortiGate-400E – FG-400E – HW)	481647	1	unidade
2	Licença de firewall principal FortiGate-400E Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web Filtering, Antispam Service, and 24x7 Fortinet) válida por 48 meses	24333	1	licença para uso de software
3	Licença de firewall de escritório remoto para as UD's (FTNT-RENEW - RENEW - 48 M – Fortigate 30E) válida por 48 meses	24333	12	licença para uso de software
4	Licença de gerenciador de firewall (FortiManager) válida por 48 meses	24333	1	licença para uso de software

2.3. Classificação dos serviços

2.3.1. Trata-se de serviço comum de caráter continuado sem fornecimento de mão de obra em regime de dedicação exclusiva, a ser contratado mediante licitação, na modalidade Pregão, em sua forma eletrônica.

2.3.2. Os serviços a serem contratados enquadram-se como solução de tecnologia da informação, sendo, portanto, abrangidos pela Instrução Normativa nº 01, de 4 de maio de 2019, da Secretaria de Governo Digital, do Ministério da Economia (IN SGD/ME nº 01, de 2019), e suas alterações, nominalmente as alterações constantes nas Instruções Normativas SGD/ME nº 202, de 2019, SGD/ME nº 31, de 2021 e SGD/ME nº 47, de 2022.

2.3.3. De acordo com o art. 3º, Inciso I da IN 01/2019, a contratação não incorrerá em mais de uma solução de TIC em um único contrato, pois os serviços a serem contratados representam um dos vários serviços de TI da Fundacentro.

2.3.4. A Equipe de Planejamento da Contratação observou os guias, manuais e modelos publicados pelo órgão do SISP conforme recomenda o art. 8º, §2 da IN 01/2019 e a supervisão será exclusivamente por servidores desta Fundacentro.

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

2.3.6. Pelo fato de o objeto desta contratação se caracterizar como “serviço comum”, nos termos do art. 1º da Lei nº 10.520/2002 e do art. 3º, II, do Decreto nº 10.024/2019, será adotada a modalidade pregão na forma eletrônica. Informa-se que o enquadramento do objeto como “serviço comum” se justifica pelo fato de se tratar da contratação cujo padrão de desempenho e qualidade pode ser objetivamente definido por meio de especificações usuais de mercado, havendo diversos fornecedores capazes de prestá-los.

3. JUSTIFICATIVA PARA A CONTRATAÇÃO

3.1. *Contextualização e Justificativa da Contratação*

3.1.1. A informação é um dos principais ativos das organizações e instituições públicas, tratando-se de um elemento fundamental para a tomada de decisões em todos os níveis, sendo determinante para a gestão governamental. Nesse sentido, os gestores precisam promover ações para prover a segurança de tais informações. Os constantes ataques cibernéticos, a necessidade de continuidade do negócio e a evolução de ameaças das mais variadas espécies criam a necessidade de contratação de uma solução que proteja as informações dos órgãos e diminua os riscos de acesso indevido as mesmas.

3.1.2. Inseridos dentro de um contexto muito dinâmico de evolução constante de tecnologia, em um curto intervalo de tempo, os equipamentos destinados à segurança da informação podem se tornar obsoletos a tal ponto de não suportarem o aumento do tráfego de internet e dados, o crescente número de novos usuários e as novas tentativas de invasões nas redes corporativas. Dentro do contexto analisado, o firewall representa um quesito de segurança fundamental, uma vez que regula o tráfego de dados entre redes distintas e impede a transmissão e recepção de informações a partir de acessos nocivos ou não autorizados na rede.

3.1.3. Partindo-se de tais pressupostos, a contratação consistirá na contratação de licenças de software de equipamento firewall corporativo e multifuncional. Essa solução inclui, dentre outras funcionalidades: anti-malware, anti-spyware, anti-vírus, anti-bot, filtro de conteúdo e filtro de URL, controle de aplicações, inspeção de pacotes, IPS, IDS, relatórios, inspeção SSL, VPNs, QoS, Autenticação de usuários e Anti-DoS de rede.

3.1.4. Também, a contratação da solução de segurança vai além da contratação das licenças. É uma busca por uma solução que continue com a maturidade em segurança de redes da FUNDACENTRO existente com firewall principal na Sede/CTN, firewalls secundários nas UD's e com gerenciamento centralizado de todos os equipamentos numa solução integrada.

3.1.5. A segurança lógica da Fundacentro é composta por várias barreiras contra invasores. O firewall é uma das primeiras barreiras e requer licença ativa para que continue protegendo a rede de dados da Fundacentro.

3.2. *Alinhamento aos Instrumentos de Planejamento Institucionais*

3.2.1. A Equipe de Planejamento da Contratação (EPC) foi designada pela Portaria FUNDACENTRO nº 630 de 17/08/2021 (SEI ID [0134242](#)), e tem como membros:

- a) Diego Ricardi dos Anjos - Demandante (coordenador)
- b) Norisvaldo Ferraz Júnior - Demandante
- c) Juan Gomes Pereira - Representante da Unidade de Compras

Tabela 2 - Alinhamento estratégico

ALINHAMENTO AO PLANO ESTRATÉGICO	
ID	Objetivos Estratégicos da FUNDACENTRO
01	Modernização Organizacional: Otimizar recursos para aumento da produtividade e investimento na área finalística
02	Produção de Conhecimento: Fortalecer a capacidade de resposta aos desafios atuais e futuros do trabalho
03	Difusão do Conhecimento: Difundir o conhecimento utilizando novas tecnologias de informação e comunicação
04	Visibilidade Institucional: Modernizar a comunicação institucional

Tabela 3 - Alinhamento PDTIC

ALINHAMENTO AO PDTIC			
ID	Necessidade	ID	Ação
N1	Garantir a disponibilidade dos serviços de TIC	A2101	Garantir a disponibilidade dos serviços de TIC
N4	Renovar os contratos de serviços de TIC com vencimento em 2021-2022		
N9	Viabilidade do teletrabalho		

Tabela 4 - Alinhamento PAC

ALINHAMENTO AO PAC 2020	
Item	Descrição
602	STIC - CONTRATO - RENOVAÇÃO DE LICENÇAS DOS FIREWALLS (firewall da Sede/CTN)
603	STIC - CONTRATO - RENOVAÇÃO DE LICENÇAS DOS FIREWALLS (firewall das UD's)
604	STIC - CONTRATO - RENOVAÇÃO DE LICENÇAS DOS FIREWALLS (solução de gerenciamento centralizado)

3.2.2. O alinhamento ao PDTIC contempla a Estratégia de Governo Digital e a Plataforma de Cidadania Digital, quando aplicáveis, viabilizando a segurança lógica necessária para o fornecimento desses serviços ao cidadão.

3.3. *Estimativa da demanda*

3.3.1. A estimativa da demanda para a solução de segurança lógica (segurança de perímetro usando equipamentos e licenças de firewall) prevista neste Termo de Referência (TR) contempla a continuidade de utilização dos equipamentos de segurança lógica (firewall) existentes em todas as UD's (por isso o licenciamento de 12 localidades) mais o equipamento principal utilizado na Sede/CTN. Contudo, o equipamento da Sede/CTN, conforme se observa no Estudo Técnico Preliminar (ETP) nº 30/2021 (SEI ID [0163469](#)) atingirá seu término de vida útil em aproximadamente 1 ano, inviabilizando futuras renovações de licenciamento. Nesse sentido, para que não seja necessário substituir todos os equipamentos, softwares e serviços, é necessária a aquisição de novo equipamento principal para a Sede/CTN. Dessa forma será mantido o gerenciamento centralizado de toda a solução de segurança lógica (firewalls) com a consequente gestão das políticas de segurança de maneira organizada, sabendo

as políticas aplicadas em cada localidade. Considera-se, portanto, uma licença para cada equipamento, que estão devidamente elencados nos requisitos técnicos deste TR.

3.4. ***Parcelamento da Solução de TIC***

3.4.1. Opta-se, nesta contratação, conforme apresentado no ETP nº 30/2021, a contratação por lote único.

3.4.2. A opção por lote único considera a imperiosa interdependência dos itens e da consequente prestação dos serviços durante a vigência do Contrato, considerando que as licenças são totalmente correlacionadas e os equipamentos operam de maneira integrada e gerenciada pela Sede/CTN.

3.4.3. Além disso, a experiência anterior do CTIC em cenários não gerenciados por um único prestador de serviços para serviços interdependentes Contrato apresentou muita dificuldade de gerenciamento e diagnóstico de possíveis problemas. Exemplo disso foram os Contratos nº 02/2013 e 03/2013. Nesse cenário em que a licitação foi realizada por itens, duas empresas diferentes venceram parte dos itens. Administrar dois contratos com a mesma finalidade exigiu o contato com diferentes Prepostos, e forçou um esforço administrativo incompatível com a força de trabalho da área de tecnologia da informação, culminando na deflagração de outra licitação, dessa vez unificando a prestação de serviços.

3.4.4. A presente contratação, embora envolva apenas 3 itens, se contratada por itens e não por lote único, exigiria o contato com diferentes prepostos e diferentes empresas, que podem ficar intercambiando possíveis problemas de licenciamento e interoperabilidade dos equipamentos, tornando a execução do contrato deficiente, ou mesmo impossibilitando tecnicamente a execução contratual.

3.4.5. Uma contratação com o não parcelamento da solução se mostra o melhor cenário econômico e de gestão.

3.4.6. A prestação dos serviços por um único fornecedor possibilita a melhor prestação de serviços, bem como do conhecimento otimizado do ambiente computacional da FUNDACENTRO, onde se presume que a prestação do serviço será mais célere, econômica, com menor risco e melhor qualidade para a Instituição.

3.4.7. Adicionalmente, destacam-se outros ganhos de ordem técnica decorrentes da adoção de um processo metodológico único para a prestação dos serviços contratados que envolvem atividades interconectadas. A opção por lote único mitigará atrasos ou retrabalhos, inerentes das diferenças metodológicas, quando da existência de mais de uma CONTRATADA.

3.4.8. Nesse aspecto, justifica-se também a opção de contratação dos serviços em um lote único pelos mesmos princípios administrativos da confiabilidade e conveniência técnica na contratação, pois como há dependência entre os serviços que compõem o objeto licitado, a restrição à inclusão de uma terceira pessoa no processo mostra-se mais adequada.

3.4.9. Pela mesma razão, a inserção de uma terceira pessoa na relação entre os órgãos e a licitante vencedora deste processo dispersaria a visão de motivos e finalidade, colocando em risco a qualidade dos serviços contratados. O modelo proposto de contratação representa a gestão integrada sem divisão de responsabilidades, inibindo conflitos, sobreposição de atividades e a diluição do comprometimento com o todo do processo.

3.4.10. Pela ótica do gerenciamento, é imperativo que uma única empresa tenha sobre si a responsabilidade dos procedimentos em execução, bem como demonstre deter conhecimento simultâneo dos itens contratados, para que possa responder pelos resultados que lhe serão exigidos nos Níveis de Serviço.

3.4.11. Sob o ponto de vista econômico a contratação única evita ônus administrativos e burocráticos consequentes à contratação concomitante de mais de uma empresa prestadora de serviços, e gera economia de escala, tempo, ganhos de eficiência e maior compromisso da CONTRATADA. O agrupamento de todos os itens para atendimento por um único licitante não só reduzirá consideravelmente os riscos de execução, como também irá permitir propostas mais consistentes e econômicas por parte dos licitantes, reduzindo os custos a serem apresentados.

3.4.12. As justificativas relacionadas acima atendem ao disposto especificamente quanto à comprovação do inter-relacionamento técnico entre os serviços contratados, da necessidade de gerenciamento centralizado, além de implicar em vantagem e economicidade para a Administração, portanto a comprovação e os fundamentos apresentados corroboram a contratação em lote único.

3.4.13. Considerando-se a inviabilidade técnica e econômica para o parcelamento do objeto da presente contratação, bem como consideradas as suas respectivas peculiaridades, interdependência e natureza acessória entre as parcelas do objeto, a contratação pretendida deverá ser realizada por Adjudicação Global.

3.4.14. A contratação ora pretendida a ser atendida por um único fornecedor, se mostra mais adequada, Neste caso, visto que se o serviço fosse dividido em itens/lotos diferentes, apesar de oferecerem soluções similares em conceito, os fornecedores trabalham com características de execução diferentes, o que poderia acarretar numa incompatibilidade técnica para integração de toda solução.

3.4.15. Conforme Acórdão 861/2013-Plenário - É lícito os agrupamentos em lotes de itens a serem adquiridos por meio de pregão, desde que possuam mesma natureza e que guardem relação entre si. Além disso, a solução de TI, objeto da contratação em tela, possui uma natural indivisibilidade, o que também inviabiliza a contratação de seus serviços por item de forma separada.

3.4.16. Segundo o acórdão 5260/2011 – TCU – 1ª câmara, de 06/07/2011, “Inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem correlação entre si”. A adjudicação global proposta nesse documento agrupa solução e serviços de uma mesma natureza, que guardam correlação entre si, seja por similaridade técnica ou de tecnologia, bem como de aplicabilidade em busca de uma única solução, sem causar qualquer prejuízo à ampla competitividade.

3.4.17. Ademais a opção pela contratação conjunta, e não fracionada, dos serviços, não constitui qualquer afronta aos termos do art. 23, §1º, da Lei 8.666/93 ou da Súmula 247 do TCU. Consta na Lei 8666/93:

“Art. 23. (...)§ 1º As obras, serviços e compras efetuadas pela administração serão divididas em tantas parcelas quantas se comprovarem técnica e economicamente viáveis, procedendo-se à licitação com vistas ao melhor aproveitamento dos recursos disponíveis no mercado e à ampliação da competitividade, sem perda da economia de escala.”

3.4.18. Por sua vez, consta na Súmula 247 do TCU:

“É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade.” (grifo nosso)

3.4.19. Tanto a disciplina legal, quanto a Súmula do TCU, indicam que a viabilidade técnica do fracionamento deve ser analisada para fins de determinar a possibilidade de licitações distintas (ou lotes distintos na mesma licitação) do objeto que se pretende adquirir. No caso em comento, o objeto licitado envolve tratamento técnico, que demanda que o fornecedor dos serviços tenha conhecimento sobre toda a solução existente. Segregar as contratações, deixando a possibilidade de empresas diferentes prestarem os serviços, é um risco enorme para a FUNDACENTRO, pois deixará aberta a oportunidade para problemas de integração e de administração da solução CONTRATADA entre diferentes fornecedores. Nesse sentido, em respeito à legislação vigente e na busca pela economicidade, se optou por garantir a padronização dos serviços a partir da contratação de um único prestador para realizar os serviços em questão.

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

3.5.1. Fornecer segurança de perímetro para os ativos de rede da Fundacentro

3.5.2. Prover acesso seguro à internet, conforme parâmetros definidos pela CTIC

- 3.5.3. Segurança no tráfego de dados dos sistemas internos, como SEI, SGPA e outros
- 3.5.4. Orquestração e gerenciamento de políticas de segurança de rede, relativas ao acesso à Internet e proteção de ameaças advindas da Internet
- 3.5.5. Viabilização do acesso via VPN para os servidores efetivos para acessarem os recursos da rede interna advindos de redes externas, como quando da utilização do programa de gestão/plano de trabalho

4. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. *Requisitos de Negócio*

- 4.1.1. Manter os serviços de tecnologia da informação, em especial a segurança lógica de rede, que são providos por meio dos equipamentos firewall localizados na Sede/CTN e nas UD's.
- 4.1.2. Uma vez que os firewalls protegem o tráfego de rede da Sede/CTN e das UD's, ele viabiliza a publicação do SEI e de outros sistemas OnPremise (dentro das dependências da Fundacentro), na Internet.
- 4.1.3. Além disso, o firewall protege a rede contra invasores externos, com tecnologias anti-malware, anti-spyware, anti-vírus, anti-bot, filtro de conteúdo e filtro de URL, controle de aplicações, inspeção de pacotes, IPS, IDS, relatórios, inspeção SSL, VPNs, QoS, Autenticação de usuários e Anti-DoS.

4.2. *Requisitos de Capacitação*

- 4.2.1. Após a entrega da solução, deverá(ão) ser(em) realizada(s) reunião(ões) para transferência de conhecimento com relação às possíveis atualizações no software dos firewalls e que apresentem novas funcionalidades para proteção da rede. Também deve apresentar informações como a ferramenta utilizada para abertura de chamados quando necessário, a escalção de chamados se necessário para um superior, transferência de contatos, e outros sistemas/meios de comunicação que se façam necessários para o adequado conhecimento da solução implantada. A documentação entregue (por meio online) deve ser suficiente para esclarecer os procedimentos a serem executados pela CTIC.

4.3. *Requisitos Legais*

- 4.3.1. São normas aplicáveis ao processo licitatório:

- Lei nº 8.666/1993: Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências;. Inciso II e § 2º: Dispõe sobre a duração dos contratos ficará adstrita à vigência dos respectivos créditos orçamentários, onde a prestação de serviços a serem executados de forma contínua, com vistas à obtenção de preços e condições mais vantajosas para a administração seja limitada a sessenta meses.
- 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, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências
- Instrução Normativa nº 5/2017- MP: Dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional.
- Instrução Normativa SLTI/MP nº 01/2010: 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.
- Instrução Normativa SGD/ME nº 01/2019: Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.
- Instrução Normativa nº 73, de 5 de agosto de 2020 - Dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

- Instrução Normativa nº 40, de 22 de maio de 2020 - Dispõe sobre a elaboração dos Estudos Técnicos Preliminares - ETP - para a aquisição de bens e a contratação de serviços e obras, no âmbito da Administração Pública federal direta, autárquica e fundacional, e sobre o Sistema ETP digital.
- Decreto nº 10.024/2019: regulamenta a licitação, na modalidade de pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal.

4.3.2. Ainda se aplicam as seguintes normas relativas à segurança da informação:

- Lei 12.527, de 18/11/2011 (que regula o acesso à informações previsto em lei);
- Decreto nº 7.724, de 16/05/2012 (que regulamenta a lei Lei 12.527, de 18/11/2011);
- Decreto nº 7.845, de 14/11/2012 (que trata do credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo);
- Decreto 9.637, de 26 de dezembro de 2018 9 (que, entre outras coisas, institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação).

4.3.3. Além das normas aqui elencadas, são aplicáveis outras normas correlatas aos processos licitatórios e às contratações no âmbito da Administração Pública Federal

4.4. **Requisitos Temporais**

4.4.1. A instalação do equipamento e das licenças deverá ocorrer no prazo máximo de 60 dias corridos após a emissão da Ordem de Fornecimento de Bens (conforme modelo no Anexo I), emitido pela Fundacentro.

4.4.2. O prazo estipulado poderá ser prorrogado por mais 60 dias a partir de solicitação formal da Contratada, sendo a prerrogativa da Fundacentro conceder ou não a prorrogação.

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

4.5.1. Durante a execução de tarefas no ambiente da FUNDACENTRO, os funcionários da CONTRATADA deverão observar, no trato com os servidores e demais colaboradores a urbanidade e os bons costumes de comportamento, tais como: asseio, pontualidade, cooperação, respeito mútuo, discrição e zelo com o patrimônio público. Deverão ainda portar identificação pessoal, de acordo com as normas internas da Instituição.

4.5.2. A disponibilização dos softwares em meio exclusivamente digital está alinhada à sustentabilidade devido à não utilização de embalagens e outros insumos relativos.

4.6. **Requisitos de Arquitetura Tecnológica**

4.6.1. *Equipamentos e números de série nas Unidades Descentralizadas (UD's) e do Gerenciador de firewalls:*

- 4.6.1.1. Product Description: EAMG/CRMG - Product Serial Number: FGT30E3U16029231
- 4.6.1.2. Product Description: UDCA/ERCA - Product Serial Number: FGT30E3U16029418
- 4.6.1.3. Product Description: EADF/CRDF - Product Serial Number: FGT30E3U16029529
- 4.6.1.4. Product Description: EABA/CRBA - Product Serial Number: FGT30E3U16029608
- 4.6.1.5. Product Description: UDBS/ERBS - Product Serial Number: FGT30E3U16029737
- 4.6.1.6. Product Description: EAES/CEES - Product Serial Number: FGT30E3U16030458
- 4.6.1.7. Product Description: EARS/CERS - Product Serial Number: FGT30E3U16030728
- 4.6.1.8. Product Description: EASC/CESC - Product Serial Number: FGT30E3U16030794
- 4.6.1.9. Product Description: EAPR/CEPR - Product Serial Number: FGT30E3U16030810

- 4.6.1.10. Product Description: EARJ/CERJ - Product Serial Number: FGT30E3U16030819
- 4.6.1.11. Product Description: EAPA/CEPA - Product Serial Number: FGT30E3U16030841
- 4.6.1.12. Product Description: EAPR/CRPE - Product Serial Number: FGT30E5620012009
- 4.6.1.13. Product Description: Gerenciador - Product Serial Number: FMG-VM0A17002560
- 4.6.1.14. *A arquitetura tecnológica dos firewalls fortinet existente na Fundacentro, contempla um firewall principal (modelo 300D) - que será substituído por um equipamento 400E, 12 firewalls de escritórios remotos (modelo 30E) e o gerenciamento centralizados dos firewalls. São requisitos gerais da solução da Fundacentro, e suas características contemplam:*
- 4.6.1.15. Todos os equipamentos firewall e a solução de gerência integrada são do mesmo fabricante, inclusive os sistemas operacionais executados por esses equipamentos.
- 4.6.1.16. Capacidade de topologias de cluster redundante de alta disponibilidade (failover) nos modos ativo-ativo (mínimo para o firewall principal da Sede/CTN) e ativo-passivo (mínimo para os firewalls dos escritórios avançados), com sincronização, em tempo real, de configuração e de estados das conexões. No caso de falha de um dos equipamentos do cluster, não deverá haver perda das configurações e nem das conexões já estabelecidas e a transição entre os equipamentos deverá acontecer de forma transparente para o usuário.
- 4.6.1.17. Implementação tanto em modo transparente (camada 2) quanto em modo gateway (camada 3).
- 4.6.1.18. Controle de acesso por endereço IP de origem e destino, por aplicação (independentemente da porta ou protocolo utilizados pela aplicação), por sub-rede e por períodos do dia, permitindo a aplicação de regras por horários e por dias da semana.
- 4.6.1.19. Criação de serviços por porta ou conjunto de portas para, no mínimo, os protocolos TCP, UDP, ICMP e IP.
- 4.6.1.20. Tags de VLAN;
- 4.6.1.21. Criação de, no mínimo, 500 VLANs padrão 802.1q;
- 4.6.1.22. São capazes de aceitar comandos de scripts acionados por sistemas externos como, por exemplo, correlacionadores de eventos;
- 4.6.1.23. Bloqueio de tráfego em função da localização geográfica dos IPs de origem e de destino;
- 4.6.1.24. Agregação de links, segundo padrão IEEE 802.3ad;
- 4.6.1.25. Ferramenta de diagnóstico do tipo tcpdump;
- 4.6.1.26. Não possuem restrições ao número de máquinas ou usuários protegidos, salvo pela capacidade do equipamento.
- 4.6.1.27. Integração com serviços de diretório LDAP, Microsoft Active Directory, RADIUS e senha do sistema operacional no próprio firewall para identificação, autenticação e registros de logs, sem limite de número de usuários em relação ao licenciamento;
- 4.6.1.28. Identificar de forma transparente os usuários autenticados por single sign-on, inclusive por meio de serviço de diretório, compatível no mínimo com as seguintes ferramentas: Microsoft Active Directory, de servidores RADIUS Microsoft Network Policy Server e OpenLDAP.
- 4.6.1.29. Criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do Microsoft Active Directory;
- 4.6.1.30. Não se utilizam de agentes instalados nos servidores LDAP, Active Directory, RADIUS, Kerberos e proxies internos, e nem nos equipamentos dos usuários.
- 4.6.1.31. Registrar a identificação do usuário em todos os logs de eventos de acesso ou de ameaças gerados pelo equipamento.

- 4.6.1.32. Métodos de autenticação de usuários para aplicações executadas sobre os protocolos TCP e UDP como, por exemplo, aplicações HTTP, HTTPS, FTP;
- 4.6.1.33. Suportar Network Address Translation (NAT 1-1, NAT 1-N, NAT N-1) de acordo com a RFC3022, nos modo estático e dinâmico;
- 4.6.1.34. Funcionalidade de fazer tradução de endereços dinâmicos um-para-N, PAT (Port Address Translation);
- 4.6.1.35. Suportar nativamente IPv6;
- 4.6.1.36. Criar políticas IPv4 e IPv6 a partir da solução de gerência
- 4.6.1.37. Suportar os protocolos de roteamento dinâmico, bem como as funcionalidades de roteamento estático, inclusive IPv6;
- 4.6.1.38. Suportar os protocolos IGMP v2, IGMP v3;
- 4.6.1.39. Funcionalidades de DHC client, server e relay;
- 4.6.1.40. Proteção e suporte a protocolos de Real Time, contemplando no mínimo: Real Time Transport Protocol (RTP), RTCP, RTMP, RTSP, H323, SIP, tanto em IPv4 quanto em IPv6.
- 4.6.1.41. Tecnologia de firewall stateful;
- 4.6.1.42. Realização de backup e restore das regras, configurações e políticas, e a transferência desse backup para armazenamento em servidores externos;
- 4.6.1.43. Funcionalidade de detecção e bloqueio de, no mínimo, os seguintes tipos de ataques: IP Spoofing, SYN Flood, UDP Flood, Port Scanning, ICMP Flood, ICMP sweep, Ataques de Força Bruta ataques Man-in-the-Middle e variações de reflexão;
- 4.6.1.44. Sincronização de horário por NTP;
- 4.6.1.45. Funcionalidade de geração de relatórios e exportação de logs;
- 4.6.1.46. No mínimo, a operação em modo gateway e transparente;
- 4.6.1.47. Mínimo de 1.000 regras ou políticas de firewall;
- 4.6.1.48. Criar vários pacotes de políticas que serão aplicados/associados à dispositivos ou grupos de dispositivos
- 4.6.1.49. Abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
- 4.6.1.50. Mecanismo de anti-spoofing;
- 4.6.1.51. Funcionalidade de exceção em SSL Inspection para sites e aplicações bancárias, não decriptando o tráfego dessas conexões.
- 4.6.1.52. Inspeção profunda de pacotes para tráfego critpografado (no mínimo em tráfego VPN e HTTPS);
- 4.6.1.53. Suporte a SNMPv2 e v3;
- 4.6.1.54. MIB própria contemplando, no mínimo, indicadores de estado do hardware e de performance equipamento
- 4.6.1.55. Suporte a, no mínimo, dois algoritmos de balanceamento de carga para novas conexões de rede a servidores internos;
- 4.6.1.56. Conexão criptografada entre estação de gerência e o equipamento, tanto em interface gráfica quanto em interface por linha de comando;.
- 4.6.1.57. Criptografar e autenticar a comunicação com solução de gerenciamento centralizado.
- 4.6.1.58. Gerenciamento remoto do equipamento por meio da rede local ou WAN e pela solução de gerenciamento centralizado;

- 4.6.1.59. Gerenciamento gráfico centralizado das funcionalidades de firewall e monitoramento de seus eventos de forma integrada ao gerenciamento centralizado da solução. Deve também permitir o gerenciamento dos processos associados por meio de CLI (command-line interface);
- 4.6.1.60. Identificar os países de origem e destino de todas as conexões estabelecidas através do equipamento.
- 4.6.1.61. Criação de políticas de segurança baseadas em geolocalização, permitindo o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países.
- 4.6.1.62. A visualização dos países de origem e destino em relatórios ou logs de eventos de acessos e ameaças.
- 4.6.1.63. Funcionalidades de gerência local do firewall:
- a) Suportar, por meio da interface gráfica de gerenciamento, a criação e administração de políticas, filtragem de URLs, monitoração de logs e captura de pacotes, sem que a interface gráfica enseje custo adicional
 - b) Capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.
 - c) Delegação de funções de administração.
 - d) Registrar em log as ações dos usuários administradores.
 - e) Identificação e utilização de usuários nas políticas de segurança.
 - f) Agrupamento lógico de objetos ("object grouping") para criação de regras.
 - g) Contabilizar a utilização ("hit counts") ou o volume de dados trafegados correspondente a cada regra de filtragem individualmente.
 - h) Possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).
 - i) Capaz de testar a conectividade dos equipamentos gerenciados.
 - j) Funcionalidade para análise de regras com capacidade de detectar regras conflitantes ou regras equivalentes.
 - k) Suportar a geração de alertas automáticos via email, SNMP e syslog.
 - l) Exportação de logs via SCP ou FTP.
 - m) Monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.
- 4.6.1.64. Controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (shaping);
- 4.6.1.65. Gerenciamento gráfico unificado das funcionalidades de QoS/Traffic Shapping integrado com o gerenciamento centralizado da solução;
- 4.6.1.66. Criação de políticas controle uso largura de banda, limitando ou expandido individualmente, baseadas em: porta ou protocolo, endereço IP de origem ou destino, grupo de usuários do Microsoft Active Directory e LDAP e aplicações (por exemplo, Youtube e WhatsApp).
- 4.6.1.67. Criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory para a funcionalidade de controle de aplicações
- 4.6.1.68. As funcionalidades de VPN não possuem qualquer restrição de licenciamento, inclusive em relação ao número de clientes, IPs e máquinas.
- 4.6.1.69. Deve permitir a arquitetura de VPN hub and spoke IPSec, tanto para topologias site-to-site ("Full Meshed" e "Estrela") como para client-to-site (remote access);
- 4.6.1.70. Criação de túneis VPN SSL/TLS;
- 4.6.1.71. Criação de túneis VPN IPSec;

- 4.6.1.72. Suporte a VPNs IPSec site-to-site e client-to-site;
- 4.6.1.73. Suporte a NAT64 e NAT46;
- 4.6.1.74. Suporte nativo ao IPv6 e tráfego IPv6 tunelado em pacotes IPv4;
- 4.6.1.75. Suporte VPN em IPv6, assim como tunelar tráfego IPv4 dentro de túneis IPSec IPv6;
- 4.6.1.76. Permite que o usuário realize a conexão VPN SSL por meio de cliente instalado no sistema operacional do seu equipamento ou por meio de interface Web do tipo portal, devendo o cliente instalável estar disponível, no mínimo, para os sistemas operacionais Windows (Vista, 7, 8 e 10), Linux, Mac OS X e para os sistemas móveis Apple iOS e Google Android. O acesso por meio da interface Web deverá ser compatível com, no mínimo, os navegadores Internet Explorer 7 ou superior, Firefox 3.6 ou superior;
- 4.6.1.77. Customização da interface Web portal VPN SSL pelos administradores do sistema, incluindo quais aplicativos, servidores e sistemas estarão acessíveis via portal;
- 4.6.1.78. Algoritmos de criptografia para túneis VPN AES-128 e AES-256;
- 4.6.1.79. Algoritmos para definição de chave de cifração 3DES e AES;
- 4.6.1.80. Algoritmos RSA, Diffie-Hellman/RSA;
- 4.6.1.81. Certificado Digital X.509 v3;
- 4.6.1.82. Inclusão (enrollment) de autoridades certificadoras;
- 4.6.1.83. Alteração dos algoritmos criptográficos da VPNs permitindo a inserção de criptografia de estado.
- 4.6.1.84. IKE – Internet Key Exchange, fases I e II;
- 4.6.1.85. Roteamento para as funcionalidades de VPN;
- 4.6.1.86. Autenticação de usuários utilizando LDAP, Microsoft Active Directory, RADIUS e certificados digitais e suportar, no mínimo, autenticação two-way com certificado digital e LDAP ou Microsoft Active Directory ou RADIUS
- 4.6.1.87. Certificados emitidos por autoridade certificadora no padrão ICP-Brasil;
- 4.6.1.88. Leitura e verificação de Certificate Revocation List (CRL);
- 4.6.1.89. NAT Transversal Tunneling (NAT-T);
- 4.6.1.90. Gerenciamento gráfico centralizado das funcionalidades de VPN e monitoramento de seus eventos de forma integrada ao gerenciamento centralizado da solução. Deve também permitir o gerenciamento dos processos associados por meio de CLI (command-line interface);
- 4.6.1.91. VPN gateway-a-gateway deverá possuir interoperabilidade com os gateways de VPN pelo menos dos seguintes fabricantes: Cisco, Checkpoint, Juniper, Palo Alto Networks, Fortinet, AKER, BluePEX, PFSense, Sophos e SonicWall.
- 4.6.1.92. Aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.
- 4.6.1.93. Abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas.
- 4.6.1.94. Forwarding multicast na solução de segurança, inclusive em modo bridge
- 4.6.1.95. Criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação
- 4.6.1.96. Aplicações multimídia como: H.323, SIP.
- 4.6.1.97. Priorização de tráfego e suportar TOS
- 4.6.1.98. Solução de filtro de conteúdo web integrado a solução de segurança

4.6.1.99. Funcionamento em modo transparente tipo “bridge” sem alterar o endereço MAC do tráfego

4.6.1.100. Suporta PBR - Policy Based Routing na solução de segurança

4.6.2. *As licenças devem atender aos seguintes requisitos mínimos:*

4.6.2.1. Permitir número ilimitado de estações de rede e usuários

4.6.2.2. Conjunto de funcionalidades IPS/IDS

- a) Possuir tecnologia de detecção baseada em assinatura, atualizadas automaticamente
- b) Possuir no mínimo um conjunto de 2.000 assinaturas de detecção e prevenção de ataques, permitindo também ataques baseados em anomalias;
- c) Decodificar múltiplos formatos de Unicode;
- d) Deverá permitir a criação de padrões de ataque de IPS manualmente
- e) Suportar fragmentação e desfragmentação IP;
- f) Detectar protocolos independentemente da porta utilizada, identificando aplicações conhecidas em portas não-padrão;
- g) Detectar e Proteger contra, no mínimo, os ataques de RPC (Remote Procedure Call), Windows ou NetBios, SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol), DNS (Domain Name System), FTP, SSH, Telnet, ICMP (Internet Control Message Protocol), SIP, SNMP, SSDP, CHARGEN, RDP (Remote Desktop Protocol), DoS (Denial of Service) e ataques com assinaturas complexas, tais como ataques TCP hijacking.
- h) Possuir proteção contra ataques como, mas não restringindo-se aos mesmos : 1) Ataques de Worm, Trojan, Backdoors, Portscans, IP Spoofing, DoS, Spywares, Botnets e malwares em geral; 2) Ataques e utilização de tecnologia P2P; 3) Ataques de estouro de pilha (buffer overflow); 5) Tráfego mal formado; 6) Cabeçalhos inválidos de protocolo; 6) Ataques de injeção (SQL Injection, LDAP Injection) e de Cross-Site Scripting; 7) Elevação de privilégio e 8) Exploits - Web Server, Web Browser ActiveX, JavaScript, Browser Plug-ins/Add-nos.
- i) Emitir alarmes na console de administração integrada, alertas via correio eletrônico, syslog e traps SNMP;
- j) Permitir monitoração do comportamento do equipamento mediante o protocolo SNMP;
- k) Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
- l) Permitir filtros de anomalias de tráfego estatístico de flooding, scan e source session limits;
- m) Permitir filtros de anomalias de protocolos, inclusive protocolos de aplicação (ex.: HTTP, SMTP, NTP, NetBIOS, HTTPS, FTP, DNS, SMB, RPC, SSH e Telnet);
- n) Deve resistir a técnicas de evasão ou ataques direcionados ao próprio equipamento, no mínimo as técnicas: IP Packet Fragmentation, Stream Segmentation, RPC Fragmentation, URL Obfuscation, HTML Obfuscation, Payload Encoding, FTP Evasion e Layered Evasions.
- o) Possuir funcionalidade que permita desativar a análise de assinaturas e protocolos;
- p) Possuir funcionalidade que permita desativar a análise de ataques a partir de endereços/faixa IP específicos;
- q) Permitir o funcionamento mínimo do engine de IPS mesmo que a comunicação com o site do fabricante esteja fora de operação;

- r) Possuir as estratégias de bloqueio, liberar e bloquear, sendo este suportando quarentenar o IP, selecionáveis tanto por conjuntos de assinaturas quanto por cada assinatura;
- s) Suportar a verificação de ataques na camada de aplicação;
- t) Possuir gerenciamento gráfico centralizado das funcionalidades de IPS/IDS e monitoramento de seus eventos de forma integrada ao gerenciamento centralizado da solução. Deve também permitir o gerenciamento dos processos associados por meio de CLI (command-line interface);
- u) Reconhecer assinaturas seletivas e filtros de ataque que devem proteger contra ataques de negação de serviços automatizados, worms, vulnerabilidades conhecidas.
- v) Taxa mínima de detecção de 90% (noventa por cento), tendo no máximo 10% (dez por cento) de falso positivo.
- w) Deverá possuir categoria exclusiva, no mínimo, para os tipos de aplicações: P2P, Games, Web, Proxy, Audio/Video e VOIP
- x) Deverá possuir capacidade de agrupar assinaturas do IPS para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;
- y) Deverá permitir ao IPS funcionar em modo transparente, sniffer e router
- z) Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory para a funcionalidade de controle de aplicações

4.6.2.3. Conjunto de funcionalidades anti-virus e anti-malware

- a) Possuir módulo de proteção contra antivírus, anti-malware e anti-bot no mesmo equipamento do firewall;
- b) Possuir funcionalidade de varredura contra vírus e malwares em tráfego HTTPS, HTTP, FTP, POP3, IMAP e SMTP;
- c) Deve ser capaz de, se houver algum atraso ou falha na realização da atualização automática, o equipamento deve ter a capacidade de alertar imediatamente o administrador através de logs, SNMP e e-mail;
- d) Deve possuir serviço de atualização automática e manual de assinaturas com o fabricante;
- e) Suportar funcionamento mínimo da engine de antivírus e anti-malwares mesmo que a comunicação com o site do fabricante esteja fora de operação;
- f) Possuir gerenciamento gráfico centralizado das funcionalidades de antivírus e anti-malware integrado com gerenciamento centralizado da solução. Deve também permitir o gerenciamento dos processos associados por meio de CLI (command-line interface);
- g) Identificação, classificação e bloqueio de malwares, contemplando no mínimo, Trojan, Spywares, Backdoors, Worms, Vírus;
- h) Taxa mínima de detecção de 80% (oitenta), tendo no máximo 15% (quinze) de falso positivo.

4.6.2.4. Conjunto de funcionalidades para tratamento de conteúdo web

- a) Possuir base mínima contendo 50 (cinquenta) milhões de sites internet web já registrados e classificados, distribuídos em, no mínimo, 40 (quarenta) categorias ou subcategorias pré-definidas;
- b) Permitir a criação de categorias personalizadas;
- c) Permitir a categorização e reclassificação de sites web por URL e por endereço IP;

- d) Prover o funcionamento mínimo do engine de filtragem web mesmo que a comunicação com o site do fabricante esteja fora de operação;
- e) Suportar filtragem e categorização das URLs suportando alta disponibilidade nos servidores do fabricante.
- f) Possuir integração com serviços de diretório LDAP e Microsoft Active Directory para autenticação de usuários;
- g) Permitir a criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do Microsoft Active Directory;
- h) Permitir a criação de regras para acesso/bloqueio por endereço IP de origem e sub-rede de origem;
- i) Permitir a criação de quotas de utilização por categorias ou usuários;
- j) Capacidade de exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários, na tentativa de acesso a recursos proibidos ou restringidos pela política de segurança do órgão;
- k) Permitir o bloqueio de páginas web por meio da construção de filtros específicos com mecanismo de busca textual;
- l) Permitir o bloqueio de URLs inválidas cujo campo CN ou DN do certificado SSL não contém um domínio válido;
- m) Permitir o bloqueio de páginas web por classificação, como páginas que facilitam a busca de áudio, vídeo, imagem, URLs originadas de spam e sites de proxys anônimos;
- n) Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;
- o) Possuir categorização de sites governamentais nacionais, mesmo não tendo domínio “.gov.br.”
- p) Categorizar as URLs com taxa de acerto mínima de 85% (oitenta e cinco), tendo no máximo 20% de categorização como desconhecida.
- q) Suportar e forçar pesquisas seguras em sistemas de buscas, contemplando no mínimo, Google, Bing e Yahoo.
- r) Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX através de: base de URL própria atualizável.
- s) Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP, endereço IP e sub-rede para a funcionalidade de filtro de conteúdo web
- t) Permitir a re-classificação de sites web, tanto por URL quanto por endereço IP

4.6.2.5. Conjunto de funcionalidades para controle de aplicações e análise profunda

- a) Possuir módulo de filtro de aplicações e de conteúdo desenvolvido e mantido pelo próprio fabricante, no mesmo equipamento do firewall;
- b) Deve ser capaz de identificar se as aplicações estão utilizando sua porta default.
- c) Deve ser capaz de identificar aplicações encapsuladas dentro de protocolos como HTTP e HTTPS.
- d) Deve ser capaz de identificar aplicações criptografadas usando SSL.
- e) Permitir o agrupamento de aplicações em grupos personalizados;
- f) Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;

- g) Identificar aplicações e permitir ou bloquear sua utilização, independentemente das portas e protocolos utilizados para conexão (inclusive tráfego criptografado), assim como possuir categorias para classificação das aplicações, bem como das técnicas de evasões utilizadas;
- h) Possuir, no mínimo, proteção para aplicações do tipo P2P, Instant Messaging, Web e VOIP;
- i) Possuir política de segurança de aplicações pré-configuradas na solução;
- j) Possuir atualização manual e automática de novas assinaturas;
- k) Permitir a criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do Microsoft Active Directory;
- l) Deve ser capaz de identificar e filtrar um mínimo de 2000 (duas mil) aplicações, contemplando no mínimo: peer-to-peer, streaming e download de áudio, streaming e download de vídeo, update de software, instant messaging, redes sociais, proxies, anonymizers, acesso e controle remoto, VOIP e email.
- m) Identificação, bloqueio e restrição em profundidade e granularidade de aplicações, contemplando no mínimo: Bittorrent, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook, Facebook Messenger, Google+, Google Talk, Google Docs, Tinder, Instagram, Twitter, Twitcam, Tweetdeck, Linkedin, Dropbox, Google Drive, Skydrive, One Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR, Webex e Telegram .
- n) Categorizar as aplicações com taxa de acerto mínima de 85% (oitenta e cinco), tendo no máximo 30% (trinta) de categorização como desconhecida.

4.6.3. *Adicionalmente aos requisitos anteriores, a solução de gerenciamento centralizado de firewalls deverá suportar, no mínimo:*

4.6.3.1. A solução gerenciável opera externamente ao equipamento principal, em um appliance virtual específico.

- a) Quando executado em ambientes virtuais, deverão ser fornecidas e implantadas, em caráter perpétuo, todas as licenças dos softwares e sistemas operacionais necessários ao funcionamento da solução.

4.6.3.2. Licenciada e permitir a gerência centralizada de todos os equipamentos e contextos virtuais que compõem a solução de alta disponibilidade.

4.6.3.3. Licenciada sem limitar número de usuários, objetos, regras de segurança, NAT e endereços IP.

4.6.3.4. Licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõe a solução de alta disponibilidade.

4.6.3.5. Deve permitir a criação e distribuição de políticas de segurança e de objetos de rede de forma centralizada.

4.6.3.6. Deve permitir a criação de relatórios customizados.

4.6.3.7. Deve possibilitar a filtragem dos logs do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário.

4.6.3.8. Deve possuir relatórios com informações consolidadas sobre: as mais frequentes fontes de conexões bloqueadas com seus destinos e serviços, os mais frequentes ataques e ameaças de segurança detectados com suas origens e destinos, os serviços de rede mais utilizados, as aplicações maiores consumidoras de banda de Internet, os usuários maiores consumidores de banda de Internet, os sítios na Internet mais visitados.

4.6.3.9. Deve permitir a geração automática e agendada dos relatórios.

4.6.3.10. Deve automatizar o sincronismo de regras, objetos e políticas em tempo real.

- 4.6.3.11. Deverá utilizar comunicação segura criptografada entre a solução de gerência e os equipamentos gerenciados.
- 4.6.3.12. Deverá manter o histórico de configurações enviadas aos equipamentos e deverá permitir o rollback das configurações.
- 4.6.3.13. Deve permitir distribuição centralizada de pacotes de atualização.
- 4.6.3.14. Deve permitir validar as regras antes de aplicá-las.
- 4.6.3.15. Possuir capacidade mínima para armazenamento de logs de 100GB.
- 4.6.3.16. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada
- 4.6.3.17. Permitir criar regras anti DoS de forma centralizada
- 4.6.3.18. A gerência deve suportar log remoto no formato syslog
- 4.6.3.19. Permitir criar, a partir da solução de gerência, VPNs entre os dispositivos gerenciados de forma centralizada, incluindo topologia (hub, spoke, dial-up), autenticações, chaves e métodos de criptografia
- 4.6.3.20. Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como licenças, horário do sistema e firmware.
- 4.6.3.21. A solução de gerência deve ser capaz de receber logs de vários dispositivos simultaneamente a, no mínimo, uma taxa de 1GB por dia.
- 4.6.3.22. Atender o disposto nas alíneas g), j), k), m) do item 4.6.2.49 e do item 4.6.2.45 de qualquer firewall gerenciado
- 4.6.3.23. Deve informar a utilização dos recursos de CPU, memória, armazenamento interno e atividade de rede dos equipamentos gerenciados.
- 4.6.3.24. Deve informar o número de conexões simultâneas e de novas conexões por segundo dos equipamentos gerenciados.
- 4.6.3.25. Deve possuir visualização mínima sumarizada de: aplicações, ameaças, URLs, endereços de origem, endereços de destino, levando-se em conta o quantitativo de sessões, de consumo de banda e categorização.
- 4.6.3.26. Deve possuir notificação via e-mail de eventos de gerência
- 4.6.4. *O equipamento principal (firewall da Sede/CTN) deverá ter as seguintes funcionalidades mínimas referentes ao hardware (item 1 da Tabela 1):*
 - 4.6.4.1. Possuir todas as funcionalidades descritas nos itens anteriores referentes aos requisitos de arquitetura tecnológica.
 - 4.6.4.2. Possuir no mínimo o throughput de 1 Gbps para todas as funcionalidades ligadas simultaneamente com inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo.
 - 4.6.4.3. O equipamento deve possuir no mínimo 01 (uma) fonte pode ser interna ou externa de alimentação, com alimentação nominal de 100~120VAC e 210~230VAC e frequência de 50 ou 60 Hz com chaveamento automático (bivolt automático). Deverá vir acompanhado de cabo de alimentação com, no mínimo, 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136.
 - 4.6.4.4. Possuir disco rígido com capacidade mínima de 100 GB SSD para armazenamento de logs.
 - 4.6.4.5. Conexões simultâneas, mínimo: 10.000.00
 - 4.6.4.6. Novas conexões por segundo: 150.000
 - 4.6.4.7. Quantidade mínima de túneis LAN to LAN: 500
 - 4.6.4.8. Quantidade mínima de túneis client to lan: 1.000
 - 4.6.4.9. Quantidade mínima de usuários VPN SSL licenciados: 250

- 4.6.4.10. Quantidade mínima de Access Points Gerenciados: 128
- 4.6.4.11. Possuir, no mínimo, 8 (oito) portas 1000 BASE T, podendo 4 portas serem SFP
- 4.6.4.12. O equipamento e seus componentes deverão ser novos, sem uso, ou reconicionados, entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais e acompanhados de todos os acessórios, cabos, conectores, kits de fixação, trilhos, fibras óticas (incluindo sua fusão, se necessário), patchcords, miniGbics, etc, necessários às suas instalações e operação em rack de 19" padrão EIA-310.
- 4.6.4.13. Não será aceito equipamento em modo End of Life, End of Support ou End-of-Sale durante a vigência do contrato, estas informações deverão estar no site do fabricante e fornecidas pelo licitante.
- 4.6.5. *O equipamento principal (firewall da Sede/CTN) deverá ter as seguintes funcionalidades mínimas referentes ao software (item 2 da Tabela 1):*
- 4.6.5.1. O equipamento objeto do item 1 deve ser do mesmo fabricante da solução gerenciada (item 3) e dos firewalls remotos (das Unidades Descentralizadas) da Fundacentro (licenças objeto do item 2). Isso é necessário para que se mantenha a estrutura de segurança lógica em operação, sem gerar custo adicional para aquisição de novos hardwares nas UD's, uma vez que apenas o firewall principal está próximo de seu end-of-life, requerendo assim, substituição.
- 4.6.5.2. O equipamento deverá atualizar firmware e softwares para novas versões durante 48 (quarenta e oito) meses, estas informações deverão estar no site do fabricante.
- 4.6.5.3. Todas as licenças de hardware e software devem ser fornecidas em caráter perpétuo, atualizadas em suas últimas versões disponíveis, não sendo permitida a cobrança de quaisquer valores adicionais pelo uso dos hardwares e softwares durante o contrato ou após o seu término.
- 4.6.5.4. As licenças de atualização de software (firmware ou drivers) e licenças de atualização de assinaturas deverão ser fornecidas pelo prazo mínimo de 48 (quarenta e oito) meses, a contar da data do recebimento definitivo dos produtos, sem ônus adicional para as atualizações e seu uso.
- 4.6.5.5. Todos os equipamentos devem ter alimentação nominal de 100~120VAC e 210~230VAC e frequência de 50 ou 60 Hz com chaveamento automático (bivolt automático). Deverá vir acompanhado de cabo de alimentação com, no mínimo, 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136. A fonte fornecida deve suportar sozinha a operação da unidade com todos os módulos de interface ativos
- 4.6.5.6. O equipamento deve possuir 1 (uma) porta de console para configuração e gerenciamento por interface de linha de comando (CLI).
- 4.6.5.7. O equipamento deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação, inclusive com seus respectivos transceivers instalados, sem custos adicionais.
- 4.6.5.8. Fornecido em hardware dedicado tipo appliance ou chassi, com sistema operacional otimizado, do mesmo fabricante, para o uso como firewall multifunção.
- a) Os equipamentos da solução ofertada, não deverão exceder 4 Unit Rack individualmente, sendo "caixas" únicas, ou seja, sem empilhamentos.
- b) O equipamento do item 1 deve ser ofertado para conexão em rack 19".
- 4.6.5.9. Deve possuir fonte(s) de energia no próprio equipamento para o item 1.
- 4.6.5.10. Suportar topologias de cluster redundante de alta disponibilidade (failover) nos modos ativo-ativo e ativo-passivo, com sincronização, em tempo real, de configuração e de estados das conexões. No caso de falha de um dos equipamentos do cluster, não deverá haver perda das configurações e nem das conexões já estabelecidas e a transição entre os equipamentos deverá acontecer de forma transparente para o usuário.
- 4.6.5.11. Deve suportar a implementação tanto em modo transparente (camada 2) quanto em modo gateway (camada 3).

- 4.6.5.12. Possuir controle de acesso por endereço IP de origem e destino, por aplicação (independentemente da porta ou protocolo utilizados pela aplicação), por sub-rede e por períodos do dia, permitindo a aplicação de regras por horários e por dias da semana.
- 4.6.5.13. Permitir criação de serviços por porta ou conjunto de portas para, no mínimo, os protocolos TCP, UDP, ICMP e IP.
- 4.6.5.14. Suportar tags de VLAN;
- 4.6.5.15. Permitir a criação de, no mínimo, 500 VLANs padrão 802.1q;
- 4.6.5.16. Ser capaz de aceitar comandos de scripts acionados por sistemas externos como, por exemplo, correlacionadores de eventos;
- 4.6.5.17. Suportar o bloqueio de tráfego em função da localização geográfica dos IPs de origem e de destino;
- 4.6.5.18. Suportar agregação de links, segundo padrão IEEE 802.3ad;
- 4.6.5.19. Possuir ferramenta de diagnóstico do tipo tcpdump;
- 4.6.5.20. Não deve possuir restrições ao número de máquinas ou usuários protegidos, salvo pela capacidade do equipamento.
- 4.6.5.21. Suportar integração com serviços de diretório LDAP, Microsoft Active Directory, RADIUS e senha do sistema operacional no próprio firewall para identificação, autenticação e registros de logs, sem limite de número de usuários em relação ao licenciamento;
- 4.6.5.22. Deve identificar de forma transparente os usuários autenticados por single sign-on, inclusive por meio de serviço de diretório, compatível no mínimo com as seguintes ferramentas: Microsoft Active Directory, de servidores RADIUS Microsoft Network Policy Server e OpenLDAP.
- 4.6.5.23. Permitir a criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do Microsoft Active Directory;
- 4.6.5.24. Não será permitida a utilização de agentes instalados nos servidores LDAP, Active Directory, RADIUS, Kerberos e proxies internos, e nem nos equipamentos dos usuários.
- 4.6.5.25. Deve registrar a identificação do usuário em todos os logs de eventos de acesso ou de ameaças gerados pelo equipamento.
- 4.6.5.26. Possuir métodos de autenticação de usuários para aplicações executadas sobre os protocolos TCP e UDP como, por exemplo, aplicações HTTP, HTTPS, FTP;
- 4.6.5.27. Suportar Network Address Translation (NAT 1-1, NAT 1-N, NAT N-1) de acordo com a RFC3022, nos modo estático e dinâmico;
- 4.6.5.28. Possuir a funcionalidade de fazer tradução de endereços dinâmicos um-para-N, PAT (Port Address Translation);
- 4.6.5.29. Suportar nativamente IPv6;
- 4.6.5.30. Permitir criar políticas IPv4 e IPv6 a partir da solução de gerência
- 4.6.5.31. Suportar, no mínimo, os protocolos de roteamento dinâmico, bem como as funcionalidades de roteamento estático, inclusive IPv6;
- 4.6.5.32. Suportar os protocolos IGMP v2, IGMP v3;
- 4.6.5.33. Possuir funcionalidades de DHC client, server e relay;
- 4.6.5.34. Possuir proteção e suporte a protocolos de Real Time, contemplando no mínimo: Real Time Transport Protocol (RTP), RTCP, RTMP, RTSP, H323, SIP, tanto em IPv4 quanto em IPv6.
- 4.6.5.35. Possuir tecnologia de firewall stateful;
- 4.6.5.36. Permitir a realização de backup e restore das regras, configurações e políticas, e a transferência desse backup para armazenamento em servidores externos;

- 4.6.5.37. Possuir funcionalidade de detecção e bloqueio de, no mínimo, os seguintes tipos de ataques: IP Spoofing, SYN Flood, UDP Flood, Port Scanning, ICMP Flood, ICMP sweep, Ataques de Força Bruta ataques Man-in-the-Middle e variações de reflexão;
- 4.6.5.38. Suportar sincronização de horário por NTP;
- 4.6.5.39. Possuir funcionalidade de geração de relatórios e exportação de logs;
- 4.6.5.40. Deve suportar, no mínimo, a operação em modo gateway e transparente;
- 4.6.5.41. Suportar, no mínimo, 1.000 regras ou políticas de firewall;
- 4.6.5.42. Permitir criar vários pacotes de políticas que serão aplicados/associados à dispositivos ou grupos de dispositivos
- 4.6.5.43. Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
- 4.6.5.44. Possuir mecanismo de anti-spoofing;
- 4.6.5.45. Possuir funcionalidade de exceção em SSL Inspection para sites e aplicações bancárias, não decriptando o tráfego dessas conexões.
- 4.6.5.46. Possuir inspeção profunda de pacotes para tráfego criptografado (no mínimo em tráfego VPN e HTTPS);
- 4.6.5.47. Possuir, no mínimo, suporte a SNMPv2 e v3;
- 4.6.5.48. Deve possuir MIB própria contemplando, no mínimo, indicadores de estado do hardware e de performance equipamento;
- 4.6.5.49. Possuir suporte a, no mínimo, dois algoritmos de balanceamento de carga para novas conexões de rede a servidores internos;
- 4.6.5.50. Possuir conexão criptografada entre estação de gerência e o equipamento, tanto em interface gráfica quanto em interface por linha de comando;.
- 4.6.5.51. Deve criptografar e autenticar a comunicação com solução de gerenciamento centralizado.
- 4.6.5.52. Permitir o gerenciamento remoto do equipamento por meio da rede local ou WAN e pela solução de gerenciamento centralizado;
- 4.6.5.53. Possuir gerenciamento gráfico centralizado das funcionalidades de firewall e monitoramento de seus eventos de forma integrada ao gerenciamento centralizado da solução. Deve também permitir o gerenciamento dos processos associados por meio de CLI (command-line interface);
- 4.6.5.54. Deve identificar os países de origem e destino de todas as conexões estabelecidas através do equipamento.
- 4.6.5.55. Deve permitir a criação de políticas de segurança baseadas em geolocalização, permitindo o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países.
- 4.6.5.56. Deve possibilitar a visualização dos países de origem e destino em relatórios ou logs de eventos de acessos e ameaças.
- 4.6.5.57. Funcionalidades de gerência local do firewall:
 - a) Deve suportar, por meio da interface gráfica de gerenciamento, a criação e administração de políticas, filtragem de URLs, monitoração de logs e captura de pacotes, sem que a interface gráfica enseje custo adicional
 - b) Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.
 - c) Deve permitir a delegação de funções de administração.
 - d) Deve registrar em log as ações dos usuários administradores.
 - e) Deve suportar a identificação e utilização de usuários nas políticas de segurança.

- f) Deve suportar agrupamento lógico de objetos ("object grouping") para criação de regras.
- g) Deve contabilizar a utilização ("hit counts") ou o volume de dados trafegados correspondente a cada regra de filtragem individualmente.
- h) Deve possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).
- i) Deve ser capaz de testar a conectividade dos equipamentos gerenciados.
- j) Deve prover funcionalidade para análise de regras com capacidade de detectar regras conflitantes ou regras equivalentes.
- k) Deve suportar a geração de alertas automáticos via email, SNMP e syslog.
- l) Deve permitir a exportação de logs via SCP ou FTP.
- m) Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários.

4.6.5.58. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (shaping);

4.6.5.59. Deve possuir gerenciamento gráfico unificado das funcionalidades de QoS/Traffic Shapping integrado com o gerenciamento centralizado da solução;

4.6.5.60. Deve suportar a criação de políticas controle uso largura de banda, limitando ou expandido individualmente, baseadas em: porta ou protocolo, endereço IP de origem ou destino, grupo de usuários do Microsoft Active Directory e LDAP e aplicações (por exemplo, Youtube e WhatsApp).

4.6.5.61. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory para a funcionalidade de controle de aplicações

4.6.5.62. As funcionalidades de VPN não podem possuir qualquer restrição de licenciamento, inclusive em relação ao número de clientes, IPs e máquinas.

4.6.5.63. Deve permitir a arquitetura de VPN hub and spoke IPSec, tanto para topologias site-to-site ("Full Meshed" e "Estrela") como para client-to-site (remote access);

4.6.5.64. Deve permitir a criação de túneis VPN SSL/TLS;

4.6.5.65. Deve permitir a criação de túneis VPN IPSec;

4.6.5.66. Possuir suporte a VPNs IPSec site-to-site e client-to-site;

4.6.5.67. Deve suportar NAT64 e NAT46;

4.6.5.68. Suportar nativamente IPv6 e tráfego IPv6 tunelado em pacotes IPv4;

4.6.5.69. Deve suportar VPN em IPv6, assim como tunelar tráfego IPv4 dentro de túneis IPSec IPv6;

4.6.5.70. Deve permitir que o usuário realize a conexão VPN SSL por meio de cliente instalado no sistema operacional do seu equipamento ou por meio de interface Web do tipo portal, devendo o cliente instalável estar disponível, no mínimo, para os sistemas operacionais Windows 10 e superiores, Linux, Mac OS, e para os sistemas móveis Apple iOS e Google Android. O acesso por meio da interface Web deverá ser compatível com, no mínimo, os navegadores Chrome ou Firefox em suas versões mais recentes;

4.6.5.71. Deve suportar a customização da interface Web portal VPN SSL pelos administradores do sistema, incluindo quais aplicativos, servidores e sistemas estarão acessíveis via portal;

4.6.5.72. Suportar algoritmos de criptografia para túneis VPN AES-128 e AES-256;

4.6.5.73. Suportar os algoritmos para definição de chave de cifração 3DES e AES;

4.6.5.74. Suportar os algoritmos RSA, Diffie-Hellman/RSA;

- 4.6.5.75. Suportar Certificado Digital X.509 v3;
- 4.6.5.76. Suportar a inclusão (enrollment) de autoridades certificadoras;
- 4.6.5.77. Permitir alteração dos algoritmos criptográficos da VPNs permitindo a inserção de criptografia de estado.
- 4.6.5.78. Suportar IKE – Internet Key Exchange, fases I e II;
- 4.6.5.79. Suportar roteamento para as funcionalidades de VPN;
- 4.6.5.80. Implementar autenticação de usuários utilizando LDAP, Microsoft Active Directory, RADIUS e certificados digitais e suportar, no mínimo, autenticação two-way com certificado digital e LDAP ou Microsoft Active Directory ou RADIUS
- 4.6.5.81. Suportar certificados emitidos por autoridade certificadora no padrão ICP-Brasil;
- 4.6.5.82. Suportar leitura e verificação de Certificate Revocation List (CRL);
- 4.6.5.83. Suportar NAT Transversal Tunneling (NAT-T);
- 4.6.5.84. Possuir gerenciamento gráfico centralizado das funcionalidades de VPN e monitoramento de seus eventos de forma integrada ao gerenciamento centralizado da solução. Deve também permitir o gerenciamento dos processos associados por meio de CLI (command-line interface);
- 4.6.5.85. VPN gateway-a-gateway deverá possuir interoperabilidade com os gateways de VPN pelo menos dos seguintes fabricantes: Cisco, Checkpoint, Juniper, Palo Alto Networks, Fortinet, AKER, BluePEX, PFSense, Sophos e SonicWall.
- 4.6.5.86. Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.
- 4.6.5.87. O equipamento deve ser apropriado para o uso em ambiente tropical com umidade relativa na faixa de 10 a 90% (sem condensação) e temperatura ambiente na faixa de 0 a 40°C.
- 4.6.5.88. Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas.
- 4.6.5.89. Suportar forwarding multicast na solução de segurança, inclusive em modo bridge
- 4.6.5.90. Permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, tipo de dispositivo, horário, protocolo e aplicação
- 4.6.5.91. Suportar aplicações multimídia como: H.323, SIP.
- 4.6.5.92. Permitir priorização de tráfego e suportar TOS
- 4.6.5.93. Possuir solução de filtro de conteúdo web integrado a solução de segurança
- 4.6.5.94. A solução de segurança deve permitir o funcionamento em modo transparente tipo “bridge” sem alterar o endereço MAC do tráfego
- 4.6.5.95. A solução de segurança deve estar licenciada para permitir número ilimitado de estações de rede e usuários
- 4.6.5.96. Deve suportar PBR - Policy Based Routing na solução de segurança

4.7. ***Requisitos de Projeto e Implantação***

- 4.7.1. A implantação do hardware será presencial, enquanto a implantação das licenças poderá ser remota ou presencial, de acordo com o definido na reunião inicial, bem como deve seguir as datas definidas pela FUNDACENTRO.

4.7.1.1. **Da instalação**

- a) Fica a critério da CONTRATANTE, definir o horário de instalação e configuração dos equipamentos e softwares, podendo tais procedimentos serem executados em feriados ou finais de semana e em horário noturno, conforme as necessidades da CONTRATANTE.

- b) A CONTRATADA deverá fornecer todos os materiais necessários à instalação física completa, à configuração e ao perfeito funcionamento da totalidade dos itens adquiridos.
- c) Constatada a ocorrência de divergência na especificação técnica ou falhas de atualização, defeitos de fabricação ou qualquer outro defeito apresentado durante a instalação dos equipamentos, fica a CONTRATADA obrigada a providenciar a instalação da licença e operacionalização do equipamento, inclusive com o fornecimento de equipamento sobressalente caso o equipamento que estava sob atualização fique paralisado por mais de 48 (quarenta e oito) horas, sujeitando-se a CONTRATADA às penalidades previstas na legislação vigente e neste T.R.
- d) Eventuais despesas de custeio com deslocamento de técnicos da CONTRATADA ao local de instalação, bem como todas as despesas de transporte, diárias, seguro ou quaisquer outros custos envolvidos ficam a cargo exclusivo da CONTRATADA.
- e) A CONTRATADA deverá comunicar a CONTRATANTE a conclusão da instalação dos equipamentos e entregar toda documentação técnica prevista, dentro dos prazos definidos neste T.R.
- f) A CONTRATADA deverá entregar o Projeto Definitivo de Instalação (PDI) no prazo máximo de 60 (sessenta) dias corridos, que por sua vez deve contemplar todas as informações referentes à conclusão dos serviços.
- g) A CONTRATADA entregará toda a documentação de instalação, a qual deverá prover nível de informação suficiente para que um técnico (externo) possa entender e refazer, caso necessário, as instalações e configurações dos equipamentos adquiridos e implantados.
- h) Após a CONTRATADA concluir toda a instalação dos equipamentos, deixando-os completamente operacionais, e a entrega de toda documentação técnica e do PDI, conforme condições e prazos exigidos neste termo de referência, a CONTRATANTE emitirá o Termo de Recebimento Provisório, contados a partir da comunicação de conclusão da instalação.

4.7.1.2. Escopo do Serviço de Instalação

- a) Fornecimento de todos os serviços necessários ao planejamento e a execução da instalação, incluindo projetos, configuração dos equipamentos de acordo com as necessidades da CONTRATANTE definidas neste T.R.
- b) A CONTRATADA deverá executar todas as atividades (físicas e lógicas) de migração dos serviços que se encontrem em operação, incluindo a elaboração do De/Para de portas e a configuração dos equipamentos. A CONTRATANTE deverá disponibilizar a topologia de rede existente para que estas atividades sejam efetuadas.
- c) A CONTRATADA, no caso de algum incidente que comprometa os serviços, deverá retornar toda solução conforme estado imediatamente anterior ao processo de instalação. Isso inclui fallback tanto de eventuais configurações alteradas (lógicas), bem como também do respectivo cabeamento (físico).
- d) Para garantir esse perfeito funcionamento e a transição das mudanças, a CONTRATADA deverá disponibilizar um técnico qualificado, com as respectivas ferramentas necessárias, para solucionar problemas oriundos da instalação ou restabelecer a rede original em até 2 (duas) horas. Caso não seja obedecido o prazo anterior, a CONTRATADA estará sujeita as penalidades previstas neste T.R.
- e) A CONTRATADA deverá ainda, independentemente de outras atividades necessárias para garantir a disponibilidade total dos serviços, executar:

- Todos os backups necessários e relacionados à atividade em questão dos equipamentos (firewalls) em produção;

- Todos os testes, antes e após as atividades de intervenção e/ou instalação, dos serviços em funcionamento no órgão que tenham relação com os equipamentos em questão.

f) A CONTRATADA deverá fornecer à equipe de gestão da implantação da FUNDACENTRO os nomes dos técnicos, juntamente com os respectivos números de documento de identidade, para que sejam identificados durante o procedimento de instalação.

g) Somente será considerada a instalação concluída quando os equipamentos estiverem operacionais, em plenas condições de funcionamento, integrado com a rede local e com capacidade de permitir acesso remoto por parte da equipe da CONTRATANTE.

h) Cabe à CONTRATADA realizar a instalação dos firmwares necessários para o funcionamento e a operação completa dos equipamentos, sendo obrigatória a inclusão no equipamento, no momento da instalação, da versão estável mais atual de todos os firmwares.

i) Todos os softwares necessários à operação dos equipamentos e soluções devem, igualmente, ser entregues instalados e operacionais. Também devem estar incluídos e licenciados (se for o caso) todos os componentes de software básico necessários ao funcionamento dos equipamentos, tais como: sistemas operacionais, controladores de dispositivos e outros pertinentes.

4.7.1.3. Documentação técnica

a) A documentação técnica de instalação deverá conter, no mínimo:

- Descrição dos recursos de hardware e software utilizados nos equipamentos.
- Lista de todos os elementos instalados contendo: nome e endereço IP do equipamento, juntamente com todas as interconexões físicas (equipamento/porta origem e equipamento/porta destino), local de instalação (prédio, andar, sala), número de série, número do bem utilizado pelo CONTRATANTE, data da instalação, data de aquisição, data de vencimento da garantia.
- Listagem das configurações dos equipamentos com comentários sobre os principais comandos e as justificativas das opções de parametrização.
- Com relação às configurações dos equipamentos, a CONTRATADA deverá implementar todas as funcionalidades requisitadas pela CONTRATANTE, estando essas minimamente restritas aos requisitos constantes na especificação técnica. Nas implementações dos ativos a serem instalados que dependam de integração com os demais elementos da rede, a CONTRATANTE será responsável por disponibilizar as informações à CONTRATADA, necessárias à harmonização desses novos ativos com os equipamentos preexistentes na rede local da CONTRATANTE.
- Configuração dos equipamentos segundo as especificações da CONTRATANTE, o que pode incluir, por exemplo, ativação de mecanismos avançados de segurança de rede local e integração com serviços de diretório para autenticação de usuários.

b) Toda documentação exigida neste Termo de Referência deverá ser entregue em mídia eletrônica.

c) A documentação técnica deverá garantir a transferência de conhecimento à CONTRATANTE, a fim de proporcionar o nível de informação necessário à operação da rede e possíveis intervenções.

4.8. *Requisitos de Garantia e Manutenção*

4.8.1. As licenças e a garantia dos equipamentos deverão ser válidas por 48 meses, com o prazo iniciando a contar a partir da emissão do Termo de Recebimento Definitivo (TRD) emitido pela Fiscalização do Contrato.

4.8.2. As licenças contratadas obrigatoriamente implicam na extensão da garantia de hardware do equipamento durante o período de validade da licença. Dessa maneira, defeitos de hardware também estarão cobertos pela garantia e seguem o disposto nos itens a seguir.

4.8.3. Durante o período de garantia, a CONTRATADA deverá estar apta a atender chamados encaminhados pela CONTRATANTE ao Centro de Atendimento da CONTRATADA, sem ônus adicional para a CONTRATANTE, oferecendo, no mínimo, os seguintes serviços:

4.8.3.1. Deve ser possível tanto acionamento via número 0800, quanto via Web, disponível 8 (oito) horas por dia, 5 (cinco) dias por semana, para solução de problemas decorrentes de defeitos e falhas nos produtos ou equipamento/software, ou seja, problemas decorrentes do fato do ativo de rede não realizar uma funcionalidade especificada ou esperada. Poderá ainda, esse serviço, ser usado para solicitar informações quanto às dúvidas, funcionalidades e quanto a procedimentos para configuração dos itens do objeto contratado.

4.8.3.2. Todos os custos decorrentes da retirada de equipamentos ou componentes para a prestação do serviço de garantia serão de responsabilidade da CONTRATADA, bem como seu retorno aos locais onde serão instalados os equipamentos pela empresa contratada.

4.8.4. No atendimento dos chamados, caso a CONTRATADA não consiga resolver o problema por meio da assistência remota, deverá a CONTRATADA realizar uma ação On-Site (no local onde está o ativo de rede) para sanar o problema e restabelecer o funcionamento normal do equipamento, obedecendo os critérios dos níveis mínimos de serviço exigidos deste TR, responsabilizando-se pelas despesas de deslocamento de seu técnico/especialista.

4.8.5. Em qualquer caso, a CONTRATADA deverá arcar com todos os procedimentos necessários à solução do problema, incluindo a substituição de quaisquer módulos defeituosos no(s) equipamento(s), bem como a substituição do(s) próprio(s) equipamentos(s), se for necessário, devendo ser atendida as seguintes condições:

4.8.5.1. Os chamados serão registrados e informados à CONTRATANTE, nos prazos estabelecidos no nível mínimo de serviço exigido deste TR, e deverão estar disponíveis, via sistema web, para acompanhamento pela equipe designada pela CONTRATANTE, contendo data e hora do chamado, o problema ocorrido, a solução, data e hora de conclusão.

4.8.5.2. Decorrido os prazos previstos no Acordo de Níveis Mínimos de Serviço, sem o atendimento devido, fica a CONTRATANTE autorizada a penalizar a CONTRATADA dentro dos parâmetros explicitados neste Termo de Referência, respeitado o direito ao contraditório e ampla defesa.

4.8.5.3. A CONTRATADA deverá encaminhar ao fiscal técnico do contrato, até o 5º dia útil de cada mês em que houver chamados, um Relatório de Acompanhamento de Nível Mínimo de Serviço, com informações de TODOS chamados abertos pela CONTRATANTE, em sua central de atendimento, contendo, pelo menos, as seguintes informações:

- a) Data, hora da abertura do chamado;
- b) Número de série do equipamento alvo do atendimento;
- c) Data e hora da chegada do técnico ao local;
- d) Data e hora da resolução do problema;
- e) Descrição do problema, incidente ou solicitação atendida e Procedimentos efetuados.
- f) Ateste(s) de atendimento e solução do(s) problema(s)

4.8.6. Garantia dos equipamentos e serviços – disposições gerais

4.8.6.1. A CONTRATADA deverá garantir a completa interoperabilidade e compatibilidade entre os Firewalls a serem adquiridos no presente Termo de Referência e os ativos já em funcionamento na CONTRATANTE. Não podendo se escusar de suas responsabilidades quanto à prestação da solução técnica para possíveis falhas ou inconsistências, bem como o auxílio técnico necessários à interoperação da rede, a fim de garantir o perfeito funcionamento dos ativos adquiridos com os demais ativos com os quais deverão interoperar.

4.8.6.2. Sendo a CONTRATADA designada para realizar a instalação dos Firewalls, será de sua responsabilidade a correção das falhas decorrentes de erros durante as atividades de instalação, sejam operacionais ou por problemas de mau funcionamento, responsabilizando-se por todos os custos envolvidos na correção dos desvios, sejam de interoperabilidade, incompatibilidade ou quaisquer outras falhas que impeçam a instalação ou o perfeito funcionamento dos Firewalls adquiridos.

4.8.6.3. A CONTRATADA deverá garantir o pleno funcionamento dos Firewalls, prestando o serviço de garantia remoto e on-site (quando, a critério da CONTRATANTE, for necessário), por um período de 48 (quarenta e oito) meses, contados a partir da data de emissão do Termo de Recebimento Definitivo.

4.8.6.4. A CONTRATADA deve garantir o funcionamento dos equipamentos, considerados isoladamente ou interligados aos demais, de acordo com as características descritas nos manuais e nas especificações aplicáveis, desde que o restante dos equipamentos de rede da CONTRATANTE esteja em condições normais de operação.

4.8.6.5. Para a referida garantia, serão considerados os eventos descritos conforme o nível mínimo de serviço exigido deste TR, devendo ser considerado para o enquadramento o grau de impacto para o serviço ou cliente afetado.

4.8.6.6. A CONTRATADA, no caso da atualização de equipamento para corrigir falhas apresentadas, deve se responsabilizar pelos custos envolvidos, inclusive eventuais trocas de hardware.

4.8.7. Garantia de hardware

4.8.7.1. A troca de qualquer unidade defeituosa deverá ser realizada em conformidade com os prazos estabelecidos no nível mínimo de serviço exigido deste TR.

4.8.7.2. A CONTRATADA deve garantir que os equipamentos fornecidos são apropriados para suportar as condições climáticas, conforme características exigidas nas especificações técnicas.

4.8.8. Garantia de software

4.8.8.1. A CONTRATADA deve disponibilizar, sem quaisquer custos adicionais à CONTRATANTE, a atualização de novas versões dos software(s) e firmware(s) fornecido(s), ou de parte(s) dele(s), decorrentes da evolução funcional ou correções do(s) anteriormente fornecido(s), durante o prazo da garantia da solução integrada de segurança.

4.8.8.2. Cabe à CONTRATADA informar, por intermédio de documento ou mensagem eletrônica, a disponibilidade de novas versões e atualizações, assim como quanto aos respectivos procedimentos de instalação. Por nova versão, entende-se por aquele que, mesmo sendo comercializado com novo nome, número de versão ou marca, retenha as funcionalidades exigidas na presente especificação técnica.

4.8.8.3. A CONTRATANTE reserva-se o direito de aceitar ou não atualizações no software ou parte dele.

4.8.8.4. A CONTRATADA deve garantir que uma nova versão do software ou firmware mantenha a compatibilidade e contenha todas as funções das versões anteriores e que a introdução desta não prejudique a interoperabilidade da mesma na rede.

4.8.8.5. A CONTRATADA deve garantir a independência entre a correção de defeitos (patches) e a geração de novas versões do software, sem ônus adicional à CONTRATANTE, em função da necessidade de atualização de componente para suportar nova versão do software.

4.8.8.6. A CONTRATADA deverá garantir o correto funcionamento de todo software instalado nos equipamentos durante o período de validade das licenças, a contar da data do Termo de Recebimento Definitivo.

4.8.8.7. Durante todo o período de garantia, a CONTRATADA obriga-se a substituir, recuperar e/ou modificar os softwares e firmwares instalados, sem ônus de qualquer natureza à CONTRATANTE, nos casos comprovados de mau funcionamento e de outras falhas, de modo a ajustá-los aos resultados que atendam às especificações técnicas solicitadas para o equipamento.

4.9. ***Requisitos de Experiência Profissional***

4.9.1. Os profissionais da contratada que atuarão na prestação dos serviços deverão ser especializados na solução de firewall especificada neste Termo de Referência.

4.10. ***Requisitos de Formação da Equipe***

4.10.1. Não se aplica.

4.11. ***Requisitos de Metodologia de Trabalho***

4.11.1. Considerando o escopo da contratação, todas as Notas Fiscais/Faturas de prestação de serviços deverão ser encaminhadas para o Fiscal Técnico do Contrato.

4.11.2. Não serão aceitos o recebimento de Notas Fiscais/Faturas por meios distintos, devendo a Contratada encaminhar todas as faturas usando o Sistema Eletrônico de Informações (SEI) da FUNDACENTRO ou, na indisponibilidade desse recurso, email designado pelo Fiscal Técnico, considerando que todas as Notas Fiscais/Faturas deverão ser encaminhadas pelo meio definido pela FUNDACENTRO. O não atendimento do exposto no item imediatamente anterior sujeitará a Contratada às sanções previstas.

4.11.3. No caso de envio via e-mail, a confirmação do recebimento do e-mail pelo Fiscal Técnico é de responsabilidade da Contratada e os prazos somente passarão a iniciar após a confirmação do recebimento pelo Fiscal Técnico.

4.11.4. Após o recebimento da prévia do faturamento, o Fiscal Técnico do Contrato emitirá o Termo de Recebimento Provisório (TRP), para que a Contratada possa emitir as Notas Fiscais de prestação dos serviços. A Contratada somente poderá emitir as Notas Fiscais após o recebimento do TRP e caso o Fiscal Técnico do Contrato encontre divergências na prévia de faturamento, deverá ocorrer o registro nas ocorrências contratuais

4.12. ***Requisitos de Segurança da Informação e Privacidade***

4.12.1. A contratada não poderá se utilizar da presente contratação para obter qualquer acesso não autorizado às informações da FUNDACENTRO.

4.12.2. É de responsabilidade da contratada garantir que as informações por ela obtidas em decorrência da execução desta contratação sejam mantidas em sigilo, não podendo ser divulgadas, exceto se previamente acordado, por escrito, entre as partes contratantes.

4.13. ***Outros Requisitos Aplicáveis***

4.13.1. A CONTRATADA deve executar o objeto do certame em estreita observância dos ditames estabelecido pela Lei 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)). Para a habilitação, o licitante deverá apresentar Declaração indicando o encarregado da credenciada responsável pela proteção de dados, nos termos do art. 41 da Lei Federal 13.709/18.

5. **RESPONSABILIDADES**

5.1. ***Deveres e responsabilidades da Contratante***

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

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

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

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

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

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

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

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

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

5.2. ***Deveres e responsabilidades da Contratada***

5.2.1. Indicar formalmente e por escrito, no prazo máximo de 5 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 dos serviços 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; e

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, o código-fonte de aplicações, 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;

6. **MODELO DE EXECUÇÃO DO CONTRATO**

6.1. ***Rotinas de Execução***

6.1.1. A reunião inicial poderá ser por videoconferência, em até 05 (cinco) dias após assinatura do Contrato Administrativo. O agendamento será de responsabilidade da CTIC;

6.1.2. Nesta reunião, será obrigatório, no mínimo, participação do Preposto da empresa contratada, Diretor de Tecnologia e o Representante da Área Requisitante, onde serão tratados os seguintes assuntos:

- a) Apresentação da equipe de fiscalização;
- b) Repasse de e-mails e nº de telefones da equipe de fiscalização para fins de comunicação;
- c) Apresentação do preposto da empresa pelo representante legal da contratada, além do descrito no item acima;
- d) Entrega, por parte da contratada, do Termo de Sigilo e Confidencialidade e dos Termos de Ciência;
- e) Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;
- f) Definir o cronograma de implantação de acordo com as exigências e prazos exigidos neste Termo de Referência.

6.1.3. O repasse à contratada de conhecimentos necessários à execução dos serviços ou ao fornecimento de bens:

- a) Descrição dos equipamentos;
- b) Locais de instalação dos equipamentos;

6.1.4. Transferência de conhecimento:

- a) A Contratada deverá seguir o disposto neste TR para que todos os conhecimentos sejam repassados para os servidores da CTIC;
- b) Os procedimentos devem ser documentados de forma a permitir compreensão por ente externo ao Contrato, no caso de transferência de conhecimento para a Fundacentro.

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

6.2.1. Devem ser fornecidas todas as licenças previstas na Contratação.

6.3. ***Mecanismos formais de comunicação***

6.3.1. Ata de reunião: Apresentação, contextualização, definição de atividades, metas e objetivos, identificação de riscos e problemas.

6.3.2. Ordem de Fornecimento de Bens: Solicitação formal da entrega dos bens.

6.3.3. Abertura de Chamado: Comunicação formal de ocorrência visando a correção de problemas detectados.

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

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

6.4.2. O Termo de Compromisso de Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, e Termo de Ciência, a ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação, encontram-se nos ANEXOS IV e V respectivamente.

7. **MODELO DE GESTÃO DO CONTRATO**

7.1. ***Critérios de Aceitação***

7.1.1. Todo o trabalho realizado pela contratada estará sujeito a avaliação técnica, sendo homologado quando estiver de acordo com o padrão de qualidade exigido pela FUNDACENTRO, mediante Termo de Aceite Provisório e, posteriormente, o Termo de Recebimento Definitivo.

7.1.2. Serão utilizados como critérios de aceitação:

- a) Os Níveis de Serviço apurados.
- b) A conformidade contratual.

7.1.3. A apuração dos níveis de serviço não considerará os períodos de indisponibilidades justificadas, que podem decorrer de:

- a) Períodos de interrupção previamente acordados.
- b) Interrupção de serviços públicos essenciais à plena execução das atividades (exemplo: suprimento de energia elétrica).
- c) Motivos de força maior.

7.1.4. O Termo de Recebimento Provisório será emitido após a entrega dos serviços e respectiva documentação para verificação de qualidade, atestes e faturamento.

7.1.5. A emissão do Termo de Recebimento Definitivo, que deflagrará o início da prestação de serviços está condicionada à apresentação do Preposto anteriormente indicado.

7.2. **Procedimentos de Teste e Inspeção**

7.2.1. A equipe técnica da FUNDACENTRO irá monitorar periodicamente a disponibilidade e versionamento das licenças. Estes dados serão base para aferir níveis de serviço e sugerir, quando cabíveis, a aplicação de glosas e sanções.

7.2.2. Dentre os procedimentos de testes e inspeções, ressaltam-se os seguintes:

- 7.2.2.1. Verificação da integridade de comunicação dos firewalls com redes externas;
- 7.2.2.2. Verificação da integridade de comunicação entre os firewalls;
- 7.2.2.3. Verificação da aplicação de políticas usando o sistema de gerenciamento centralizado;
- 7.2.2.4. Verificação da notificação quando da aplicação de políticas individuais nos equipamentos, alertando da divergência em relação à política do sistema de gerenciamento centralizado.

7.3. **Níveis Mínimo de Serviço Exigidos**

7.3.1. Os Níveis Mínimos de Serviço Exigidos são indicadores mensuráveis estabelecidos pelo órgão/entidade para aferir objetivamente os resultados pretendidos com a contratação.

7.3.2. O Indicador a seguir tem como objetivo aferir se houve atraso na entrega das licenças.

IAE – INDICADOR DE ATRASO DE ENTREGA DE OS	
Tópico	Descrição
Finalidade	Medir o tempo de atraso na entrega dos produtos e serviços constantes na Ordem de Fornecimento de Bens.
Meta a cumprir	IAE < = 0 A meta definida visa garantir a entrega dos produtos e serviços constantes na Ordem de Fornecimento de Bens dentro do prazo previsto.
Instrumento de medição	Através das ferramentas disponíveis para a gestão de demandas, por controle próprio da Contratante e lista de Termos de Recebimento Provisório e Definitivo emitidos.
Forma de acompanhamento	A avaliação será feita conforme linha de base do cronograma registrada na OS. Será subtraída a data de entrega dos produtos da OS (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data de início da execução da OS.

Periodicidade	Para cada Ordem de Fornecimento de Bens encerrada e com Termo de Recebimento Definitivo.
Mecanismo de Cálculo (métrica)	<p>IAE = <u>TEX – TEST</u> TEST</p> <p>Onde: IAE – Indicador de Atraso de Entrega da OS; TEX – Tempo de Execução – corresponde ao período de execução da OS, da sua data de início até a data de entrega dos produtos da OS. A data de início será aquela constante na OS; caso não esteja explícita, será o primeiro dia útil após a emissão da OS. A data de entrega da OS deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes no Termo de Referência. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução da OS continua a correr, findando-se apenas quanto a Contratada entrega os produtos da OS e haja aceitação por parte do fiscal técnico. TEST – Tempo Estimado para a execução da OS – constante na OS, conforme estipulado no Termo de Referência.</p>
Observações	<p>Obs1: Serão utilizados dias úteis na medição.</p> <p>Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias úteis no cômputo do indicador.</p> <p>Obs3: Não se aplicará este indicador para as OS de Manutenções Corretivas do tipo Garantia e aquelas com execução interrompida ou cancelada por solicitação da Contratante.</p>
Início de Vigência	A partir da emissão da OS.
Faixas de ajuste no pagamento e Sanções	<p>Para valores do indicador IAE:</p> <p>De 0 a 0,10 – Pagamento integral da OS; De 0,11 a 0,20 – Glosa de 0,5% sobre o valor da OS; De 0,21 a 0,30 – Glosa de 0,75% sobre o valor da OS; De 0,31 a 0,50 – Glosa de 1% sobre o valor da OS; De 0,51 a 1,00 – Glosa de 1,25% sobre o valor da OS; Acima de 1 – Será aplicada Glosa de 1,5% sobre o valor da OS e multa de 2% sobre o valor do Contrato.</p>

7.3.3. Os níveis mínimos de serviço esperados para essa contratação referentes ao atendimento de chamados técnicos, bem como para os atendimentos aos eventos associados estão indicados na Tabela 5, obedecendo também:

7.3.3.1. A classificação da severidade do evento será determinada pela CONTRATANTE

7.3.3.2. Todos os prazos especificados são contados a partir da abertura do respectivo número de identificação do chamado

7.3.3.3. A abertura do chamado deve fornecer um número de identificação (protocolo de atendimento) fornecido pela CONTRATADA.

7.3.3.4. O atendimento aos chamados pode ocorrer remotamente (preferencialmente), ou de forma presencial.

7.3.3.5. Um chamado classificado de acordo com essas severidades não pode ser reclassificado a medida que é resolvido em outra. A severidade deve levar em conta o fator que foi usado na sua abertura e seguir esse mesmo critério até a sua completa solução.

Tabela 5 - Prazos de atendimento

Equipamentos	Localidades	Severidade	Medidas para o Indicador
Todos	São Paulo	Crítica	4 horas
		Normal	8 horas
		Baixa	24 horas
	Demais localidades	Crítica	8 horas
		Normal	16 horas
		Baixa	36 horas

Tabela 6 - Classificação de severidade de Incidentes

Crítica	São consideradas como “crítica” todas as falhas cujas consequências tenham impactos negativos, gerando indisponibilidade sobre o serviço e o tráfego e/ou recursos. São situações que exijam atenção imediata. Ex: Situação de indisponibilidade total do equipamento, funcionamento intermitente ou parcial do equipamento, que possa levar à interrupção intermitente, parcial ou total de serviços ou perda de tráfego
Normal	Problemas que não prejudicam significativamente o funcionamento dos sistemas/serviços do equipamento. São problemas sérios ou perturbações, que afetam uma área específica ou determinada funcionalidade do equipamento. Ex: reinicialização de módulos, slots ou portas com defeitos, degradação de desempenho, perda de funcionalidades
Baixa	Solicitação de informações sobre o funcionamento dos equipamentos, possíveis configurações ou usos, que não gerem interrupções, nem indisponibilidade de determinada área ou uma funcionalidade específica

7.3.3.6. O descumprimento total ou parcial das obrigações assumidas pela CONTRATADA, referente ao não atendimento aos Níveis Mínimos de Serviço da Tabela 5, resguardados os procedimentos legais pertinentes, sem prejuízo nas demais sanções cabíveis, poderá acarretar as seguintes penalidades de acordo com a Tabela 7 a seguir.

Tabela 7 - Classificação de severidade de Incidentes

Severidade	Descrição	Penalidade
Crítica	Até 8 horas úteis de atraso, além do prazo indicado na Tabela 5	1) Advertência
	Superior a 8 horas úteis e inferior ou igual a 16 horas úteis de atraso, além do prazo indicado na Tabela 5	2) Fator de Ajuste de Pagamento (FAP) 01 - Multa de 0,2% (zero vírgula dois por cento) calculada sobre o valor da licença do equipamento, sem prejuízo ao item anterior
	Superior a 16 horas úteis, além do prazo indicado na Tabela 5	3) FAP 02 - Multa de 0,4% (zero vírgula quatro por cento) por hora de atraso, calculada sobre o valor da licença do equipamento, sem prejuízo ao item anterior, e outras sanções administrativas previstas
Normal	Até 16 horas úteis de atraso, além do prazo indicado na Tabela 5	4) Advertência
	Superior a 16 horas úteis e inferior ou igual a 24 horas úteis de atraso,	5) FAP 03 - Multa de 0,1% (zero vírgula um por cento) por hora de atraso, calculada sobre o valor da licença do equipamento, sem prejuízo ao item anterior

	além do prazo indicado na Tabela 5	
	Superior a 24 horas úteis, além do prazo indicado na Tabela 5	6) FAP 04 - Multa de 0,2% (zero vírgula dois por cento) por hora de atraso, calculada sobre o valor da licença do equipamento, sem prejuízo ao item anterior, e outras sanções administrativas previstas
Baixa	Até 48 horas úteis de atraso, além do prazo indicado na Tabela 5	7) Advertência; 8) FAP 05 - Multa de 0,05% (zero vírgula zero cinco por cento) por hora de atraso, calculada sobre o valor da licença do equipamento, sem prejuízo ao item anterior, e outras sanções administrativas previstas

7.4. ***Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento***

7.4.1. Comete infração administrativa nos termos da Lei nº 8.666, de 1993 e da Lei nº 10.520, de 2002, a CONTRATADA que:

- a) inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;
- b) ensejar o retardamento da execução do objeto;
- c) falhar ou fraudar na execução do contrato;
- d) comportar-se de modo inidôneo; ou
- e) cometer fraude fiscal.

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

7.4.2.1. Advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado e sempre que no mês de referência a porcentagem de tempo de atividade mensal não atingir 99,9% será feita advertência por escrito à contratada, após comunicado o Gestor do Contrato;

7.4.2.2. Multa:

- a) 0,1% (um décimo por cento) até 0,2% (dois décimos por cento) por dia sobre o valor adjudicado em caso de atraso na execução dos serviços, limitada a incidência a 15 (quinze) dias. Após o décimo quinto dia e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;
- b) 0,1% (um décimo por cento) até 10% (dez por cento) sobre o valor adjudicado, em caso de atraso na execução do objeto, por período superior ao previsto no subitem acima, ou de inexecução parcial da obrigação assumida;
- c) 0,1% (um décimo por cento) até 15% (quinze por cento) sobre o valor adjudicado, em caso de inexecução total da obrigação assumida;
- d) 0,2% a 3,2% por dia sobre o valor mensal do contrato, conforme detalhamento constante das duas tabelas a seguir; e
- e) 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autorizará a Administração CONTRATANTE a promover a rescisão do contrato;

f) As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

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

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

7.4.2.5. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados.

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

7.4.2.7. Para efeito de aplicação de multas, às infrações são atribuídos graus, de acordo com as tabelas a seguir:

Tabela 8 - Sanções

Id	Ocorrência	Glosa / Sanção
1	Não comparecer injustificadamente à Reunião Inicial.	Advertência. Em caso de reincidência, 0,5% sobre o valor total do Contrato.
2	Quando convocado dentro do prazo de validade da sua proposta, não celebrar o Contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não manter a proposta, falhar ou fraudar na execução do Contrato, comportar-se de modo inidôneo ou cometer fraude fiscal.	A Contratada ficará impedida de licitar e contratar com a União, Estados, Distrito Federal e Municípios e, será descredenciada no SICAF, ou nos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4º da Lei nº 10.520/2002, pelo prazo de até 5 (cinco) anos, sem prejuízo das demais cominações legais, e multa de 1% do valor da contratação.
3	Ter praticado atos ilícitos visando frustrar os objetivos da licitação.	A Contratada será declarada inidônea para licitar e contratar com a Administração.
4	Demonstrar não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
5	Não executar total ou parcialmente os serviços previstos no objeto da contratação.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
6	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por até de 30 dias, sem comunicação formal ao gestor do Contrato.	Multa de 5% sobre o valor total do Contrato. Em caso de reincidência, configura-se inexecução total do Contrato por parte da empresa, ensejando a rescisão contratual unilateral.
7	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços solicitados, por mais de 30 (trinta) dias, sem comunicação formal ao gestor do contrato.	Contratada será declarada inidônea para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
8	Não prestar os esclarecimentos imediatamente, referente à execução dos serviços, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 48 horas úteis.	Multa de 0,1% sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela Contratante, até o limite de 30 dias úteis.
		Após o limite de 5 dias úteis, aplicar-se-á multa de 1% do valor total do Contrato.
9	Provocar intencionalmente a indisponibilidade da prestação dos serviços quanto aos componentes de	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial

	software (sistemas, portais, funcionalidades, banco de dados, programas, relatórios, consultas, etc).	do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
10	Permitir intencionalmente o funcionamento dos sistemas de modo adverso ao especificado na fase de levantamento de requisitos e às cláusulas contratuais, provocando prejuízo aos usuários dos serviços.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
11	Comprometer intencionalmente a integridade, disponibilidade ou confiabilidade e autenticidade das bases de dados dos sistemas.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
12	Comprometer intencionalmente o sigilo das informações armazenadas nos sistemas da contratante.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, sem prejuízo às penalidades decorrentes da inexecução total ou parcial do contrato, o que poderá acarretar a rescisão do Contrato, sem prejuízo das demais penalidades previstas na Lei nº 8.666, de 1993.
13	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 5% do valor total do Contrato.

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

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

7.4.3.2. Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

7.4.3.3. Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

7.4.4. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999

7.4.5. As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

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

7.4.7. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

7.4.8. Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização - PAR.

7.4.9. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto

de 2013, seguirão seu rito normal na unidade administrativa.

7.4.10. O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

7.4.11. As penalidades serão obrigatoriamente registradas no SICAF.

7.4.12. As reincidências de glosas, por três meses consecutivos, da prestação de serviços com um conjunto de indicadores de nível de serviço e desempenho inferiores aos níveis mínimos requeridos poderão ser qualificadas como descumprimento das obrigações contratuais, podendo ensejar à Contratada a respectiva sanção.

7.5. **Do Pagamento**

7.5.1. Para aceite do recebimento provisório e posterior encaminhamento ao pagamento, deverão ser apresentados os seguintes documentos em formato eletrônico para o Fiscal Técnico do Contrato:

7.5.1.1. Relatório contendo o atendimento das licenças em relação à arquitetura tecnológica prevista neste TR.

7.5.1.2. Relatório contendo o atendimento das licenças em relação à execução do objeto, conforme item 6 deste TR.

7.5.1.3. Prévia da Nota Fiscal/Fatura dos Serviços prestados;

7.5.1.4. A regularidade fiscal e trabalhista da contratada;

7.5.2. O CTIC analisará a documentação e emitirá o Termo de Recebimento Provisório. Eventuais erros no fornecimento da documentação relativa à prestação do serviço (e respectivo faturamento) por parte da contratada ensejará a suspensão do processo de pagamento até que todos os vícios documentais sejam sanados. Nestes casos, a CONTRATADA, sob nenhuma hipótese, poderá responsabilizar a CONTRATANTE por retenção dos pagamentos, tampouco abrirá margem para cobrança de qualquer tipo de juros ou taxa de mora. Ainda, caberão à CONTRATADA eventual multa de mora, em decorrência de descumprimento contratual.

7.5.3. O pagamento será efetuado pela Contratante no prazo de 30 dias, contados do recebimento da Nota Fiscal/Fatura.

7.5.4. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

7.5.5. A emissão da Nota Fiscal/Fatura será precedida do recebimento provisório do serviço, conforme este Termo de Referência

7.5.6. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

7.5.7. Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no do art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.

7.5.8. O setor competente para proceder o pagamento deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

7.5.8.1. o prazo de validade;

7.5.8.2. a data da emissão;

7.5.8.3. os dados do contrato e do órgão contratante;

- 7.5.8.4. o período de prestação dos serviços;
- 7.5.8.5. o valor a pagar; e
- 7.5.8.6. eventual destaque do valor de retenções tributárias cabíveis.
- 7.5.9. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante;
- 7.5.10. Nos termos do item 1, do Anexo VIII-A da Instrução Normativa SEGES/MP nº 05, de 2017, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:
- 7.5.10.1. não produziu os resultados acordados;
- 7.5.10.2. deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;
- 7.5.10.3. deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.
- 7.5.11. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
- 7.5.12. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.
- 7.5.13. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.
- 7.5.14. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.
- 7.5.15. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.
- 7.5.16. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.
- 7.5.17. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.
- 7.5.18. Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.
- 7.5.19. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, em especial a prevista no artigo 31 da Lei 8.212, de 1993, nos termos do item 6 do Anexo XI da IN SEGES/MP n. 5/2017, quando couber.
- 7.5.20. É vedado o pagamento, a qualquer título, por serviços prestados, à empresa privada que tenha em seu quadro societário servidor público da ativa do órgão contratante, com fundamento na Lei de Diretrizes Orçamentárias vigente.

7.5.21. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela é calculada mediante a aplicação da seguinte fórmula:

$EM = I \times N \times VP$, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

$I = (TX) \quad I =$	$\frac{(6 / 100)}{365}$	$I = 0,00016438$ TX = Percentual da taxa anual = 6%
----------------------	-------------------------	--

8. ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

8.1. O valor estimado da presente contratação, conforme levantamento realizado seguindo o disposto no ETP nº 30/2021 consta na tabela a seguir.

Tabela 9 - Valores estimados para a contratação

Lote	Item	Descrição	Qtd.	Unidade de medida	Valor unitário estimado para 48 meses	Valor total estimado para 48 meses
1	1	Equipamento firewall principal para a Sede/CTN (FortiGate-400E – FG-400E – HW)	1	unidade	133.149,48	133.149,48
	2	Licença de firewall principal FortiGate-400E Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web Filtering, Antispam Service, and 24x7 Fortinet) válida por 48 meses	1	licença para uso de software	436.826,24	436.826,24
	3	Licença de firewall de escritório remoto para as UD's (FTNT-RENEW - RENEW - 48 M – Fortigate 30E) válida por 48 meses	12	licença para uso de software	23.981,31	287.775,72
	4	Licença de gerenciador de firewall (FortiManager) válida por 48 meses	1	licença para uso de software	104.575,56	104.575,56
Total estimado para 48 meses						962.327,00

8.2. A apresentação das propostas deverá seguir o modelo apresentado no Anexo II - Modelo para apresentação de propostas.

9. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

9.1. As despesas decorrentes com a referida aquisição correrão à conta da Dotação Orçamentária da União de acordo com subitens a seguir.

9.1.1. Despesas referentes ao item 1:

9.1.1.1. Gestão/Unidade: 264001

9.1.1.2. Ação: Administrativa

9.1.1.3. Fonte: 0100000000

9.1.1.4. Programa de Trabalho: 204577

9.1.1.5. Elemento de Despesa: 44905237

9.1.1.6. PI: 22000401113

9.1.2. Despesas referentes aos itens 2, 3 e 4:

9.1.2.1. Gestão/Unidade: 264001

9.1.2.2. Ação: Administrativa

9.1.2.3. Fonte: 0100000000

9.1.2.4. Programa de Trabalho: 204577

9.1.2.5. Elemento de Despesa: 33904006

9.1.2.6. PI: 22000401113

9.2. O cronograma físico-financeiro compreende o início dos faturamentos somente após a instalação realizada e validada pela CTIC, conforme os "Requisitos de Implantação", "Modelo de Execução do Contrato" e "Modelo de Gestão do Contrato", que estabelecem os prazos e requisitos a serem cumpridos previamente à execução da despesa mensal.

9.3. O relatório conclusivo do ETP nº 30/2021, demonstrou que as licenças com vigência de 48 (quarenta e oito) meses se mostram vantajosas ao interesse público, visto que resultará em economia significativa de recursos para a Administração. Pelo exposto, com fundamentação no art. 40, inciso XIV, alínea d, da Lei 8.666/1993, no parecer nº 00254/2020/CONJUR-MS/CGU/AGU e no item 6 do Parecer nº 00012/2020/CNMLC/CGU/AGU e, considerando que há previsão de prestação de garantia pela contratada, nos termos do Art. 56 da Lei nº 8.666/93, é justificável o licenciamento por 48 (quarenta e oito meses). O pagamento se dará uma única vez e corresponderá ao fornecimento das licenças (e seus respectivos serviços delineados neste Termo de Referência) durante todo o período de vigência do contrato.

9.4. Fica a Contratada obrigada a devolver a integralidade do valor antecipado na hipótese de inexecução do objeto atualizado monetariamente pela variação acumulada do Índice Nacional de Preços ao Consumidor Amplo (IPCA), ou índice que venha a substituí-lo, desde a data do pagamento da antecipação até a data da devolução, conforme determina a alínea d do Item XIV, do Art. 40 da Lei 8666/93.

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

9.5. Todos os atos decorrentes da aplicação do pagamento de que trata esta cláusula serão disponibilizados em sítio oficial da internet, observados, no que couber, os requisitos previstos no § 3º do art. 8º da Lei nº 12.527, de 18 de novembro de 2011, com o nome do contratado, o número de sua inscrição na Secretaria Especial da Receita Federal do Brasil, o prazo contratual, o valor e o respectivo processo de aquisição ou contratação.

9.6. Além disso, as licenças são aplicadas nos equipamentos e, uma vez ativadas, devem operar pelos 48 (quarenta e oito) meses. O histórico da Fundacentro dá subsídio, pois no Contrato anterior, as licenças dos equipamentos foram utilizadas por 48 (quarenta e oito meses), demonstrando a continuidade do uso as licenças e dos serviços atrelados a elas.

10. DA SUBCONTRATAÇÃO

10.1. Não será admitida a subcontratação do objeto licitatório.

11. ALTERAÇÃO SUBJETIVA

11.1. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

12. GARANTIA DA EXECUÇÃO

12.1. A Contratada apresentará, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do Contratante, contado da assinatura do contrato, comprovante de prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária, em valor correspondente a 5 % (cinco por cento) do valor total do contrato, com validade durante a execução do contrato e 90 (noventa) dias após término da vigência contratual, devendo ser renovada a cada prorrogação.

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

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

12.2. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

12.2.1. prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

12.2.2. prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;

12.2.3. multas moratórias e punitivas aplicadas pela Administração à contratada; e

12.2.4. obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela contratada, quando couber.

12.3. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item anterior, observada a legislação que rege a matéria.

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

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

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

12.7. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

12.8. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a Contratada obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificada.

12.9. A Contratante executará a garantia na forma prevista na legislação que rege a matéria.

12.10. Será considerada extinta a garantia:

12.10.1. com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Contratante, mediante termo circunstanciado, de que a Contratada cumpriu todas as cláusulas do contrato;

12.10.2. no prazo de 90 (noventa) dias após o término da vigência do contrato, caso a Administração não comunique a ocorrência de sinistros, quando o prazo será ampliado, nos termos da comunicação, conforme estabelecido na alínea "h2" do item 3.1 do Anexo VII-F da IN SEGES/MP n. 05/2017.

12.11. O garantidor não é parte para figurar em processo administrativo instaurado pela contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.

12.12. A contratada autoriza a contratante a reter, a qualquer tempo, a garantia, na forma prevista no neste Edital e no Contrato.

13. DA VIGÊNCIA DO CONTRATO

13.1. O contrato vigorará por 48 (quarenta e oito) meses, contados a partir da data da sua assinatura, não podendo ser prorrogado.

13.2. Para a vigência proposta, também se considera:

13.2.1. As licenças utilizadas serem de uso contínuo: Os equipamentos utilizados (firewalls) são patrimônio da Fundacentro e as licenças são obrigatórias para que os equipamentos desempenhem sua função, qual seja, a proteção de perímetro dos servidores de aplicação, desktops, notebooks e demais equipamentos conectados à rede de dados da Sede/CTN e das UD's. A não utilização de licenças implica na nulidade de função dos dispositivos e implica diretamente na disponibilidade dos serviços tecnológicos prestados pela Fundacentro para a sociedade. Além disso, sem as licenças, os equipamentos e tudo o que eles protegem ficam expostos e vulneráveis às constantes ameaças existentes na internet. Isso comprova que as licenças são essenciais e de uso contínuo para que os equipamentos desempenhem suas funções.

13.2.2. Além disso, há a diminuição do risco de interrupção da prestação dos serviços: Um maior período de vigência contratual confere maior segurança para a Fundacentro pois esse serviço de uso de licença de software é contínuo, reduzindo os riscos inerentes quando ocorre uma nova contratação e novas implantações nesses equipamentos:

a) Necessidade de paralisação dos equipamentos para aplicação das licenças em um período de 48 meses requer menos tempo de indisponibilidade da rede;

13.2.3. Portanto, sempre que há uma nova contratação eleva-se o risco de interrupção dos serviços prestados, prejudicando os trabalhos administrativos e finalísticos da FUNDACENTRO.

13.3. Aliado aos fatos anteriormente mencionados, vale ressaltar que as licenças do fabricante são precificadas em moeda estrangeira (dólar). A Fundacentro conta com experiência em outro processo (SEI ID [47648.000411/2021-96](#)) referente ao reajuste de preços de peças/partes de equipamento que tem parte de suas peças cujos valores são cotados em moeda estrangeira ou que contém matérias-primas que tiveram altíssima variação de preços (acima do IPCA, por exemplo). Nesse caso extremo, uma vigência de 12 meses na contratação pretendida neste Termo de Referência, e a fixação do IPCA como índice de reajuste, frustraria a renovação do contrato, pois uma variação da moeda estrangeira acima do IPCA seria um impeditivo para a renovação das licenças (e a não renovação do contrato poderia expor o perímetro de rede da Fundacentro às ameaças externas, pois seria necessária nova contratação em tempo não hábil). Por último e muito importante, ressalta-se que a estimativa de custo apresentada no ETP nº 30/2021 aponta que adquirir as licenças por 48 meses apresenta melhores preços do que adquirir por 12 meses e renovar as licenças desses equipamentos de uso continuado a cada 12 meses. Por isso evidencia-se a vantajosidade econômica da aquisição das licenças por 48 (quarenta e oito) meses.

14. DO REAJUSTE DE PREÇOS

14.1. Os preços são fixos e irreajustáveis.

15. DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

15.1. Regime, Tipo e Modalidade da Licitação

15.1.1. O regime da execução dos contratos é de EMPREITADA POR PREÇO GLOBAL.

15.1.2. O tipo e critério de julgamento da licitação é o MENOR PREÇO POR GRUPO para a seleção da proposta mais vantajosa.

15.1.3. De acordo com o §1º do Art. 1º do Decreto nº 10.024, de 20 de setembro de 2019, esta licitação deve ser realizada na modalidade de PREGÃO NA FORMA ELETRÔNICA.

15.1.4. O Modo de Disputa será ABERTO E FECHADO.

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

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

15.2.1. Foi definida a não aplicação do direito de preferência e margens de preferência estabelecidos na Lei Complementar n.º 123/2006 sob o preconizado no Art. 48 Inciso II da mesma lei. Especificamente, o objeto contratado trata de serviço cuja denominação genérica trata de cessão temporária de direitos sobre programas de computador locação de software.

15.2.2. Ressalta-se que o Inciso I do Art 8º do Decreto nº 7.174, de 12 de Maio de 2010, que regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo poder Público e pelas demais organizações sob o controle direto ou indireto da União, aponta que as regras de preferência a serem aplicadas são as dispostas no Capítulo V da Lei Complementar nº 123, de 2006.

15.3. Critérios de Qualificação Técnica para a Habilitação

15.3.1. Comprovação de aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, mediante a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado.

15.3.1.1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a serviços executados com as seguintes características mínimas:

a) No mínimo 01 (um) atestado(s) ou declaração(ões) de capacidade técnica, em nome da licitante, expedido por pessoa jurídica de direito público ou privado, que comprove a aptidão para o fornecimento de licença de firewall principal (modelo fortinet 300D ou similar).

b) No mínimo 01 (um) atestado(s) ou declaração(ões) de capacidade técnica, em nome da licitante, expedido por pessoa jurídica de direito público ou privado, que comprove a aptidão para o fornecimento de licença de firewall de escritório remoto (modelo fortinet 30E ou similar).

c) No mínimo 01 (um) atestado(s) ou declaração(ões) de capacidade técnica, em nome da licitante, expedido por pessoa jurídica de direito público ou privado, que comprove a aptidão para a prestação de serviços de aplicação de atualização e administração de firewalls central e de escritório remoto.

15.3.2. Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente;

15.3.3. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior, conforme item 10.8 do Anexo VII-A da IN SEGES/MPDG n. 5, de 2017.

15.3.4. Poderá ser admitida, para fins de comprovação de quantitativo mínimo do serviço, a apresentação de diferentes atestados de serviços executados de forma concomitante, pois essa situação

se equivale, para fins de comprovação de capacidade técnico-operacional, a uma única contratação, nos termos do item 10.9 do Anexo VII-A da IN SEGES/MPDG n. 5/2017.

15.3.5. O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços, consoante o disposto no item 10.10 do Anexo VII-A da IN SEGES/MPDG n. 5/2017.

15.3.6. Conforme item 1.7 do Anexo I da IN SGD/ME nº 01/2019, o licitante vencedor deverá apresentar declaração que ateste a não ocorrência do registro de oportunidade, seguindo o modelo apresentado no Anexo VI deste T.R.

16. DA SUSTENTABILIDADE AMBIENTAL

16.1. Não se vislumbra impacto ambiental, pois os equipamentos estão instalados na Sede/CTN e UD's, conforme suas características.

16.2. A CONTRATADA obriga-se a implantar, na execução dos serviços, boas práticas ambientais, devendo as especificações dos insumos necessários para a execução dos serviços, atender as normas ambientais vigentes, principalmente no que tange ao uso de produtos biodegradáveis.

16.3. A CONTRATADA deverá atender, no que couber, as recomendações contidas no Capítulo III, DOS BENS E SERVIÇOS, com ênfase no art. 5º da Instrução Normativa nº 01/2010 STI/MP, 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.

16.4. Deverão ser adotadas pela CONTRATADA, todas as normas federais, estaduais e municipais quanto aos critérios de preservação ambiental, além das orientações das entidades públicas que versem sobre a matéria, dentre as quais as seguintes: I - Todos os resíduos gerados durante o serviço deverão ser dispostos em lugar adequado ou aterro sanitário, em conformidade com a resolução do CONAMA 307/2002 e suas posteriores alterações (Resoluções 348/2004, 431/2011 e 448/2012).

17. DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

17.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria Fundacentro nº 630, de 17 de agosto de 2021 (SEI ID [0119345](#)).

17.2. Conforme o §6º do art. 12 da IN SGD/ME nº 1, de 2019, o Termo de Referência ou Projeto Básico será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC, e aprovado pela autoridade competente.

Norisvaldo Ferraz Júnior
Analista em C&T
Matrícula 1503899
(assinado eletronicamente)

Diego Ricardi dos Anjos
Coordenador da CTIC
Matrícula 1959350
(assinado eletronicamente)

Juan Gomes Pereira
Assistente em C&T
Matrícula 1989562
(assinado eletronicamente)

Aprovo.

Encaminha-se à Autoridade Competente para prosseguimento da contratação.

Allan David Soares

Diretor Substituto da Diretoria de Conhecimento e Tecnologia
(assinado eletronicamente)

Aprovo.

Encaminha-se à Diretoria de Administração e Finanças para iniciar procedimento licitatório, segundo o art. 38 da Lei nº 8.666, de 21 de junho de 1993.

Luciana Ferrari Siqueira

Presidente da FUNDACENTRO
(assinado eletronicamente)



Documento assinado eletronicamente por **Diego Ricardi dos Anjos, Coordenador(a)**, em 03/11/2022, às 16:22, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Norisvaldo Ferraz Junior, Analista em Ciência e Tecnologia**, em 03/11/2022, às 16:22, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Juan Gomes Pereira, Assistente em Ciência e Tecnologia**, em 04/11/2022, às 10:57, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Luciana Ferrari Siqueira, Presidente**, em 11/11/2022, às 20:20, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site https://sei.fundacentro.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0180645** e o código CRC **71EBC9D2**.

ANEXO I - ORDEM DE FORNECIMENTO DE BENS

1 – IDENTIFICAÇÃO			
Nº da OS/OFB		Data de emissão	
Contrato nº			
Objeto do Contrato			
Contratada		CNPJ	
Preposto			
Início vigência		Fim vigência	
ÁREA REQUISITANTE			
Unidade			
Solicitante		E-mail	

2 – ESPECIFICAÇÃO DOS BENS E VOLUMES ESTIMADOS					
Item	Descrição do bem ou serviço	Métrica	Valor unitário (R\$)	Qtde/Vol.	Valor Total (R\$)
1					
...					
Valor total estimado da OFB					

3 – INSTRUÇÕES COMPLEMENTARES	
<ul style="list-style-type: none"> A OFB deverá ser executada de acordo com o especificado no Termo de Referência. As licenças e os serviços a elas atrelados poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do contrato, às custas da CONTRATADA, sem prejuízo da aplicação de penalidades. O descumprimento dos níveis mínimos de serviço, poderão ensejar a aplicação das sanções previstas no Termo de Referência. A CONTRATADA declara concordância em executar as atividades descritas nesta OFB, de acordo com as especificações estabelecidas pela FUNDACENTRO definidas no CONTRATO. 	

4 – DATAS E PRAZOS PREVISTOS			
Data de Início:		Data do Fim:	
CRONOGRAMA DE EXECUÇÃO/ENTREGA			
Item	Tarefa/entrega	Início	Fim
1			
...			

5 – ASSINATURA E ENCAMINHAMENTO DA DEMANDA	
Autoriza-se a entrega das licenças correspondentes à presente OFB, no período e nos quantitativos acima identificados.	
<p>_____</p> <p><Nome ></p> <p><Responsável pela demanda/ Fiscal Requisitante></p> <p>Matr.: <Nº da matrícula></p>	<p>_____</p> <p><Nome ></p> <p>Gestor do Contrato</p> <p>Matr.: <Nº da matrícula></p>

São Paulo, xx de xxxxxxxx de 20xx

ANEXO II - MODELO PARA APRESENTAÇÃO DE PROPOSTAS

NOME DA EMPRESA LICITANTE:

CNPJ:

ENDEREÇO:

TELEFONE:

E-mail:

Lote	Item	Descrição	Qtd.	Unidade de medida	Valor unitário estimado para 48 meses	Valor total estimado para 48 meses
1	1	Equipamento firewall principal para a Sede/CTN (FortiGate-400E – FG-400E – HW)	1	unidade		
	2	Licença de firewall principal FortiGate-400E Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web Filtering, Antispam Service, and 24x7 Fortinet) válida por 48 meses	1	licença para uso de software		
	3	Licença de firewall de escritório remoto para as UD's (FTNT-RENEW - RENEW - 48 M – Fortigate 30E) válida por 48 meses	12	licença para uso de software		
	4	Licença de gerenciador de	1	licença		

	firewall (FortiManager) válida por 48 meses		para uso de software		
Total estimado para 48 meses					

A Contratada apresenta como Preposto do Contrato a ser firmado, o(a) Sr(a). _____,
email para contato: _____.

O papel do preposto, segundo a Instrução Normativa SGD/ME 01 de 04 de abril de 2019 é ser o representante da contratada, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto à contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual.

ANEXO III - TERMOS DE RECEBIMENTO PROVISÓRIO E DEFINITIVO

1 - IDENTIFICAÇÃO			
CONTRATO Nº	xx/aaaa		
CONTRATADA	<Nome da Contratada>	CNPJ	xxxxxxxxxxxxx
Nº DA OS/OFB	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2 – ESPECIFICAÇÃO DOS PRODUTOS/BENS E VOLUMES DE EXECUÇÃO			
SOLUÇÃO DE TIC			
<Descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>			
ITEM	DESCRIÇÃO DO BEM OU SERVIÇO	MÉTRICA	QUANTIDADE
1	<Descrição igual ao da OS/OFB de abertura>	<Ex.: PF>	<n>
...			
TOTAL DE ITENS			

RECEBIMENTO PROVISÓRIO

3 – RECEBIMENTO PROVISÓRIO

Por este instrumento, atestamos, para fins de cumprimento do disposto no art. 33, inciso II, alínea “a”, da IN SGD/ME nº 01/2019, atualizada pela IN SGD/ME nº 31/2021, que os <serviços / bens> correspondentes à <OS/OFB> acima identificada, conforme definido no Modelo de Execução do contrato supracitado, foram recebidos provisoriamente na presente data e serão objetos de avaliação por parte da CONTRATANTE quanto à adequação da entrega às condições contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato.

Ressaltamos que o recebimento definitivo destes serviços ocorrerá após a verificação dos requisitos e demais condições contratuais, desde que não se observem inconformidades ou divergências quanto às especificações constantes do Termo de Referência e do Contrato acima identificado que ensejem correções por parte da CONTRATADA.

4 - ASSINATURA**FISCAL TÉCNICO**

<Nome do Fiscal Técnico do Contrato>

Matrícula: xxxxxx

<Local>, <dia> de <mês> de <ano>.

RECEBIMENTO DEFINITIVO**3 – ATESTE DE RECEBIMENTO DEFINITIVO**

Por este instrumento atestamos, para fins de cumprimento do disposto na alínea “f”, inciso II, e alínea “d”, inciso III, do art. 33, da IN SGD/ME Nº 1/2019, alterada pela IN SGD/ME nº 31/2021, que os <serviços / bens> correspondentes à <OS/OFB> acima identificada foram <prestados/entregues> pela CONTRATADA e atendem às condições contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Termo de Referência do Contrato acima indicado.

4 – DESCONTOS EFETUADOS E VALOR A LIQUIDAR

De acordo com os critérios de aceitação e demais termos contratuais, <não> há incidência de descontos por desatendimento dos indicadores de níveis de serviços definidos.

<Não foram / Foram> identificadas inconformidades técnicas ou de negócio que ensejam indicação de glosas e sanções, <cuja instrução corre em processo administrativo próprio (nº do processo)>.

Por conseguinte, o valor a liquidar correspondente à <OS/OFB> acima identificada monta em R\$ <valor> (<valor por extenso>).

Referência: <Relatório de Fiscalização nº xxxx ou Nota Técnica nº yyyy>.

5 - ASSINATURA**FISCAL TÉCNICO**

<Nome do Fiscal Técnico do Contrato>

Matrícula: xxxxxx

<Local>, <dia> de <mês> de <ano>.

FISCAL REQUISITANTE

<Nome do Fiscal Requisitante do Contrato>

Matrícula: xxxxxx

<Local>, <dia> de <mês> de <ano>.

6 - AUTORIZAÇÃO PARA FATURAMENTO**GESTOR DO CONTRATO**

Nos termos da alínea “e”, inciso I, art. 33, da IN SGD/ME nº 01/2019, atualizada pela IN SGD/ME nº 31/2021, AUTORIZA-SE a **CONTRATADA** a <faturar os serviços executados / apresentar as notas fiscais dos bens entregues> relativos à supracitada <OS/OFB>, no valor discriminado no item 4, acima.

<Nome do Gestor do Contrato>

Matrícula: xxxxxxxx

<Local>, <dia> de <mês> de <ano>

ANEXO IV - TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

Pelo presente instrumento a Fundação Jorge Duprat Figueiredo de Segurança e Medicina do Trabalho, sediada na Rua Capote Valente, 710, Pinheiros, São Paulo, CEP 05409-002, CNPJ 62.428.073/0001-36, doravante denominada CONTRATANTE, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ nº <Nº do CNPJ>, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º <nº do contrato> doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE; CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção; CONSIDERANDO o disposto na Política de Segurança da Informação e Privacidade da CONTRATANTE;

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

1. OBJETO

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

2. CONCEITOS E DEFINIÇÕES

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

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

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de 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 Art. 87 da Lei nº. 8.666/93.

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 Paulo, 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**

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.

São Paulo, ____ de _____ de 20__.

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

TESTEMUNHAS	
<hr/>	<hr/>
<Nome> <Qualificação>	<Nome> <Qualificação>

ANEXO V - TERMO DE CIÊNCIA

IDENTIFICAÇÃO

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

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

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

São Paulo, XX de XXXX de 20XX.

Assinatura e identificação do representante legal da CONTRATADA

ANEXO VI - DECLARAÇÃO DE NÃO OCORRÊNCIA DE REGISTRO DE OPORTUNIDADE

Razão Social:
CNPJ:
Endereço da Sede:

Pela presente DECLARAÇÃO, a Contratada atesta a não ocorrência do registro de oportunidade - para a Fundação Jorge Duprat Figueiredo de Segurança e Medicina do Trabalho (FUNDACENTRO) - junto ao fabricante da solução para o fornecimento das licenças de que trata a presente contratação .

Assinatura e identificação do representante legal da CONTRATADA

Criado por [norisjunior](#), versão 7 por [norisjunior](#) em 21/10/2022 10:36:30.